LTC Group — Nota

Mesures de sécurité techniques et organisationnelles — Nota

LTC Group SRL · Version 1.0 · 12 août 2026 · contact@ltcai.be

Mesures de sécurité techniques et organisationnelles

1. Principes

La sécurité de Nota repose sur quatre principes appliqués dès la conception, et non ajoutés a posteriori :

- **Défense en profondeur** : plusieurs couches de protection indépendantes — réseau, application, données, pipeline IA — de sorte que la défaillance d'une seule couche ne compromette pas l'ensemble du système.
- **Moindre privilège** : chaque rôle utilisateur, chaque compte de service et chaque accès LTC ne dispose que des droits strictement nécessaires à sa fonction.
- **Privacy by design** : la protection des données est intégrée à l'architecture elle-même — pseudonymisation systématique par Veil™ en amont de tout LLM cloud, cloisonnement logique strict des données par étude, chiffrement systématique en transit et au repos — plutôt que rajoutée en surface.
- **Environnements séparés** : le développement et le staging s'exécutent sur une infrastructure LTC distincte de la production, alimentée exclusivement par des données fictives ; les données de production ne sont jamais utilisées en développement ou en test.

Réponse directe aux cinq domaines habituellement couverts par une revue de sécurité :

Domaine	Mesure Nota	Détail
Chiffrement des données en transit et/ou au repos	TLS 1.2+/1.3 en transit ; AES-256 au repos (base de données, stockage objets, sauvegardes) ; clés gérées par LTC, secrets en gestionnaire dédié	§2
Gestion des accès (droits, rôles)	RBAC par étude, moindre privilège, cloisonnement logique strict par étude (RLS, option d'instance dédiée), revue périodique des accès, accès LTC à la production restreint/nominatif/journalisé	§3
Mécanismes d'authentification (mots de passe, 2FA)	E-mail et mot de passe fort ; 2FA TOTP obligatoire pour les administrateurs, activable pour tous ; verrouillage après échecs répétés ; itsme (OIDC) envisagé	§4

Domaine	Mesure Nota	Détail
	comme authentification forte complémentaire, démarche d'onboarding en cours	
Journalisation / traçabilité des accès	Journal d'audit append-only (qui, quoi, quand) sur toute donnée de dossier, consultable par l'administrateur de l'étude, y compris les actions de l'agent IA	§5
Sauvegardes et restauration	Sauvegardes quotidiennes chiffrées, rétention 35 jours, hébergées en UE (OVHcloud, France), tests de restauration périodiques, RPO 24 h / RTO cible 24 h	§6

2. Chiffrement

Tous les flux entre le poste de l'utilisateur, Nota et ses sous-traitants sont chiffrés en **TLS 1.2+/1.3**. Au repos, les données sont chiffrées en **AES-256** sur l'ensemble des supports de persistance : base de données (PostgreSQL 16 + pgvector, sur l'instance OVHcloud dédiée), stockage objets S3-compatible (documents de la GED) et sauvegardes.

La gestion des clés de chiffrement reste sous le contrôle exclusif de LTC. Les secrets applicatifs (identifiants techniques, clés d'API, jetons) sont conservés dans un gestionnaire de secrets dédié, jamais en clair dans le code source ou les fichiers de configuration.

3. Gestion des accès & rôles

L'accès aux données est structuré par un modèle **RBAC (Role-Based Access Control) appliqué par étude** : chaque utilisateur n'accède qu'aux données de son étude, jamais à celles d'une autre. Techniquement, Nota repose sur une **base mutualisée avec cloisonnement logique strict** : le Row-Level Security de PostgreSQL est activé et forcé sur chaque table métier (une policy par table, clé par étude), indépendamment des contrôles applicatifs. Une **instance physiquement dédiée par étude est proposée en option** pour les études qui l'exigent.

Rôle	Portée d'accès typique
Notaire titulaire/associé	Accès complet aux dossiers de l'étude ; supervision des rôles
Administrateur d'étude	Gestion des comptes utilisateurs et des rôles, paramétrage de sécurité, consultation du journal d'audit
Collaborateur	Dossiers de l'étude selon assignation et habilitation
Comptable	Données patrimoniales et financières liées aux dossiers
Stagiaire	Accès restreint, sous supervision

Rôle	Portée d'accès typique
Client de l'étude (portail)	Son propre dossier uniquement ; e-mail et mot de passe fort avec 2FA TOTP, itsme envisagé en complément (onboarding en cours)

Le principe de **moindre privilège** s'applique à chaque rôle, avec séparation entre comptes d'administration et comptes d'usage courant. Les habilitations font l'objet d'une **revue périodique**, sous la responsabilité de l'administrateur de l'étude.

