

PROGRAMMA VAN EISEN

Specificatie van eisen voor het eDepot



INHOUDSOPGAVE

1	Standaard	3
2	Invoer	3
3	Beheer	5
4	Systeem	7
5	Beschikbaar stellen	9
6	Beveiliging	10
7	Leverancier	11

1 Standaard

1.1	Norm	<ul style="list-style-type: none"> • ISO 14721:2012 (OAIS-referentiemodel) • NEN-ISO 27001/27002 • NEN-ISO 15489-1 (2018) • NEN 2082 (2008) • NEN-ISO 23081 (2006) • NEN-ISO 16175 (2010) • NEN 2084 (2015) • ED3 Eisen duurzaam digitaal depot (http://www.lopai.nl/pdf/ED3-v2.pdf) • Westfries Metadatamodel volgens TMLO (WFMM) • Gemma – Procesarchitectuur, Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) (V1.0, 2010) en de StUF-ZKN: Standaard Uitwisselingsformaat sectormodel Zaken (V3.10, 2010) en de StUF zaak- en documentservices (v1.2) • WCAG 2.0 Web Content Accessibility Guidelines
1.2	Wet en regelgeving	Nederlandse Wet- en regelgeving: Archiefwet 1995, Archiefbesluit 1995 en Archiefregeling 2009, Wetten AVG, Wob, Who, Woo en Wet Elektronische handtekening (http://wetten.overheid.nl/BWBR0015046/2003-05-21).

2 Invoer

2.1	Ingest	Gegevensoverdracht geschiedt via een upload naar een ingest-module van het systeem.
2.2	Ingest	Het systeem heeft de mogelijkheid geëncrypteerde informatieobjecten te herkennen en signaleert deze bij ingest.
2.3	Ingest	Het systeem heeft de mogelijkheid geëncrypteerde bestanden te accepteren.
2.4	Ingest	Het systeem kan na handmatige invoer bij het inlezen een SIP maken.
2.5	Ingest	De invoeromgeving laat bij handmatige invoer toe dat informatieobjecten zowel individueel als meervoudig handmatig in te voeren in het systeem.
2.6	Prestatie	Het systeem kent geen beperkingen op niveau van grootte, omvang of aantallen van in te voeren objecten en ondersteunt de gelijktijdige opname van zeer grote hoeveelheden informatieobjecten.
2.7	Opslag	Het systeem heeft een schaalbare opslaginfrastructuur die rekening houdt met digitale duurzaamheid ¹ en een voortdurende volumetoename.
2.8	Metadata	De datering is gecertificeerd en wordt opgeslagen als metadata element voor elk van de onderdelen van een overdracht.

¹ Zoals geformuleerd in de DUTO-eisen voor duurzame toegankelijkheid (<https://wiki.nationaalarchief.nl/pagina/DUTO:Kwaliteitseisen>) en de 'Bewaar- en beheerstrategie (BBS)' voor het Westfries eDepot (juni 2018).

