

IttesAI: security overzicht

Bij Ittes staat jouw data centraal. We combineren beproefde technieken met heldere afspraken. Zo weet je precies wat wij doen en welke keuzes jij hebt.

Samenvatting van onze beveiligingsmaatregelen

Cloudservers in eigen beheer

Servers van Ittes, afgeschermd met SSH en IP-toegangscontrole op onze kantoorlocaties.

Datalaag op maat

MySQL voor gestructureerde data, Qdrant voor tekst en Minio voor documenten.

Volledige encryptie

MySQL versleuteld at rest, HTTPS verkeer, TLS voor Qdrant communicatie.

Beveiligde aanmelding

Microsoft 365 login met Entra ID en 2FA.

Veilige wachtwoorden

Opgeslagen met bcrypt en extra controle tegen gekende datalekken via het k-anonymity model.

Authentieke beveiliging

Rate limiting en bescherming tegen user enumeration.

Samenwerking met AI providers

Gratis AI-modellen gebruiken vaak persoonlijke data om zichzelf slimmer te maken. Bij IttesAI gebeurt dit niet. Wij werken enkel met betalende API's van betrouwbare AI-providers en maken duidelijke afspraken over wat er met jouw data gebeurt. Zo blijft jouw informatie veilig en vertrouwelijk.

Jij blijft eigenaar

Je kan je gebruikersdata of volledige workspace data verwijderen via één actie.

1. Waar staat jouw data

Onze databases en het platform draaien op servers onder beheer van Ittes, gehost bij onze cloudpartner. Servertoegang verloopt via het SSH protocol en is enkel mogelijk vanuit vertrouwde kantoor IP-adressen.



MySQL

Voor tabellen zoals workspaces, users en conversaties. Gestructureerde data opslag met volledige encryptie.



Qdrant

Voor tekstchunks zodat de AI relevante context kan ophalen. Geoptimaliseerd voor snelle zoekopdrachten.



Minio

Voor bestanden zoals PDF, Word, beelden en video. Veilige opslag met strikte toegangscontrole.

2. Encryptie en transport

MySQL

MySQL is versleuteld at rest met Transparent Data Encryption op basis van AES 256 CBC. De MySQL server staat op dezelfde machine als de app, waardoor interne verbindingen het toestel niet verlaten. Verkeer met de buitenwereld verloopt verplicht via HTTPS.

Qdrant

Qdrant draait op een aparte server voor rekenkracht en gebruikt TLS en HTTPS voor alle communicatie. Qdrant biedt geen encryptie in rust. De impact is enkel relevant bij een reeds gecompromitteerde server, daarom kiezen we hier voor performantie, streng netwerkbeheer en duidelijke scheiding per klant.

Minio

Minio bewaart persoonlijke bestanden per klant in aparte buckets. De standaard bewaartermijn is 6 maanden. Encryptie in rust staat ingepland, de toegang blijft afgeschermd en verkeer naar buiten verloopt via HTTPS.

3. Applicatiebeveiliging

1

Prisma ORM

We verbinden veilig met de database via Prisma. Dit voorkomt veel voorkomende kwetsbaarheden zoals SQL injectie en houdt migraties onder controle.

2

Sessiebeheer

Sessies worden beheerd met NextAuth en werken met ondertekende JWT-tokens. De token wordt gevalideerd bij elke aanvraag. Sessies eindigen automatisch zodra je de browser sluit.

4. Aanmelden en identiteiten

Je kiest tussen aanmelding met [Microsoft 365](#) of met [credentials](#).

Microsoft 365 login

- We gebruiken Entra ID met OAuth 2.0
- Je voert gegevens in op Microsoft pagina, niet bij Ittes
- 2FA uit je Microsoft tenant geldt automatisch ook bij IttesAI
- Je kan aanmelding beperken tot enkel Microsoft login

Credentials login

- Wachtwoorden gehasht met bcrypt
- E-mails versleuteld met AES 256 CBC met unieke IV
- SHA 256 hash voor sneller zoeken
- E-mailadres blijft onzichtbaar in de database

Extra bescherming

Rate limiting

Te veel mislukte aanmeldpogingen zorgen voor een wachttijd. Pogingen per IP en per e-mail worden gelogd en automatisch opgeschoond.

