Beoordeling door ICT en privacy

ZorgPMO · 13 november 2026 · versie 2026-11-13.5

Leveranciersdossier voor ICT, CISO, FG en architecten. Per onderwerp wat is ingericht en welk bewijs u kunt opvragen.

Beoordeelt u ZorgPMO namens uw ICT-afdeling, CISO, functionaris gegevensbescherming of architectuurteam? Hier staat per onderwerp wat is ingericht en welk bewijs u kunt opvragen.

Statussen: Ingericht (29)

Waarvoor dit dossier is

ZorgPMO is een online platform voor programma's, projecten en samenwerking in zorgorganisaties. Het is geen elektronisch patiëntendossier. Aanbieder is WeDesignworks (KvK 77708091).

Dit dossier beantwoordt de vragen van een ICT-afdeling bij een leveranciersbeoordeling. Wie heeft toegang? Kunnen andere organisaties bij onze gegevens? Waar staan ze? Hoe is de software getest? Wat gebeurt er bij een incident?

De beveiligingsverklaring, de verwerkersovereenkomst, het bewaarbeleid en het leveranciersoverzicht staan als aparte documenten onder Vertrouwen.

Hoe we kwaliteit bewaken

ZorgPMO wordt ontwikkeld met moderne hulpmiddelen, waaronder AI-ondersteuning bij het schrijven van code. De beveiliging rust daarom op controles die voor iedere release hetzelfde zijn en die een release tegenhouden als ze falen.

Elke klantrelease doorloopt twaalf automatische controles in een aparte bouwstraat, los van de ontwikkelomgeving. Haalt een release één controle niet, dan kan die niet worden uitgerold. Handmatig goedkeuren ondanks een fout is technisch uitgesloten.

Alle tien vastgelegde releases tot en met 10 november 2026 hebben alle twaalf controles gehaald. Per release kunt u het bouwlog, de uitkomst per controle en het ondertekende manifest opvragen.

Twaalf controles bij iedere release

Unit- en integratietests — *Ingericht*

Backend-contracttests en frontendtests draaien in tijdelijke, synthetische PostgreSQL- en Redis-omgevingen. Tests gebruiken nooit klantdata.

Bewijs op aanvraag: Bouwlog per release

Typecontrole en codecontrole — *Ingericht*

TypeScript-typecontrole en lintcontrole van de broncode.

Geheimenscan — *Ingericht*

gitleaks (vaste versie, met checksum gecontroleerd) doorzoekt de broncode op wachtwoorden, sleutels en tokens. Een vondst stopt de release.

Bewijs op aanvraag: Scanuitkomst per release

Kwetsbare afhankelijkheden — *Ingericht*

Trivy controleert de gebruikte softwarebibliotheken. Een bekende kwetsbaarheid met ernst HIGH of CRITICAL stopt de release.

Bewijs op aanvraag: Scanuitkomst per release

Containerscan en software-inventaris (SBOM) — *Ingericht*

Elk gebouwd image wordt gescand. Per component maken we een software-inventaris. Bij een nieuw gemelde kwetsbaarheid zien we zo direct of ZorgPMO die bibliotheek gebruikt.

Bewijs op aanvraag: SBOM per component

Testmigraties en applicatieproef — *Ingericht*

Databasemigraties en een opstart- en API-proef draaien op synthetische omgevingen met precies de images die naar klanten gaan.

Omgevingsisolatie — *Ingericht*

Een automatische test probeert vanuit de ene organisatie bij de andere te komen. Onder Scheiding tussen organisaties staat wat er precies wordt getest.

Bewijs op aanvraag: Testuitvoer per release

Ondertekening — *Ingericht*

Het manifest met de exacte image-digests wordt digitaal ondertekend en gecontroleerd. Klantomgevingen draaien alleen onveranderlijke, ondertekende images.

Bewijs op aanvraag: Ondertekend manifest

Scheiding tussen organisaties

Eigen omgeving per organisatie — *Ingericht*

Iedere organisatie krijgt een eigen set containers. Dat is een eigen PostgreSQL-database met eigen databaserol en wachtwoord, eigen bestandsopslag met eigen sleutels, eigen cache (Redis), eigen taakwachtrij (RabbitMQ), eigen API, workers en frontend, op een eigen afgeschermd netwerk. Er is geen gedeelde klantdatabase. Ontwikkeling en demo zijn aparte omgevingen.

Automatische cross-tenant-test bij elke release — *Ingericht*

In de bouwstraat starten twee synthetische organisaties naast elkaar. Zonder sessie is er geen toegang. Een sessie van organisatie A wordt bij B geweigerd. A kan een werkruimte van B niet via de API opvragen. Beide hebben een eigen netwerk en eigen opslagvolumes. Vanuit de API-container van A is de database van B niet vindbaar. De opslagsleutels van B worden door de bestandsopslag van A geweigerd. Cache en opslag starten leeg en bevatten alleen eigen gegevens.

