Memo

Technolution

Technolution B.V.
Burg. Jamessingel 1
P.O. Box 2013
2800 BD Gouda
The Netherlands

T +31 (0)182 59 40 00
E info@technolution.com
I www.technolution.com

Aan: DSH

Van: Technolution

Onderwerp: Niet functionele eisen

Datum: 21-3-2025

Classificatie: Technolution vertrouwelijk

1. Non-functionele eisen

Op basis van ISO25010:2023

1.1. Performance efficiency

1.1.1. Time behavior

Responstijd voor kritieke acties < 2 sec, verwerking zichtbaar binnen 5 sec.

1.1.2. Resource utilization

Geen harde eisen, wordt gestuurd op basis van hosting kosten. Dit kan door de maandelijkse kosten onderdeel te laten zijn van de aanbesteding en hier een gunningscriteria van te maken.

1.1.3. Capacity

Ondersteuning voor maximaal 100 gelijktijdige gebruikers, uitbreiding moet wel mogelijk zijn.

1.2. Compatibility

Technisch beheer door leverancier inclusief hosting en financieel management. Onder voorbehoud eigenaarschap code en data: dit regelen via exit plan (waarbij code, inrichting omgeving, laatste versie data backup ter beschikking zijn). Exit plan regulier te oefenen.

1.2.1. Co-existence

Delivery en deployment in de vorm van Docker containers, autoscaling en load balancing zijn optioneel.

1.2.2. Interoperability

API’s worden standaard geïmplementeerd op basis van REST met json als bestandsformaat.

1.3. Reliability

1.3.1. Faultlessness

Data integriteit en vertrouwelijkheid zijn belangrijk en moeten betrouwbaar zijn.
Testrapport bij elke oplevering vereist. User acceptance door DSH.
Minimaal 80% test coverage (automatische tests), handmatige tests voor de resterende functionaliteiten (regressie van belangrijke functies).

1.3.2. Availability
Uptime van 98% per maand, hersteltijd maximaal 4 uur binnen kantooruren (ma-vr, 09:00-17:00)

1.3.3. Fault tolerance
Automatische herstart bij storingen mogelijk, geen automatische failover.

1.3.4. Recoverability
Hersteltijd (RTO): Systeemherstel binnen 4 uur.
Max. dataverlies (RPO): Maximaal 1 uur, back-ups elk uur, incrementele updates elke 10 minuten.
Back-ups: Elk uur, bewaard voor 30 dagen. Elke dag redundante opslag in een DSH account (voor exit plan, in de vorm van een csv export op basis van 'Landelijk data formaat'.

1.4. Security

2.1.1. Confidentiality & Authenticity
Multi-Factor Authentication (MFA) verplicht, AES-256 encryptie voor opslag en TLS 1.3 voor transport.
Niveau van beveiliging te onderhouden conform marktstandaarden en overheidsadviezen (waaronder NCSC).

1.4.1. Integrity
Basisvalidaties op inkomende data, logging van wijzigingen, geen directe (handmatige) toegang tot de database toegestaan.

2.1.2. Non-repudiation & Accountability
Logging van kritieke wijzigingen (wijziging van rechten) en acties (logins, data invoer, data uitvoer).
Logmeldingen moeten herleidbaar zijn tot specifieke accounts.
Logs bewaard voor een 1 jaar.

1.4.2. Resistance
Basis WAF en DDoS-bescherming via cloudprovider, handmatige mitigatiestrategieën.

1.5. Maintainability
Minimaal 3,5 sterren in SIG-analyse of vergelijkbaar, code voldoet aan CLEAN CODE principes en is goed gedocumenteerd.

1.6. Flexibility

1.6.1. Adaptability
Basisconfiguratie mogelijk via instellingen, wijzigingen via code-aanpassingen en handmatige implementaties.

1.6.2. Scalability
Handmatige schaalvergroting mogelijk, maar niet volledig automatisch.

1.6.3. Installability

Installatie via automatische setup-scripts en/of ondersteuning voor CI/CD-deployments. Mogelijke downtime moet vooraf worden aangekondigd en moet voldoen aan beschikbaarheidseisen (zie 1.3.2). Roll-back moet altijd mogelijk zijn.

1.6.4. Replaceability

Cloudagnostische architectuur en infrastructuur scripts (bijv. middels Terraform of OpenTofu), data-export mogelijkheid volgens het ‘landelijk dataformat’. Zie ook 1.3.4.

2. Service Level Agreement (SLA) – Beheer en Onderhoud

2.1. Beschikbaarheid & Uptime
Zie 1.3.2

2.2. Incidentbeheer & Hersteltijden (RTO & RPO)
Zie 1.3.4

2.3. Monitoring & Logging
24/7 monitoring met automatische alerts, monitoring logs minimaal 30 dagen bewaard.

2.4. Beveiliging & Patching
Maandelijkse updates en security-patches binnen 7 dagen.

2.5. Back-ups & Dataherstel
Zie 1.3.4

2.6. Ondersteuning & Servicevenster
1e lijns helpdesk voor eindgebruikers (Industrie partijen en netbeheerders) wordt door DSH zelf ingevuld.
2e lijns helpdesk door leverancier, hiervoor gelden onderstaande eisen. Kantooruren (ma-vr 09:00-17:00) support, reactietijd van 8 uur, 1 uur bij (mogelijke) security incidenten.

2.7. Wijzigingsbeheer & Releases
Zie 1.6.3

2.8. Continuïteitsbeheer
De leverancier moet een exitplan opstellen en onderhouden.

Memo

3. Service Level Agreement (SLA) – Ontwikkeling en Change Management

3.1. Doorlooptijd van Changes

Nieuwe features binnen 8 weken, fixes voor security issues binnen 24 uur. Fixes voor blokkerende bugs 3 wekdagen, overige bugfixes binnen 4 weken.