Niet-prijsgeven van gebruikers

Foutmeldingen en user enumeration verraden niet of een e-mail bestaat.

Wachtwoordlek-controle

We toetsen nieuwe wachtwoorden af tegen de Have I Been Pwned databank via k-anonymity. We sturen enkel de eerste 5 tekens van de SHA-1 hash.

5. Hoe en wanneer verlaat data het platform

IttesAI praat met enkele partners wanneer jij dat nodig vindt.



AI providers

OpenAI, Anthropic, Google, Perplexity en Stability AI. Wij sturen enkel wat nodig is, zoals je vraag, context van het gesprek en eventueel geselecteerde documenten of instellingen. Doorgestuurde data wordt niet gebruikt om modellen te trainen



Sociale media

Via Postmaster. We sturen enkel de inhoud en media van geplande posts naar bijvoorbeeld Facebook, Instagram en LinkedIn.

SharePoint-integratie en data embedding

Je kiest zelf welke bestanden de AI mag kennen. Onze partner Truto verwerkt die bestanden tot veilige tekstchunks en laat Cohere Multilingual v3 embeddings berekenen. Daarna schrijven zij de vectors met chunks naar onze Qdrant en verwijderen de data bij hen. Maandelijks synchroniseren we wijzigingen. Truto bewaart je data niet en werkt onder duidelijke privacyafspraken.

6. GDPR en bewaartermijnen

Wij bewaren enkel wat nodig is voor de werking van het platform:

- E-mail als gebruikersnaam
- Eventueel wachtwoord voor credentials
- Geüploade of gesynchroniseerde bestanden
- Conversaties en output voor bewerking in de app
- Een IP bij mislukte logins

Jouw opties:

- *Verwijder mijn gebruikersdata:* wist alle persoonlijke data.
- *Verwijder workspace data:* wist alle data op werkruimteniveau.



Logs van mislukte logins worden maximaal een maand en een week bijgehouden en dan opgeschoond. Persoonlijke bestanden in Minio worden standaard na 6 maanden verwijderd.

Jij beslist over je data

Verwijder mijn gebruikersdata

Verwijdert persoonlijke data gelinkt aan jouw account. Je e-mail blijft nodig om in te loggen, tenzij je het account laat verwijderen of het e-mailadres wijzigt.

Verwijder workspace data

Verwijdert data op werkruimteniveau. Beheerders kunnen dit starten. Je kan ook per record verwijderen in de apps.

7. Aanbevolen voor jouw bedrijf

01

Gebruik **Microsoft 365 login** en verplicht **2FA** in je tenant. Dan geldt 2FA automatisch ook in IttesAI.

02

Controleer je **retentiebeleid** en beslis zelf welke data periodiek verwijderd wordt.

8. Veelgestelde vragen

Wordt mijn data gebruikt om AI-modellen te trainen?

Neen. Wij gebruiken betaalde API's waarbij data niet wordt ingezet om modellen te trainen.

Welke data sturen jullie mee naar een AI-provider?

Enkel wat nodig is voor de functie die jij gebruikt. Bijvoorbeeld de vraag, relevante gesprekscontext en in het geval van SharePoint de relevante tekststukken die jij vooraf hebt goedgekeurd.

Hoe veilig is de klassieke login?

Wachtwoorden worden gehasht met bcrypt, e-mails versleuteld met AES-256 CBC, en we controleren wachtwoorden tegen gekende lekken. Brute force wordt beperkt met rate limiting.

Is alles versleuteld?

- MySQL: volledig versleuteld at rest.
- Qdrant: TLS voor verkeer, geen encryptie at rest.
- Minio: encryptie at rest gepland, verkeer altijd via HTTPS.