Privacy & beveiliging

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

Technische verklaring. Maatregelen verschillen per release en omgeving.

Doel en verantwoordelijke

ZorgPMO ondersteunt programma’s, projecten en samenwerking. Aanbieder is WeDesignworks, KvK 77708091, gevestigd aan Oranje Vrijbuiterskade 200. Niek Boersen is verantwoordelijk voor informatiebeveiliging en het contact bij incidenten. Contact: info@zorgpmo.nl. Deze verklaring is bedoeld voor gebruikers, ICT-afdelingen en privacyfunctionarissen.

Deze verklaring beschrijft de inrichting en de grenzen daarvan. Zij is geen certificaat, onafhankelijke audit of garantie van volledige naleving van ISO/IEC 27001 of NEN 7510. Een ontwikkelde functie is pas van toepassing op een klantomgeving nadat de betreffende release en configuratie daar zijn gecontroleerd. Vraag bij een beoordeling om de versie en het bewijs voor jouw omgeving.

Geen patiëntgegevens

ZorgPMO is geen elektronisch patiëntendossier. Patiëntnamen, BSN’s, gezondheidsgegevens, herleidbare casuïstiek en medische dossiers mogen niet worden ingevoerd, geüpload, via opmerkingen gedeeld of aan AI aangeboden. Dit geldt ook voor screenshots, notulen, demonstraties, supportvragen en bijlagen. Gebruik fictieve of werkelijk geanonimiseerde procesinformatie. Pseudoniemen kunnen nog steeds persoonsgegevens zijn.

Er kunnen wel bedrijfsgevoelige gegevens worden verwerkt, waaronder budgetten, reorganisatieplannen, besluiten, risicoanalyses en interne documenten. Accountnamen, zakelijke e-mailadressen, rollen en bijdragen zijn persoonsgegevens. De klant bepaalt welke gegevens noodzakelijk zijn en welke gebruikers deze mogen zien.

Identiteit en toegang

Persoonlijke accounts en servercontroles begrenzen toegang tot werkruimten, projecten en onderdelen. Een verborgen knop is niet de autorisatiegrens. Accountbeëindiging en rolwijziging moeten worden opgevolgd met intrekking van lidmaatschappen, sessies en technische toegang.

De beveiligingsuitbreiding beëindigt sessies uiterlijk bij de eerstvolgende middernacht in Europe/Amsterdam en nooit later dan 24 uur na inloggen. Gebruik verlengt die termijn niet. Platformbeheer heeft een kortere sessieduur. Bestaande applicatiesessies moeten bij invoering van het nieuwe beleid opnieuw aanmelden.

Authenticatorcodes en herstelcodes zijn beschikbaar. Een klantomgeving kan via beheer tweestapsverificatie verplicht stellen. De uitbreiding ondersteunt WebAuthn-passkeys met controle van omgeving, challenge, handtekening, aanwezigheid en lokale gebruikersverificatie. Passkeys kunnen als tweede factor na het wachtwoord worden gebruikt. TOTP blijft een herstel-/alternatieve methode en is zelf niet phishingbestendig.

Technische API-tokens zijn aparte toegangsmiddelen. In de uitbreiding geldt maximaal 90 dagen vanaf uitgifte. Een eerdere vervaldatum blijft gelden. Rotatie, intrekking en het beperken van de rechten van het bijbehorende account blijven noodzakelijk. Een API-token krijgt geen extra rechten boven dat account.

Web- en API-beveiliging

De uitbreiding gebruikt een gedeelde CSRF- en herkomstcontrole voor muterende verzoeken met een ingelogde browsersessie. De browser stuurt daarvoor een CSRF-token mee.
Server-naar-serverauthenticatie vereist een eigen toegangsmiddel. Het meesturen van een willekeurige header heft browsercontroles niet op.

