Beveiligings- en architectuursamenvatting

LectaMe, aangeboden door LYNT V.O.F. (KvK 97241229) · Versie 1.0 · 14 november 2026

Meest actuele versie en bijbehorende stukken: https://lectame.com/voor-scholen/leveranciersinformatie

Beveiliging

Hosting [Beschikbaar]: Eén productieserver (VPS) bij Leaseweb in Amsterdam, met twee instanties van de applicatie achter een proxy, en zelf gehoste database, authenticatie en bestandsopslag.

Schoolisolatie [Beschikbaar]: Elke school is een eigen organisatie; gegevens hangen via dat id aan één school. Toegang wordt zowel in de database (row-level security) als in de applicatie afgedwongen. Getest met twee fictieve scholen in een QA-omgeving; een beheerder van school A krijgt voor school B een 404.

Externe diensten [Beschikbaar]: Cloudflare (DNS, CDN, beveiliging, terugval-AI voor docentinhoud, bedoeld zonder persoonsgegevens van studenten), Groq (AI voor docentinhoud, bedoeld zonder persoonsgegevens van studenten), Resend (e-mail), Mollie (betalingen) en optioneel Google Analytics na toestemming.

Inloggen en MFA voor platformbeheer [Beschikbaar]: Toegang tot platformbeheer vereist een tweede factor.

MFA voor schoolbeheerders [Nog in voorbereiding]: Een tweede factor is vereist voor onder meer rolbeheer, het bewaarbeleid en de schoolbrede export. Een bredere eis voor alle schrijfhandelingen en een verplichte inschrijving zijn gebouwd of ontworpen maar nog niet voor alle scholen ingeschakeld.

Logging [Beschikbaar]: Audit- en beheerlogs leggen wie wat deed, zonder de inhoud van studentwerk. Foutlogs worden geanonimiseerd en maximaal 30 dagen bewaard.

Back-ups en herstel [Niet bevestigd]: Dagelijkse back-ups, lokaal en versleuteld offsite. De bewaartermijnen staan in het privacyoverzicht. Een hersteltijd en maximaal dataverlies (RTO/RPO) zijn nog niet gemeten en worden daarom niet toegezegd.

Melden van kwetsbaarheden [Beschikbaar]: Meldpunt tech@lynt.nl met een openbaar beleid in security.txt en op de beveiligingspagina; een melder mag na ongeveer 14 dagen reactietijd publiceren. Het alarmpad van monitoring tot ontvanger is nog niet met een proefalarm getest.

Architectuur op hoofdlijnen

Gebruiker (student, docent, schoolbeheerder of gast) ’ Cloudflare (DNS, CDN, beveiliging) ’ proxy.

Proxy ’ twee applicatie-instanties (A en B) op één server bij Leaseweb, Amsterdam.

Applicatie ’ zelf gehoste database (met schoolisolatie) en bestandsopslag, beide op dezelfde server.

Applicatie ’ AI: studentinhoud niet extern; docentinhoud (bedoeld zonder persoonsgegevens van studenten, ook transcriptie van docentaudio) via een gegevensklasse-poort naar Groq, met Cloudflare Workers AI als terugval.

Applicatie ’ e-mail via Resend; audit- en foutlogs op de server.

Database en opslag ’ versleutelde back-ups, lokaal en offsite (locatie en verwerker offsite niet bevestigd).