Bewijs op aanvraag: Testuitvoer per release

Controle bij een echte inrichting — *Ingericht*

Bij de oplevercontrole in september 2026 is een tijdelijke klantorganisatie via de normale aanvraagroute ingericht. Toegang tot de werkruimte van een andere klant werd geweigerd (HTTP 403). Een sessiecookie werd bij de andere klant geweigerd (401). Een ondertekende bestandslink werkte niet bij de andere klant (403). Een directe netwerkverbinding naar de database van de andere klant werd geblokkeerd.

Bewijs op aanvraag: Opleverrapport

Platformbeheer afgeschermd — *Ingericht*

Het platformbeheer heeft een eigen database en draait zonder rootrechten, met een alleen-lezen bestandssysteem, zonder Docker-socket en zonder klantconfiguraties. Infrastructuuracties worden alleen door een lokale worker uitgevoerd, na expliciete goedkeuring door de eigenaar, en worden vastgelegd in een auditlog.

Inloggen, rechten en sessies

Persoonlijke accounts en tweestapsverificatie — *Ingericht*

Iedere gebruiker heeft een persoonlijk account. Tweestapsverificatie is beschikbaar via een authenticator-app met herstelcodes en via passkeys (WebAuthn). Een organisatie kan tweestapsverificatie voor al haar gebruikers verplicht stellen. Wij adviseren dat.

Sessies en API-tokens — *Ingericht*

Een sessie eindigt uiterlijk om middernacht Nederlandse tijd en nooit later dan 24 uur na inloggen. Gebruik verlengt die termijn niet. Platformbeheer heeft een kortere sessieduur. Technische API-tokens zijn maximaal 90 dagen geldig en krijgen nooit meer rechten dan het bijbehorende account. Het aantal verzoeken per gebruiker is begrensd.

Rechten worden aan de serverkant gecontroleerd — *Ingericht*

Elke API-aanvraag wordt aan de serverkant gecontroleerd op lidmaatschap van werkruimte, project en rol. Een verborgen knop is dus nooit de grens. Tussen organisaties wordt dit bij elke release automatisch getest.

Aanmelden met Microsoft Entra ID — *Ingericht*

Per organisatie in te schakelen. Medewerkers melden zich aan met het Microsoft-account van uw organisatie via OpenID Connect met PKCE, via onze aanmeldservice auth.zorgpmo.nl. We controleren handtekening, uitgever, doelgroep, geldigheid, nonce en tenant-ID. Alleen uw eigen Entra-tenant en vooraf toegestane e-maildomeinen worden geaccepteerd. We vragen alleen openid, profile en email, bewaren geen Microsoft-tokens en ontvangen geen wachtwoorden. Uw ICT geeft eenmalig beheerderstoestemming en kan via Conditional Access tweestapsverificatie, apparaat- of locatie-eisen afdwingen. Entra bepaalt wie iemand is. Wat iemand in ZorgPMO mag zien, bepalen de rollen in ZorgPMO.

Toegang intrekken — *Ingericht*

De beheerder van de organisatie kan gebruikers direct uit werkruimtes en projecten verwijderen. Met Microsoft-login ingeschakeld blokkeert het uitschakelen of verwijderen van een account in uw Entra-tenant

iedere nieuwe Microsoft-aanmelding. Een lopende sessie eindigt uiterlijk dezelfde nacht. Heeft iemand daarnaast een eigen ZorgPMO-wachtwoord of zijn er API-tokens uitgegeven, verwijder de persoon dan ook in ZorgPMO en trek de tokens in.

Gegevens, versleuteling en locatie

Geen patiëntgegevens — *Ingericht*

Patiëntgegevens, BSN's, gezondheidsgegevens en herleidbare casuïstiek zijn contractueel uitgesloten, ook in bijlagen, notulen en opmerkingen. De app en de activatie tonen deze grens. Een inhoudscontrole zoekt in ondersteunde tekst-, Word- en PDF-bestanden naar duidelijke aanwijzingen, zoals mogelijke BSN's.

Versleuteling tijdens transport — *Ingericht*

Al het verkeer loopt via HTTPS met automatisch aangevraagde en dagelijks gecontroleerde certificaten. Cookies gebruiken waar van toepassing Secure, HttpOnly en SameSite. Uitgaande mail gaat via TLS.

Versleutelde back-ups en wachtwoorden — *Ingericht*

Externe back-ups zijn versleuteld (Restic). Wachtwoorden worden gehasht opgeslagen en specifieke geheimen versleuteld.

Datalocatie — *Ingericht*

Productie draait in een datacenter van DigitalOcean in Amsterdam (AMS3). Versleutelde externe back-ups staan bij DigitalOcean in Frankfurt (FRA1). Beide locaties liggen in de EU. DigitalOcean is een Amerikaans bedrijf. Contract, verwerkersafspraken en doorgiftewaarborgen staan in het leveranciersoverzicht.