2.9	Metadata	Bij ieder invoer wordt een timestamp opgenomen van het moment van opname in het eDepot samen met de identificatie van de overdragen partij.
2.10	Metadata	Elk informatieobject krijgt vanuit het bedrijfstoepassing een persistent identifier mee.
2.11	Transitie & Quarantaine	Bij het invullen van de metadata kunnen aan verschillende informatieobjecten tegelijk eenzelfde metadata waarde worden toegekend.
2.12	Transitie & Quarantaine	Metadata kan worden toegevoegd of aangepast door de functioneel beheerder.
2.13	Transitie & Quarantaine	Bij bevestiging van de overdracht laadt het systeem de stukken en bestanden met bijhorende beschrijvende gegevens in het doelarchief op.
2.14	Transitie & Quarantaine	Er is transitieomgeving (een digitale samenwerkingsruimte) waar gewerkt kan worden aan het op orde brengen van de vereiste ingest-bestanden met behulp van specifieke tooling die de leverancier ter beschikking stelt.
2.15	Transitie & Quarantaine	In de verwerking van de opname van documenten passeren alle stukken via de transitieomgeving de quarantaine omgeving. Daar wordt gecheckt op malware die kan leiden tot vernietiging of beschadiging van de collectie. (fase A)
2.16	Transitie & Quarantaine	Het systeem beschikt over een geïsoleerde quarantaine omgeving waar externe niet gecontroleerde digitale bronnen kunnen worden gedecontamineerd.
2.17	Transitie & Quarantaine	Het systeem beschikt over een transitieomgeving die door informatiebeheerders gebruikt kan worden voor kwalitatieve controle en correctie zolang er geen sprake is van een automatische koppeling.
2.18	Transitie & Quarantaine	Mogelijkheid voor handmatig starten van upload proces.
2.19	Transitie & Quarantaine	Bij geweigerde invoer biedt de transitieomgeving de mogelijkheid voor evaluatie, foutafhandeling en herstel. Bij upload van informatie worden mappen zonder inhoud geïdentificeerd en gepresenteerd in overzichten.
2.20	Transitie & Quarantaine	Het systeem legt een beheerder een overzicht voor van gefaalde invoer, niet-conforme invoer en van verplichte metadata die niet werd ingevoerd.
2.21	Transitie & Quarantaine	Het is mogelijk aan te geven welke stukken of bestanden voor invoer in het systeem in aanmerking komen.
2.23	Transitie & Quarantaine	De beschreven invoer kan tijdelijk worden opgeslagen tot ze volledig is beschreven.
2.24	Transitie & Quarantaine	De overdragende partij kan de invoer handmatig activeren.
2.25	Transitie & Quarantaine	Het systeem kan dubbelingen detecteren en een lijst daarvan genereren.
2.26	Fase B	Het systeem kan een automatisch invoer proces lopen waarbij bedrijfsapplicaties informatieobjecten plaatsen in het archief op basis van informatiestatus, processtap of ander event, al dan niet periodiek, in de applicatieve omgeving.
2.27	Fase B	Er worden actieve koppelvlakken gerealiseerd voor rechtstreekse gegevensuitwisseling (bevraging en ingest) tussen de bedrijfstoepassingen en het eDepot.
2.28	Fase B	Automatisch ingevoerde stukken aangebracht door bedrijfstoepassingen worden via de quarantaine omgeving direct overgebracht naar de bewaaromgeving.

3 Beheer

3.1	Metadata	Invoermaskers (sjablonen) kunnen worden gedefinieerd.
3.2	Metadata	Een functioneel beheerder kan verplichte of optionele velden configureren: aanpassen, toevoegen, instellen, verplichtstellen, deactiveren, enz.
3.3	Metadata	Het instellen van verplicht of optioneel in te vullen kan verschillen per objecttype (ook wanneer het om hetzelfde veld gaat).
3.4	Metadata	Het is mogelijk dat meerdere waarden voor een metadata veld kunnen worden opgegeven.
3.5	Metadata	Metadata wordt overgeërfd van een hoger niveau, tenzij de functioneel beheerder anders aangeeft.
3.6	Metadata	Het systeem kan onbeperkt een relatie leggen tussen termen, afzonderlijke metadatering en informatie objecten.
3.7	Objecttype	Het systeem laat zonder beperking verschillende objecttypes toe.
3.8	Objecttype	Reeds gecreëerde informatieobjecten houden de definitie die van toepassing was bij hun creatie, maar kunnen naderhand worden aangepast, indien nieuwe objecttypes in werking treden.
3.9	Bewaartermijn	Het systeem kent geen beperking ten aanzien van de bewaartermijnen.
3.10	Bewaartermijn	Vastleggen en wijzigen van een bewaartermijn kan ook handmatig worden uitgevoerd door de functioneel beheerder.
3.11	Bewaartermijn	Bij een termijn kan gerekend worden met alle tijdwaarden in iedere gewenste volgorde.
3.12	Bewaartermijn	Handmatige toekenning van een bewaartermijn heeft prioriteit boven een hiërarchische overerving van een reeds toegekende bewaartermijn.
3.13	Bewaartermijn	De basis voor het opstarten van de berekening van de specifieke bewaartermijn is de datum van afsluiten van een dossier of een nader aan te geven eigenschap.
3.14	Bewaartermijn	Informatieobjecten kunnen zonder ingevulde vernietigingsdatum worden uitgeplaatst.
3.15	Opschorting	De bewaartermijn van een uitgeplaatst informatieobject kan worden aangepast of opgeschort door de functioneel beheerder.
3.16	Opschorting	De functioneel beheerder dient minimaal de volgende gegevens in te voeren bij het opschorten of aanpassen: <ul style="list-style-type: none"> • Datum van invoer van opschorting; • Identiteit van de gemachtigde persoon die de opschorting initieerde; • De reden voor de invoering van de opschorting.
3.17	Opschorting	Wanneer alle opschortingen op een informatieobject zijn opgeheven zet het systeem de uitvoering van de bewaartermijn verder.
3.18	vernietiging	Het systeem genereert periodiek notificaties aan de verantwoordelijke beheerder(s) en het is mogelijk de periodiciteit aan te passen.
3.19	vernietiging	Het systeem produceert leesbare geautomatiseerde overzichtslijsten van

