VaultLM

Aperçu sécurité VaultLM

Flux de données et principes de sécurité pour l'IA documentaire confidentielle

CE QU'EST VAULTLM

Un espace contrôlé entre documents confidentiels et IA. VaultLM applique droits, masquage et pseudonymisation avant le traitement externe, puis renvoie des réponses avec sources et piste d'audit.

1. Documents

Les originaux entrent dans un coffre gouverné avec droits et conservation.

2. Protéger

Les identifiants sensibles sont masqués et pseudonymisés.

3. Minimiser

Seuls les extraits pertinents et autorisés sont sélectionnés.

4. Service IA

Le service externe choisi reçoit le contexte protégé minimal.

5. Preuves

La réponse revient avec passages cités et usage consigné.

RESTE DANS VAULTLM

Fichiers originaux, correspondances d'identité, droits et conservation.

ENVOYÉ AU TRAITEMENT IA

Uniquement les extraits minimaux, autorisés et pseudonymisés.

PRINCIPES DE SÉCURITÉ

Lié aux droits

L'accès IA ne dépasse jamais le droit d'ouvrir les sources.

Fail-closed

Si le masquage requis est indisponible, la requête externe s'arrête.

Fondé sur les documents

Les requêtes externes sont liées à des sources autorisées du coffre.

Vérifiable

Sources, service utilisé et audit soutiennent la revue humaine.

LIMITES HONNÊTES

Un masquage réversible est une pseudonymisation, pas une anonymisation. La détection automatique n'est pas infaillible et une revue humaine reste nécessaire. VaultLM soutient la gouvernance et les preuves sans garantir automatiquement la conformité.

CALENDRIER AI ACT

D'autres dispositions de l'AI Act s'appliquent à partir du 2 août 2026. Les règles relatives aux systèmes à haut risque ont des échéances ultérieures : 2 décembre 2027 pour les systèmes autonomes et 2 août 2028 pour les systèmes intégrés à des produits