Bewijs op aanvraag: Leveranciersoverzicht

Geheimen en sleutels — *Ingericht*

Wachtwoorden en sleutels staan niet in de broncode. Dat wordt bij iedere release gescand. Providerwachtwoorden staan versleuteld in het platformbeheer of in afgeschermde bestanden op de server. Iedere klantomgeving krijgt eigen, beperkte sleutels, bijvoorbeeld een eigen mailsleutel met eigen quotum.

Externe AI en koppelingen — *Ingericht*

AI-functies en externe koppelingen staan standaard uit en worden alleen per organisatie ingeschakeld na afspraak. WeDesignworks gebruikt klantinhoud niet om AI-modellen te trainen.

Back-ups en herstel

Dagelijkse back-ups — *Ingericht*

Iedere nacht (02:35 UTC) wordt per omgeving een kopie gemaakt van database, bestanden en configuratie. Die staat lokaal op de server en versleuteld op een tweede locatie in Frankfurt. Vóór iedere release-uitrol wordt een extra kopie gemaakt.

Bewijs op aanvraag: Back-uprapporten

Herstel uit back-up — *Ingericht*

Herstel uit de externe back-up is getest met een synthetische database en bestandsset. Herstel gebeurt altijd in een nieuwe database, nooit over de bestaande heen. Zo gaan er geen nieuwere gegevens verloren.

Kwetsbaarheden, logging en incidenten

Kwetsbaarhedenbeheer — *Ingericht*

Bij iedere release worden afhankelijkheden en images gescand. Een oplossing voor een kwetsbaarheid gaat als nieuwe release door dezelfde twaalf controles. Kwetsbaarheden kunt u vertrouwelijk melden via info@zorgpmo.nl.

Logging en audit — *Ingericht*

Beveiligingsrelevante verzoekuitkomsten worden vastgelegd met gebruiker, route, methode en status, zonder wachtwoorden, cookies, tokens of volledige inhoud. Alle beheeracties op het platform staan met actor in een auditlog.

Incidentmelding — *Ingericht*

Meld incidenten via info@zorgpmo.nl. Bij een (vermoedelijke) inbreuk op persoonsgegevens informeren we u zonder onredelijke vertraging. Ons uitgangspunt is een eerste melding binnen 24 uur na kennisname, met wat op dat moment bekend is. Zo houdt u tijd over voor uw eigen meldplicht, in beginsel 72 uur richting de Autoriteit Persoonsgegevens. De definitieve afspraak staat in de verwerkersovereenkomst.

Eén vaste verantwoordelijke — *Ingericht*

Niek Boersen is verantwoordelijk voor informatiebeveiliging en het aanspreekpunt bij incidenten. Vervanging en bereikbaarheid buiten kantooruren leggen we per klant vast.

Normen en wetten

AVG. ZorgPMO verwerkt persoonsgegevens van gebruikers en medewerkers, zoals naam, zakelijk e-mailadres, rol en bijdragen aan projecten. Uw organisatie is verwerkingsverantwoordelijke, WeDesignworks verwerker. Een modelverwerkersovereenkomst staat onder Vertrouwen.

DPIA. Of een gegevensbeschermingseffectbeoordeling nodig is, bepaalt uw organisatie. Wij leveren de informatie die u daarvoor nodig hebt.

NEN 7510. Zorgaanbieders moeten aantoonbaar volgens deze norm werken, hun leveranciers beoordelen en beveiligingseisen contractueel vastleggen. Dit dossier is bedoeld als input voor die leveranciersbeoordeling.

ISO 27001. Het platformbeheer bevat registers in de opbouw van een managementsysteem voor informatiebeveiliging: risico’s, toepasselijkheid, leveranciers, incidenten, toegangsreviews en herstelproeven.

OWASP ASVS 5.0 en OWASP Top 10 (2025). Broken Access Control staat in de Top 10 op de eerste plaats. Daarom testen we de scheiding tussen organisaties bij iedere release.

NCSC ICT-beveiligingsrichtlijnen voor webapplicaties. We gebruiken ze naast ASVS bij de technische inrichting.

Cyberbeveiligingswet (Cbw). Sinds 15 augustus 2026 van kracht als Nederlandse uitwerking van NIS2. Ziekenhuizen die eronder vallen, moeten onder meer hun leveranciersrisico’s beheersen. Dit dossier helpt daarbij.

Wat u bij ons kunt opvragen

Releasebewijs voor de versie die bij uw organisatie draait: bouwlog, uitkomst van alle twaalf controles en het ondertekende manifest.

De uitvoer van de cross-tenant-isolatietest en het opleverrapport van de inrichtingscontrole.

Een architectuuroverzicht met componenten en datastromen.

De verwerkersovereenkomst met omgevingsbijlage, het bewaarbeleid en het leveranciersoverzicht.

Back-up- en herstelbewijs van uw omgeving.

Wilt u zelf testen? Een pentest door of namens uw organisatie op een aparte testomgeving is bespreekbaar, na afspraak over scope en tijdvenster. Mail naar info@zorgpmo.nl.

Actuele versie: https://zorgpmo.nl/vertrouwen/ict-beoordeling/