		vernietiging per tenant, welke een onderdeel van de systeem gebruiksomgeving zijn.
3.20	vernietiging	Vernietiging conform de door het systeem gegenereerde vernietigingslijst wordt uitgevoerd na vrijgave door de geautoriseerde beheerder en het fiat van de zorgdrager. Dit fiat wordt opgenomen in de audit trail.
3.21	Rapportage & dashboarding	Het systeem beschikt over een dashboardfunctionaliteit met mogelijkheden voor numerieke en grafische rapportering welke door de functioneel beheerder waar nodig uit te breiden is op basis van alle in het systeem aanwezige variabelen/velden.
3.22	Rapportage & dashboarding	De functioneel beheerder kan zelf datasets bepalen ten behoeve van rapportage.
3.23	Rapportage & dashboarding	Het dashboard beschikt over een drill-downfunctie met de volgende minimale initiële dataset: <ul style="list-style-type: none"> • Volume(s) en groei opslag; • Aantal en groei informatieobjecten op alle aggregatieniveau's; • Aantallen per zorgdrager; • Statusoverzicht volgens bewaringsfase of periode; • Aantal stukken in een specifieke bewaringsfase of periode.
3.24	Rapportage & dashboarding	Het systeem kan een rapport genereren met overzicht van alle in het systeem aanwezige variabelen/velden.
3.25	Rapportage & dashboarding	Detailrapportages over informatieobjecten of gebruikersgroepen zijn beschikbaar en door de functioneel beheerder uit te breiden.
3.26	Rapportage & dashboarding	Detailrapportages over het aantal, de herkomst, het moment, het doel van de raadplegingen en de rol van de raadpleger zijn beschikbaar en door de functioneel beheerder uit te breiden.
3.27	Rapportage & dashboarding	Vanuit het dashboard kan de beheerder minimaal: <ul style="list-style-type: none"> • op basis van een steekproef bestanden openen die door het transformatie proces zijn gegaan (na de automatische consistency check); • de transformatie valideren; • en indien niet gevalideerd, de transformatie van bestanden die gelopen zijn voor de regel opnieuw opstarten; • indien niet gevalideerd, de transformatie voor het betrokken bestand opnieuw opstarten.
3.28	Gebruikers-omgeving	De gebruikersinterface is aanpasbaar door de functioneel beheerder.
3.29	Autorisatie	De functioneel beheerder kan zelfstandig gebruikers, rollen, en beheerders aanmaken.
3.30	inrichting	Het systeem kan worden opgesplitst in sectoren en tenants.
3.31	Continuïteit	Nieuwe deelnemers of tenants kunnen worden toegevoegd en bestaande deelnemers of tenants kunnen worden samengevoegd of verwijderd.
3.32	Privacy & informatiebeveiliging	Het is mogelijk het archief op te delen in verschillende segmenten waarvoor andere beveiligingsregels van toepassing zijn.
3.33	Export & migratie	Het systeem bevat een exportmogelijkheid, waarmee de functioneel beheerder zelfstandig een gedeeltelijke of volledige migratie van de data op alle aggregatieniveau's en/of metadata en/of auditinformatie uit het

