BÂTISSEURS D'HERITAGES

Plateforme OPTIGEST360

POLITIQUE DE SÉCURITÉ

Mesures techniques et organisationnelles de sécurité des données

Version : [date] — 09/11/2026

Finalité couverte : Gestion de l'application OPTIGEST360

ALERTE – À LIRE AVANT USAGE

Document créé le 09/11/2026 pour le dépôt ARTCI (champ « politique de sécurité », étape 4). Décrit l'état réel du dispositif.

Ne déclare que des mesures en place. 2FA : prévue, non encore active — à activer avant diffusion grand public. Aucun audit externe réalisé à ce jour.

—

ARTICLE 1 – OBJET

La présente politique décrit les mesures techniques et organisationnelles mises en œuvre par BÂTISSEURS D'HERITAGES pour garantir la sécurité et la confidentialité des données traitées dans OPTIGEST360, conformément à la loi n°2013-450 du 19 juin 2013.

ARTICLE 2 – ARCHITECTURE ET RÉSEAU

- Hebergement sur serveurs situes en France (LWS), datacenters declares certifies ISO/IEC 27001 ; copies de sauvegarde conservees chez le meme hebergeur, en France.
- Accès applicatif exclusivement en HTTPS (chiffrement TLS des communications).
- Réseau segmenté et pare-feu au niveau de l'infrastructure d'hébergement.
- Détection et prévention des intrusions assurées au niveau de l'hébergeur.

ARTICLE 3 – ACCÈS ET AUTHENTIFICATION

- Accès aux données limité aux personnes autorisées ; gestion des habilitations par rôles et droits d'accès adaptés aux fonctions ; principe du moindre privilège.
- Authentification par identifiant et mot de passe individuel haché ; mot de passe initial provisoire transmis par e-mail, à modifier à la première connexion. L'authentification à double facteur (2FA) est prévue.
- Procédure d'attribution, de modification et de retrait des droits d'accès.

L'accès d'un agent de la Société à l'espace d'un client est subordonné à un motif écrit, conservé et horodaté. Cette règle est une règle d'organisation : elle n'est pas, à ce jour, imposée par le logiciel. Depuis le 26/10/2026, chaque client peut consulter l'intégralité des accès effectués sur son espace.

ARTICLE 4 – JOURNALISATION

Les accès et actions sur les données (connexion/déconnexion, consultation, création, modification, suppression) sont journalisés. Les journaux permettent d'identifier l'utilisateur ainsi que la date et l'heure de l'action.

ARTICLE 5 – PROTECTION DES DONNÉES

- Chiffrement des données au repos (base de données, systèmes de stockage) et en transmission (TLS).
- Environnements de développement et de test alimentés en données anonymisées ou fictives.
- Protection des supports et des postes (antivirus, contrôle d'accès).

ARTICLE 6 – SAUVEGARDE ET SUPPRESSION

- Sauvegardes régulières (quotidiennes) externalisées chez l'hébergeur, conservées 14 à 30 jours, chiffrées et protégées contre les accès non autorisés ; contrôle d'intégrité.
- Suppression des données lorsqu'elles ne sont plus nécessaires, y compris dans les sauvegardes au terme de leur cycle ; procédure de suppression sécurisée.

ARTICLE 7 – VIOLATIONS DE DONNÉES

Une procédure de gestion des violations est définie : identification, signalement, analyse, mesures correctives, notification des personnes concernées et de l'autorité compétente lorsque cela est requis. Un registre des violations est tenu. La Société notifie au Client toute violation le concernant dans les meilleurs délais, et au plus tard 72 heures après en avoir pris connaissance.

ARTICLE 8 – PRESTATAIRES ET MAINTENANCE

Les prestataires ayant accès aux données sont soumis à des obligations de confidentialité ; les opérations de maintenance et de télémaintenance sont encadrées et supervisées par une personne habilitée. Les conditions de restitution et de destruction des données en fin de contrat sont formalisées. Le seul destinataire est LWS - Ligne Web Services, etabli en France.

ARTICLE 9 – CERTIFICATIONS ET AUDITS

La Société s'appuie sur les garanties de son hébergeur, dont les datacenters sont déclarés certifiés ISO/IEC 27001. BÂTISSEURS D'HERITAGES ne dispose pas, à ce jour, d'une certification en propre et n'a pas fait réaliser d'audit de sécurité externe.