L'**accès de LTC aux données de production** est distinct de ces rôles : il est **restreint** (personnel technique habilité uniquement), **nominatif** (pas de compte partagé), **journalisé** dans le journal d'audit, et n'intervient que pour des besoins de support, **sur autorisation de l'étude**.

4. Authentification

L'authentification s'effectuera par e-mail et mot de passe fort avec 2FA TOTP ; l'intégration d'itsme (OIDC) comme mode d'authentification forte, en particulier pour le portail client, fait l'objet d'une démarche d'onboarding en cours.

- **email + mot de passe fort**, avec exigences de robustesse (longueur, complexité) — mode d'authentification actif dès l'ouverture ;
- **itsme (OIDC)** — authentification forte envisagée, en particulier pour le portail client de l'étude ; intégration non encore disponible, en cours d'onboarding.

Une **authentification à deux facteurs (2FA) par TOTP** vient renforcer l'authentification par e-mail et mot de passe : **obligatoire pour tous les comptes administrateurs**, elle est **activable par tout autre utilisateur**. Un mécanisme de **verrouillage de compte après un nombre d'échecs répétés** limite les tentatives d'accès frauduleuses. Les sessions sont gérées **côté serveur**, ce qui permet leur invalidation immédiate en cas de besoin (déconnexion forcée, changement de mot de passe, révocation).

5. Journalisation & traçabilité

Un **journal d'audit append-only** — c'est-à-dire non modifiable a posteriori, y compris par les équipes techniques de LTC — enregistre **qui** a accédé à **quelle** donnée de dossier, **quand**, et quelle action y a été réalisée (consultation, création, modification, export, suppression). Ce journal est **consultable par l'administrateur de l'étude**, qui garde ainsi un contrôle direct sur l'usage fait des données de son étude, y compris sur les interventions de support de LTC.

Durée de conservation du journal d'audit. Les entrées du journal sont conservées **12 mois glissants par défaut**, durée **paramétrable par l'étude jusqu'à 36 mois** — de quoi couvrir un cycle complet d'audit de la profession — puis **purgées automatiquement** à échéance. La durée retenue par l'étude, responsable du traitement, est consignée dans son paramétrage de rétention. Le caractère append-only interdit toute modification ou suppression unitaire d'une entrée avant son échéance, y compris par

LTC : seule la purge automatique par expiration s'applique. À la fin du contrat, le journal suit le sort des données de dossiers (restitution puis suppression sous 60 jours, article 13 du DPA). Les entrées ne contiennent pas le contenu des dossiers, mais l'identité du compte, l'horodatage, l'action et la référence de l'objet concerné.

Les actions de l'**assistant IA agentique** (recherche IA globale opérant sur dossiers, mails, GED et connecteurs) sont tracées selon le même principe que les actions humaines : chaque action de l'agent est journalisée, ce qui permet à l'étude de vérifier a posteriori ce que l'agent a consulté ou proposé. Cette traçabilité s'inscrit dans le contrôle humain systématique du produit — le notaire relit, corrige et valide toujours le résultat avant tout effet juridique.

6. Sauvegardes & restauration

Les sauvegardes de la base de données et du stockage objets sont **quotidiennes**, **chiffrées (AES-256)** et **conservées en UE** sur l'infrastructure **OVHcloud (France)**. La **rétention est de 35 jours**, au-delà desquels les sauvegardes expirent et sont purgées automatiquement — ce délai s'applique également, en aval, à la purge des sauvegardes lors d'une résiliation.

Des **tests de restauration périodiques** vérifient que les sauvegardes sont effectivement exploitables, et pas seulement produites. Un plan de continuité documenté fixe des objectifs de reprise : **RPO (perte de données maximale tolérée) de 24 heures** et **RTO (délai de reprise du service) cible de 24 heures**.