		systeem te maken, zonder informatie- of kwaliteitsverlies.
--	--	--

4 Systeem

4.1	Preservatie	Het systeem biedt de garantie en kan aantonen dat vorm, inhoud, structuur en metadata exact hetzelfde blijven zoals bij invoer of na een geautoriseerde wijziging.
4.2	Preservatie	Authentieke bestanden kunnen worden getransformeerd naar gangbare standaardformaten die geldig zijn op het moment van raadpleging.
4.3	Preservatie	Een transformatie of transformatieregel voor preservatie wordt gedefinieerd als een oorspronkelijk bestand, een doel bestand formaat (MIME type) en periode van toepasbaarheid.
4.4	Preservatie	Het systeem accepteert emulatiesoftware.
4.5	Formaten	Het systeem houdt rekening met de verschillende (sub)versies van een bestandsformaat.
4.6	Formaten	Aangeboden raadpleeg software die de informatieobjecten over de tijd raadpleegbaar en bruikbaar moeten houden volgt de ontwikkeling van nieuwe versies of nieuwe software.
4.7	Formaten	Het is mogelijk transformatiemodules en viewing technologie toe te voegen.
4.8	Formaten	Voor elk van de rollen en gebruikersgroepen die het systeem gaan gebruiken wordt aangegeven wat het standaard raadpleegformaat is voor het informatieobject dat getoond wordt.
4.9	Logging	Alle handelingen en acties uitgevoerd door gebruikers van het systeem, beheerders en door het systeem zelf worden gelogd in een audit trail.
4.10	Logging	Logresultaten mogen niet aanpasbaar zijn.
4.11	Logging	Het moet mogelijk zijn om logevents en logvariabelen toe te voegen en te verwijderen.
4.12	Logging	Het systeem bevat functionaliteit die toelaat dat geautoriseerde gebruikers, ook zij met beperkte technische kennis van het systeem, kunnen zoeken naar informatie in de audit trail.
4.13	Logging	De log data heeft dezelfde levensduur als het informatieobject waarop het betrekking heeft.
4.14	Logging	De logging zal de performance van het systeem niet aantasten.
4.15	Logging	De audit trail mag niet te bewerken zijn en is beschikbaar voor directe raadpleging door beheerders.
4.16	Rapportage & dashboarding	Systeemprestaties worden weergegeven in een rapportage.
4.17	Rapportage & dashboarding	Het systeem biedt een dashboard aan voor het ondervragen van de logging gegevens en de audit trail informatie met een verdieping naar detailinformatie op ieder gewenst niveau.

4.18	Rapportage & dashboarding	Er kunnen rapportages vanuit de audit trail worden gegenereerd.
4.19	Performance	De reactiesnelheid van het systeem wordt niet beïnvloed door het aantal actieve gebruikers.
4.20	Performance	Rapportages en schermen worden maximaal binnen 5 seconden gegenereerd.
4.21	Toegankelijkheid	Alleen geregistreerde geautoriseerde gebruikers of systemen hebben toegang tot het systeem voor het niet-openbare/uitgeplaatste deel.
4.22	Toegankelijkheid	Confidentiële informatie moet afgeschermd kunnen worden.
4.23	Toegankelijkheid	Het systeem is alleen te benaderen via de aangewezen diensten (services) en gebruikersinterface(s).
4.24	Toegankelijkheid	Onderliggende opslagcomponenten (database en bestandsopslag) kunnen niet direct benaderd worden zonder de eDepot applicatie.
4.25	Toegankelijkheid	In geval van inbreuk wordt dit direct gesignaleerd, gemeld, getraceerd en worden herstelacties uitgevoerd.
4.26	Toegankelijkheid	Reeds unieke (niet-URI) eigenschappen van een informatieobject kunnen gebruikt worden in de URI als sleutel.
4.27	Toegankelijkheid	Om door te verwijzen van een niet-informatie resource naar een informatie resource kan het systeem gebruik maken van 303-redirects of fragment-identifiers.
4.28	Toegankelijkheid	Het systeem biedt ondersteuning voor content-negotiation voor elke URI met een representatie in HTML(+RDFa) en ten minste één andere gestructureerd formaat.
4.29	Gegevensuitwisseling	Het systeem ondersteunt minimaal onder andere: <ul style="list-style-type: none"> • CMIS v1.0/1.1 • StUF-ZKN 3.10 (Standaard Uitwisseling Formaat voor RGBZ 1.0) • Zaak- en Documentservices v1.0/1.1/1.2
4.30	Gegevensuitwisseling	Het systeem biedt een SPARQL integratie.
4.31	Gegevensuitwisseling	Het systeem biedt gegevens aan via een DCAT protocol.
4.32	Gegevensuitwisseling	Het systeem moet bestaande master data kunnen refereren en synchroniseren.
4.33	Gegevensuitwisseling	Referentie(master)data kan geïntegreerd worden uit bestaande bouwstenen, of uit toekomstige bouwstenen.
4.34	Continuïteit	Het moet mogelijk zijn afzonderlijke, gespecialiseerde onderdelen van het systeem te laten evolueren (upgrade of vervanging) zonder dat het systeem in gevaar komt of vervangen moet worden.
4.35	Continuïteit	Het is mogelijk het onderliggende database management systeem te vervangen zonder enige consequentie voor het eDepot.
4.36	Continuïteit	Het is mogelijk de quarantaine omgeving te vervangen door een ander systeem of andere oplossing.
4.37	Continuïteit	Portabiliteit wordt aantoonbaar gegarandeerd.
4.38	Gebruikers-omgeving	De gebruikersomgeving is in het Nederlands inclusief een online helpfunctionaliteit.
4.39	Fase B	Het is mogelijk om informatieobjecten geautomatiseerd over te dragen via een bedrijfstoepassing.