Verzoekpieken worden per identiteit begrensd, met afzonderlijke grenzen voor wijzigen en lezen. Overschrijding levert HTTP 429 en een wachttijd op. Invoeromvang en zeer grote JSON-resultaten zijn begrensd. Dit is aanvullend op netwerkbescherming: geen belofte dat iedere DDoS-aanval kan worden opgevangen.

HTTP-cookies gebruiken waar van toepassing Secure, HttpOnly en SameSite. HTTPS beschermt transport. Authenticatie- en API-antwoorden worden niet publiek gecachet. De reverse proxy moet aangeleverde client-IP-headers alleen van vertrouwde infrastructuur accepteren.

Bestanden en inhoudelijke controle

De uitbreiding controleert geüploade bestanden ’s nachts op malware met ClamAV. Er zijn per omgeving twee standen. Nachtelijke controle achteraf, sinds 13 november 2026 actief op de ontwikkelomgeving: nieuwe bestanden zijn direct beschikbaar en worden de eerstvolgende nacht gescand. Bij een malwarevondst of geweigerde inhoud wordt het bestand geblokkeerd. Quarantaine vooraf, de strengere stand: nieuwe of gewijzigde bestanden blijven tot een geslaagde scan geblokkeerd en kunnen dus niet direct worden gedownload of doorgestuurd. Downloadlinks verwijzen dan naar de daadwerkelijk gecontroleerde kopie, zodat een nog geldige uploadlink deze niet achteraf kan vervangen. In klantomgevingen staat de scan nog niet aan. Eerder als onveilig gemarkeerde bestanden blijven in beide standen geblokkeerd.

De aanvullende inhoudscontrole zoekt bij ondersteunde tekst-, Word- en PDF-bestanden naar enkele duidelijke aanwijzingen voor patiëntgegevens, waaronder mogelijke BSN’s. Versleutelde of niet veilig uitleesbare documenten kunnen worden geweigerd. Dit is beperkte preventie en geen volledige DLP, OCR of garantie dat patiëntgegevens worden herkend. De gebruiksgrens blijft onverkort gelden.

De scanlimiet is 32 MB per bestand in de uitbreiding. Een lagere omgevingslimiet blijft leidend. Een schone malwareuitslag bewijst niet dat een document inhoudelijk correct, rechtmatig of vrij van alle onbekende dreigingen is.

De scan start tussen 01:00 en 06:00 Nederlandse tijd, standaard rond 04:00. Virusdefinities worden direct ervoor gedownload in een aparte, kortlevende container. De scanner zelf draait zonder internettoegang, met een vaste geheugenlimiet, en stopt na de nachtjob. Vóór de eerste echte bestanden wordt de engine getest met een EICAR-testbestand. Bij onvoldoende vrij geheugen, definities ouder dan zeven dagen of een scanfout wordt niets als schoon gemarkeerd, krijgt de platformbeheerder een melding en wordt de uitkomst in het platformbeheer vastgelegd. Een geplande taak is op zichzelf geen bewijs dat een bestand gecontroleerd is. Dat bewijs is het nachtrapport per omgeving.

Isolatie, opslag en sleutels

Beheerde omgevingen hebben eigen databases en bestandsopslag. Ontwikkeling en klantreleases hebben gescheiden uitrolroutes. Klantgegevens worden niet automatisch vervangen door een ontwikkeluitrol.

Specifieke geheimen worden versleuteld opgeslagen. Wachtwoorden worden gehasht. Externe Restic-back-ups gebruiken versleuteling. Dit bewijst niet dat alle actieve schijven of databasevelden versleuteld zijn. Opslagversleuteling, sleutelisolatie, herstel van sleutels en providerinstellingen moeten per omgeving met operationeel bewijs worden bevestigd.

Sleutelrotatie wordt als beheerproces geregistreerd: inventarisatie, eigenaar, wijzigingsvenster, overlap, herencryptie waar nodig, verificatie en intrekking. Bestaande encryptiesleutels worden niet blind vervangen: dat kan gegevens onherstelbaar maken.