7. Sécurité réseau & infrastructure

Nota est hébergé sur une **instance OVHcloud (France, UE — certifiée ISO 27001) dédiée**, gérée intégralement par LTC (applicatif, base de données, stockage, IA propriétaires), **sans mutualisation** avec d'autres charges. L'exposition réseau est réduite au strict nécessaire : **seul le reverse-proxy TLS est accessible publiquement** ; les services internes — base de données, IA propriétaires LTC, workers de traitement — **ne sont pas exposés sur internet**. Les composants applicatifs sont **isolés par conteneurs**, ce qui limite la surface d'impact en cas de compromission d'un composant isolé.

8. Pipeline IA

Rappel d'un invariant produit déjà détaillé dans les pages IA de ce centre de confiance : **aucune donnée nominative de dossier n'est transmise à un LLM cloud**. Avant tout appel, le texte passe par **Veil™**, le moteur propriétaire de pseudonymisation de LTC (détection déterministe C1, NER bilingue fr/nl C2, LLM critique local C3). La **table de réversion réside exclusivement en mémoire vive**, dans un vault dédié, **chiffrée AES-256-GCM** (clé de session aléatoire) : elle n'est jamais transmise ni persistée côté fournisseur d'inférence. Le durcissement mémoire du vault (mlock non-swappable, désactivation du swap et des core-dumps) est **planifié avant le pilote** et n'est pas encore actif. Des

tests automatisés anti-fuite (« corpus no-leak ») s'exécutent en continu pour vérifier l'absence de fuite de données nominatives.

9. Cycle de développement sécurisé

Le cycle de développement de Nota intègre la sécurité à chaque étape : **revues de code** systématiques, **tests automatisés** — dont les tests anti-fuite du pipeline Veil —, **intégration et déploiement continus (CI/CD)**, et **analyse continue des dépendances** avec application prioritaire des correctifs de sécurité. Les environnements de développement et de test restent isolés de la production et n'utilisent que des données fictives.

LTC, structure de moins de dix personnes, ne détient **aucune certification de sécurité propre** à ce stade. L'approche s'appuie sur les certifications des infrastructures sous-jacentes — **OVHcloud (ISO 27001)** pour l'hébergement, **AWS (ISO 27001/27017/27018, SOC 2)** pour l'inférence Bedrock — ainsi que sur la présente démarche de sécurité documentée. Un **test d'intrusion (pentest) indépendant est planifié avant la mise en production du pilote**.

10. Gestion des incidents et continuité

La gestion des incidents de sécurité s'appuie sur une **procédure documentée**, détaillée dans le DPA : détection par monitoring et alertes, qualification de l'incident, **notification au client responsable — l'étude — sans délai injustifié et au plus tard 24 heures après constat**, avec les informations prévues à l'article 33.3 du RGPD, tenue d'un **registre interne des incidents**, et post-mortem systématique. Cette procédure de notification des violations relève du DPA et s'applique sans exception aux incidents touchant des données de dossiers.

La continuité de service s'appuie sur les sauvegardes et les objectifs de reprise décrits en §6, complétés par un support en jours ouvrés belges (email et visio), une **première réponse en moins de 4 heures ouvrées**, un traitement prioritaire des incidents critiques et un **objectif de disponibilité mensuelle de 99,5 %** — formulés comme objectifs de niveau de service au stade pilote.

11. Sensibilisation de l'équipe

L'équipe LTC suit des **sessions périodiques de sensibilisation** à la sécurité et à la protection des données, portant notamment sur la manipulation des données de dossiers, les bonnes pratiques d'accès et la reconnaissance des tentatives d'ingénierie sociale. Une **politique interne d'utilisation de l'IA**, écrite et signée des fondateurs, est effective depuis le 12/08/2026 : elle encadre l'usage des outils d'IA en interne et rappelle le passage obligatoire par Veil™ pour toute donnée de dossier avant tout traitement par un LLM externe. Compte tenu de la taille de la structure (moins de dix personnes), la gouvernance sécurité est portée directement par les fondateurs, sans dilution de responsabilité.

LTC Group SRL · BCE 1036.831.317 · Rue du Noir Jambon 13, 7830 Thoricourt, Belgique · contact@ltcai.be
Document publié dans le centre de confiance Nota : https://www.ltcai.be/nota/confiance