4.40	Fase B	Het is mogelijk informatieobjecten in het eDepot te raadplegen vanuit bedrijfstoepassingen.
4.41	Fase B	Bedrijfstoepassingen krijgen inzicht in dossier- of activiteit gebonden beheermaatregelen op de informatieobjecten.

5 Beschikbaar stellen

5.1	Raadplegen	Directe bevraging vanuit bedrijfstoepassingen middels actieve koppelingen is voorzien.
5.2	Raadplegen	Raadplegen van informatieobjecten door publiek moet ten minste plaatsvinden door het gebruik het bestaande collectie beheersysteem Mais Flexis.
5.3	Zoeken	Het systeem laat integratie met een (full tekst) indexeringsmechanisme toe voor het raadplegen vanuit de aangesloten deelnemers.
5.4	Zoeken	Op alle in het systeem aanwezige variabelen/velden moet gezocht kunnen worden. Het moet hierbij mogelijk zijn om zoekvragen samen te stellen met alle mogelijke combinaties van variabelen/velden.
5.5	Zoeken	Het moet mogelijk zijn om binnen elk aggregatieniveau te kunnen zoeken, maar ook over alle aggregatieniveaus heen.
5.6	Zoeken	Het systeem biedt per zoekopdracht een filter aan voor aggregatieniveau, metadata of het informatieobject.
5.7	Zoeken	De aangesloten deelnemers hebben een eigen tenant en kunnen niet buiten hun eigen tenant zoeken.
5.8	Gebruikersomgeving	De gebruikersinterface is intuïtief, consistent, relevant, ondersteunend en flexibel.
5.9	Tijdelijke opstelling	In geval van tijdelijke openstelling voor onderzoek kan aan de betrokken partijen voor de looptijd van een procedure toegang verleend worden tot de archiefbestanden die binnen de juridische procedure of het onderzoek worden behandeld.
5.10	Fase B	Raadplegen van de informatieobjecten door deelnemers moet door gebruik van actieve koppelvlakken met de bedrijfstoepassingen kunnen plaatsvinden. Het betreft een vraag/antwoord bericht en deze moet synchroon verlopen.