3.2. Codekwaliteit & Reviewproces

Zie 1.3.1 en 1.5

3.3. Test- en Validatieproces

Zie 1.3.1

3.4. Change Management & Releasebeleid

Zie 1.6.3

3.5. Documentatie & Kennisbeheer

Per release worden onderstaande documenten opgeleverd waarvan de inhoud overeenkomt met de genoemde J-STD-016-1995 document(en):

Ontwerp:

- **System/Subsystem Design Description** (SSDD) - Het ontwerp van het systeem
- **Interface Design Description** (IDD) - Het ontwerp van één of meer interfaces
- **Database Design Description** (DBDD) - Het ontwerp van de database

Testplan:

- **Software Test Plan** (STP) - Een plan voor het uitvoeren van het kwalificerend testen
- **Software Test Description** (STD) - Test cases/procedures voor de kwalificerende testen

Testrapport:

- **Software Test Report** (STR) - De testresultaten van het kwalificerende testen

Release notes:

- **Software Version Description** (SVD) - Een lijst van opgeleverde bestanden en gerelateerde informatie

De documenten worden via een formeel traject goed gekeurd door de opdrachtgever en er vindt versie en wijzigingsbeheer plaats. De documenten zijn altijd opvraagbaar door opdrachtgever.

3.6. Security in Ontwikkeling

Regelmatige pentesten door externe partij (te organiseren door DSH, leverancier verleent medewerking). OWASP checks in bouwstraat (rapportages beschikbaar op aanvraag).

Memo

4. Overige Contractuele Afspraken met Leverancier

4.1. Aansprakelijkheid en Verzekeringen

Wie is verantwoordelijk bij schade of fouten in de dienstverlening?

Beperkingen van aansprakelijkheid: Tot welk bedrag is de leverancier aansprakelijk bij schade? Bijvoorbeeld een limiet per incident of per jaar.
Uitsluitingen: Situaties waarin de leverancier niet aansprakelijk wordt gehouden (bijv. overmacht, externe cyberaanvallen).
Verzekeringen: Leverancier moet een bedrijfsaansprakelijkheidsverzekering en eventueel een cyberverzekering hebben.

4.2. Intellectueel Eigendom (IE) en Gebruiksrechten

Wie bezit de rechten op de software en data?

Eigendom van ontwikkelde software: Blijft het eigendom bij de leverancier of wordt het overgedragen aan de klant?
Licenties: Gebruiksrechten van de software (bijvoorbeeld exclusief of niet-exclusief, onbeperkt of met beperkingen).
Broncode toegang: Toegang tot broncode bij beëindiging contract of bij faillissement leverancier (escrow-regeling).
Gebruik van open-source componenten: Welke licenties gelden en wie is verantwoordelijk voor naleving?

4.3. Geheimhouding en Gegevensbescherming (AVG/GDPR)

Hoe wordt omgegaan met vertrouwelijke informatie en persoonsgegevens?

Non-disclosure agreement (NDA): Leverancier mag geen bedrijfs- of klantgegevens delen met derden.
Verwerking van persoonsgegevens: Leverancier moet voldoen aan de AVG (bijv. verwerkersovereenkomst).
Locatie van data-opslag: Is data-opslag binnen de EU verplicht of mogen er externe datacenters worden gebruikt?
Datalekprocedure: Wat gebeurt er bij een datalek? Binnen hoeveel tijd moet het worden gemeld?

4.4. Exitstrategie en Overdracht

Wat gebeurt er als het contract eindigt?

Overdracht van data en software: In welk format en binnen welke termijn moet data worden overgedragen?
Overdracht van documentatie en kennis: Moet de leverancier zorgen voor overdracht aan een opvolgende partij?
Ondersteuning na beëindiging: Mag de klant nog tijdelijke support ontvangen na contractbeëindiging?

Memo

4.5. Prijsmodellen en Facturering

Welke kostenstructuur wordt gehanteerd?

Vaste prijs vs. Urenbasis: Werkt de leverancier met een vaste prijs of een uurtarief?
Meerwerkafspraken: Hoe wordt omgegaan met extra werk buiten de oorspronkelijke scope?
Betaaltermijnen: Binnen hoeveel dagen moet een factuur worden betaald?
Indexering van tarieven: Worden prijzen jaarlijks verhoogd? Op basis waarvan?

4.6. Contractduur en Opzegvoorwaarden

Hoe lang loopt het contract en hoe kan het beëindigd worden?

Looptijd van het contract: Bijvoorbeeld 1, 3 of 5 jaar, met automatische verlenging of niet.
Opzegtermijn: Hoeveel maanden van tevoren moet een contract worden opgezegd?
Redenen voor ontbinding: Onder welke omstandigheden kan het contract direct worden beëindigd (bijv. wanprestatie, faillissement)?

4.7. Escalatie- en Conflictmanagement

Hoe worden geschillen tussen partijen opgelost?

Escalatieprocedure: Stappenplan bij problemen, inclusief verantwoordelijke contactpersonen.
Mediation of arbitrage: Moet een onafhankelijk orgaan conflicten beslechten vóór juridische stappen?
Rechtskeuze en bevoegde rechtbank: Welk land en welke rechtbank is bevoegd bij juridische geschillen?

4.8. Compliance en Certificeringen

Welke normen en certificeringen moet de leverancier naleven?

ISO 27001 (informatiebeveiliging)
ISO 9001 (kwaliteitsmanagement).
SOC 2 Type II voor cloud-diensten en beveiliging.
AVG/GDPR-naleving bij verwerking van persoonsgegevens.
Overheidseisen (bijv. BIO-standaarden als het om publieke instellingen gaat).
ISO14001 (milieu)
CO_2-prestatieladder