Beheer, bewijs en controle

Het beheer bevat registers voor ISMS-scope, risico’s en maatregelen, toepasselijkheid, leveranciers, bewaarbeleid, incidenten, toegangsreviews, sleutelbeheer, herstelproeven, interne audit en managementreview. Elk dossier kan een eigenaar, deadline, bewijsreferentie, beoordelaar en vervolgactie krijgen. Wijzigingen worden met actor en eerdere inhoud vastgelegd.

Een status Beoordeeld betekent dat een beoordeling is geregistreerd. Deze bewijst niet automatisch dat de inhoud juist is of de auditor onafhankelijk was. De volledige toepasselijkheidsverklaring moet tegen de geldende norm worden gecontroleerd. Een jaarlijks managementbesluit en een onafhankelijke interne audit kunnen niet door software worden vervangen.

Toegangsreviews worden minimaal per kwartaal en bij relevante personeelswijzigingen gepland. Herstelproeven worden minimaal per kwartaal gepland. Een incidentoefening, interne audit en managementreview worden minimaal jaarlijks gepland. De feitelijke uitvoering, bevindingen en opvolging worden in de dossiers verantwoord.

Logging en incidenten

De uitbreiding registreert beveiligingsrelevante verzoekuitkomsten met actor, route, methode en status. Volledige verzoek- en antwoordinhoud, wachtwoorden, sessiecookies en API-sleutels horen niet in deze logboeken. Logtoegang is beperkt tot noodzakelijk beheer. Verdere centrale detectie en bereikbaarheid worden per dienstverlening afgesproken. Er wordt geen permanent bemand SOC geclaimd.

Meld incidenten vertrouwelijk via info@zorgpmo.nl. De coördinator registreert kennisnametijd, ernst, getroffen omgeving, betrokken gegevens, containment, bewijs, communicatie en herstel. Bij een persoonsgegevensinbreuk informeert de verwerker de klant zonder onredelijke vertraging. De klant beoordeelt de meldplicht aan de AP en betrokkenen. Waar verplicht geldt voor de AP in beginsel 72 uur vanaf kennisname. Die termijn is geen wachttijd voor ZorgPMO.

Continuïteit en bewaarbeleid

Er bestaan lokale herstelkopieën en voorzieningen voor versleutelde externe back-ups. Een geslaagde synthetische herstelproef is geen bewijs van de RPO/RTO van alle klantomgevingen. Per omgeving moeten frequentie, herstelpunten, maximale hersteltijd, locaties en verantwoordelijke worden vastgelegd.

RPO is het maximaal aanvaardbare gegevensverlies in tijd. RTO is de beoogde hersteltijd. Zonder schriftelijk bevestigde omgevingsafspraak wordt geen specifieke waarde of beschikbaarheidsgarantie toegezegd. Bewaartermijnen en verwijdering volgen het aparte bewaarbeleid en de verwerkersafspraken.

Cloudflare en andere dienstverleners

Cloudflare is voorbereid als DNS-/webbeveiligingslaag, maar wordt pas als actief aangemerkt nadat de eigenaar de DNS-overgang heeft uitgevoerd en de configuratie is gecontroleerd. Tijdens voorbereiding verandert de bestaande route niet.

Bij gebruik van de proxy eindigt TLS aan de rand van Cloudflare en wordt een afzonderlijke versleutelde verbinding met het origine gebruikt (Full strict). Cloudflare kan daarbij IP-adressen, technische metadata en doorgestuurde HTTP-inhoud verwerken. Authenticated applicatie- en API-inhoud mag niet via publieke caching worden gedeeld. Cloudflare is geen end-to-endversleuteling waarbij de provider geen inhoud kan zien.

Mail en SSH blijven buiten de gewone HTTP-proxy. DNSSEC, certificaten, mailrecords en herkomstcontroles moeten bij de overgang worden geverifieerd. Providercontracten, internationale verwerking en aanvullende waarborgen staan in het leveranciersregister en moeten vóór gebruik worden beoordeeld.

Actuele versie: https://zorgpmo.nl/vertrouwen/beveiliging/