6 Beveiliging

6.1	Metadata	De volgende verificatiegegevens van een gecertificeerde handtekening worden meegenomen als metadata: <ul style="list-style-type: none"> • Certificatie server. • Titularis van de handtekening. • Moment van handtekening.
6.2	Privacy & informatiebeveiliging	De leverancier stemt in met de verwerkersovereenkomst welke door het WFA is opgesteld.
6.3	Privacy & informatiebeveiliging	De leverancier stemt in met de GIBIT-inkoopvoorwaarden.
6.4	Privacy & informatiebeveiliging	HTTPS (HTTP/TLS1.2) wordt afgedwongen.
6.5	Privacy & informatiebeveiliging	Het systeem ondersteunt Identity and Access Management zoals 2-factor authenticatie, RBAC en beschikt over aantoonbare A certificaten, IPv4, IPv6 en DNSSEC.
6.6	Privacy & informatiebeveiliging	Overdracht kan plaatsvinden via sFTP.
6.7	Privacy & informatiebeveiliging	VPN moet kunnen worden ingericht.
6.8	Privacy & informatiebeveiliging	Verbinding via Digitnetwerk (in combinatie met Digikoppeling) is mogelijk.
6.9	Privacy & informatiebeveiliging	In functie van rol en/of groep worden permissies op informatie objecten toegekend.
6.10	Privacy & informatiebeveiliging	In functie van rol en/of groep worden permissies op functionaliteit van het systeem toegekend.
6.11	Privacy & informatiebeveiliging	Het is mogelijk supplementaire malwarescanners toe te voegen.
6.12	Privacy & informatiebeveiliging	Alle inkomende en uitgaande datastromen met het eDepot dienen via een beveiligde verbinding te verlopen.
6.13	Continuïteit	Het systeem garandeert dat data die opgenomen wordt rond beheersprocessen in het archief steeds correct worden opgenomen en continue kunnen worden gegarandeerd, ook bij heropstart na uitvallen van het systeem of van delen ervan.
6.14	Continuïteit	Disaster Recovery Policy en back-up procedure zijn gegarandeerd, uitgewerkt en sluiten aan op de infrastructuur van de deelnemende organisaties.
6.15	Continuïteit	Potentiële malware op de gebruikersomgeving van de raadpleger mag het archief dat het benadert niet in gevaar brengen.
6.16	Continuïteit	Er is aanwijsbare continue monitoring op de firewall ten einde ongeautoriseerde toegang of onbekende patronen te kunnen ontdekken en hier adequaat op te kunnen reageren. SIEM-oplossing strekt tot de aanbeveling.
6.17	Continuïteit	Het is mogelijk de malware scanning infrastructuur voor de quarantaine omgeving te vervangen.

7 Leverancier

7.1	Implementatie	Er wordt een correct werkend en duurzame productie- en een acceptatieomgeving opgeleverd. Elk van de omgevingen werkt onafhankelijk in het traject van de implementatie. Het is mogelijk instellingen en inrichting tussen de omgevingen door te geven of te promoten.
7.2	Projectplan	De leverancier beschrijft het projectplan binnen 2 weken na opdrachtverlening met ten minste de volgende onderdelen: <ul style="list-style-type: none"> • Planning en tijdspad; • De basisvoorziening eDepot wordt uiterlijk binnen 4 maanden na de definitieve gunning van de overeenkomst opgeleverd; • Activiteiten per fasering; • Resultaten voor de implementatie van het systeem; • Rollen, taken en verantwoordelijkheden; • Invulling beheerorganisatie; • Projectorganisatie; • Projectmethodiek; • Training en opleiding; • Doelarchitectuur en ontwerp eindproduct waarbij rekening wordt gehouden met de in het architectuurmodel aangegeven vereiste eigenschappen van het systeem en de aangegeven infrastructuur van de regio Westfriesland..
7.3	Opleiding	De leverancier stelt een plan op binnen 4 weken na opdrachtverlening voor training en opleiding waarbij ten minste wordt benoemd: <ul style="list-style-type: none"> • Benodigde voorbereiding door de beheerorganisatie; • Door de leverancier beschikbaar gestelde opleidingsmaterialen; • Omschrijving van de opleiders; • Benodigde uren en frequentie; • Leerdoelen; • Voorwaarden op leslocatie (Westfries Archief); • Samenwerking met Westfriesland Academie; • Opzet van de lesinhoud; • Leerdoelen.
7.4	Evaluatie	Voor elk van de te implementeren onderdelen / deelprojecten wordt er wekelijks een rapportage van de voortgang en aan het einde een evaluatie document aangeleverd.
7.5	Documentatie	De leverancier zal een overzicht van de systeemarchitectuur, inclusief het datamodel aanleveren.
7.6	Diensten	De leverancier voert werkings- en functionele testen en begeleidt tijdens acceptatietesten.
7.7	Diensten	De door de leverancier geleverde projectmedewerkers zijn Nederlandstalig.