VaultLM

VaultLM beveiligingsoverzicht

Datastroom en beveiligingsprincipes voor AI op vertrouwelijke documenten

WAT VAULTLM IS

Een gecontroleerde werkruimte tussen vertrouwelijke documenten en AI. VaultLM past rechten, datamaskering en pseudonimisering toe vóór externe AI-verwerking en geeft antwoorden terug met bronnen en een audit trail.

1. Documenten

Originele bestanden komen in een beheerde vault met rechten en bewaartermijnen.

2. Beschermen

Gevoelige identificerende gegevens worden gemaskeerd en gepseudonimiseerd.

3. Minimaliseren

Alleen relevante en toegestane passages worden geselecteerd.

4. AI-dienst

De gekozen externe AI-dienst ontvangt minimale beschermde context.

5. Bewijs

Het antwoord komt terug met bronpassages en vastgelegd gebruik.

BLIJFT IN VAULTLM

Originele bestanden, identiteitskoppelingen, rechten en bewaartermijnen.

NAAR AI-VERWERKING

Alleen minimaal benodigde, toegestane en gepseudonimiseerde passages.

BEVEILIGINGSPRINCIPES

Rechtengebonden

AI-toegang gaat nooit verder dan het recht om de bron te openen.

Fail-closed

Is noodzakelijke maskering niet beschikbaar, dan stopt de externe AI-vraag.

Documentgebonden

Externe AI-vragen zijn gekoppeld aan toegestane vaultbronnen, niet aan een vrije promptproxy.

Controleerbaar

Bronnen, route-informatie en auditgebeurtenissen ondersteunen menselijke controle.

EERLIJKE GRENZEN

Omkeerbare maskering is pseudonimisering, geen anonimisering. Automatische herkenning is niet onfeilbaar; menselijke controle blijft nodig bij gevoelige of impactvolle beslissingen. VaultLM ondersteunt governance en bewijs, maar garandeert niet automatisch juridische compliance.

AI ACT-TIMING

Vanaf 2 augustus 2026 gelden meer onderdelen van de AI Act. Voor hoog-risicosystemen gelden latere termijnen: 2 december 2027 voor zelfstandige systemen en 2 augustus 2028 voor systemen die in gereguleerde producten zijn ingebouwd.