Programma van Eisen - Architectuur & ICT

1. Informatielaag

1.1	De operationele informatie (weegbonnen, routelijsten, planningen, opdrachten, etc) moeten kunnen worden ontsloten vanuit de applicatie zelf.
1.2	De data moet beschikbaar kunnen worden gesteld aan het BI-tool van Cyclus (Qliksense) om zodoende eenduidig interpreteerbare en consistentie informatievoorziening te faciliteren aan de organisatie.

2. Applicatielaag

2.1	De gebruikersinterface moet Nederlandstalig zijn.
2.2	De toepassing dient (op alle relevante niveaus) adequaat gedocumenteerd te zijn. Documentatie voor eindgebruikers van de toepassing dient in ieder geval Nederlandstalig beschikbaar te zijn. De overige documentatie is tenminste Engelstalig.
2.3	De handelingen die worden uitgevoerd in de applicatie moeten gelogd en via een transparant audit trail herleid kunnen worden.
2.4	Cyclus kan in de applicatie de taken, bevoegdheden en verantwoordelijkheden beleggen, door middel van gebruikersgroepen en de daarbij behorende autorisatie toewijzen.
2.5	Cyclus wenst geen maatwerk of onbeheersbare processen en protocollen voor uitzonderingen en incidentele activiteiten.
2.6	Het eigenaarschap van de data behoort toe aan Cyclus.
2.7	Gebruik van de applicatie is ergonomisch verantwoord (beperkt muisgebruik, optische schermen etc)
2.8	Cyclus wil geen ontwikkelpartner zijn van nieuwe software of nieuwe technieken (innovator), maar wil wel voorin het peloton rijden bij het toepasbaar maken van technieken die door het eerste stadium succesvol gekomen zijn (vulgraad, inwonerportalen, etc.)
2.9	Voor de aan de SaaS dienst onderliggende hardware en software wordt gebruikt gemaakt van gangbare producten, programmeertalen en diensten, zodat uw dienstverlening overdraagbaar, veilig en beheersbaar blijft. Op verzoek is voor Cyclus gedetailleerd inzicht in de technische - en securityarchitectuur van de aangeboden dienst beschikbaar.
2.10	In het (datacenter) netwerk van SaaS leverancier wordt zonering toegepast om omgevingen (klanten, productie, test, etc.) van elkaar te scheiden.
2.11	Er wordt voorzien in de mogelijkheid om toegang tot de applicatie primair vanaf het netwerk van Cyclus toe te staan én buiten het Cyclus netwerk dmv MFA af te dwingen.
2.12	Het uitgeven van de juiste rechten aan useraccounts gebeurt automatisch dmv het SCIM protocol. Cyclus gebruikt Microsoft Azure AD.
2.13	De kleurstelling van het systeem is overal gelijk en rustig voor de ogen. Uitzondering zijn zaken die aandacht nodig hebben van de gebruiker
2.14	De applicatie neemt in specifieke situaties de gebruiker mee in het oplossen van conflicten in het systeem
2.15	De systeemstatus is na een handeling altijd zichtbaar voor de gebruiker
2.16	Schaalbaarheid is mogelijk voor kleinere schermen of grote letters tbv slechtziende collega's of mobiele devices

3. Berichten en gegevens

3.1	De behandeling van informatieobjecten binnen processen is zodanig dat dit authentieke, integere, vindbare, raadpleegbare en interpreteerbare informatie binnen een organisatie garandeert.
3.2	Voor alle gegevenssets wordt bepaald of het gaat om proces specifieke informatie of te delen informatie. Gaat het om te delen informatie dan worden hiervoor standaarden afgesproken. Het gebruik van deze standaarden is verplicht. (vb Stosag)
3.3	Voor de duurzaamheid en toegankelijkheid van gegevens dient gebruik gemaakt worden van open standaarden.
3.4	Elk informatieobject kent een volledige beschrijving van inhoud en kolom definitie
3.5	Ten behoeve van authenticiteit zijn informatieobjecten onlosmakelijk voorzien van een unieke identificatie, het tijdstip van creatie/ontvangst/verzending en de auteur/bron. Dit vindt geautomatiseerd plaats.
3.6	Uw applicatie logt alle wijzigingen per gebruiker tot minimaal 6 maanden. Daarnaast wordt de laatste mutatie van een veld oneindig bewaard en pas overschreven bij een nieuwe mutatie.

3.7	De digitale weegbonnen in uw applicatie voldoen aan de wettelijke regels van archivering en worden automatisch minimaal 7 jaar bewaard.
3.8	Het systeem waarborgt de integriteit en volledigheid van de gegevens en transacties bij het beëindigen of (ongewild) afbreken van gebruikerssessies.

4. Privacy

4.1	Het gebruik van cookies of pixeltrackers is niet toegestaan. Google analytics mag niet worden gebruikt (ook niet met privacy-vriendelijke instellingen).
4.2	De oplossing biedt de mogelijkheid om vertrouwelijkheidscategorieën in te richten. Toegang tot functies en schermen is gekoppeld aan een rol. Gebruikers worden aan één of meerdere rollen gekoppeld. Op rol-niveau kan per vertrouwelijkheidscategorie de standaard autorisaties ingericht worden voor zaken/processen.
4.3	Autorisaties kunnen door een beheerinterface eenvoudig worden geconfigureerd. Het hele rollen- en rechtenmodel binnen de oplossing kan op één plek geconfigureerd worden.
4.4	Per gebruiker (accountnaam) dient gelogd te worden welke (persoons-)gegevens zijn bevraagd, zodat er voldaan kan worden aan de AVG richtlijnen.
4.5	Data Protection Impact Assessment (DPIA) op basis van de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) classificatie vindt plaats in combinatie met een privacytoets in het kader van de Algemene Verordening Gegevensbescherming (AVG)

5. Informatiebeveiliging

5.1	Toegang tot de werkplek betekent tot alle applicaties die de gebruiker nodig heeft (via SSO!). Een gebruiker logt maar 1 keer in.
5.2	Encryptie van data en het uitvoeren van penetratietesten (pentest) zijn een standaard onderdeel van de informatiebeveiliging architectuur principes.
5.3	E-herkenning is de wijze waarop Cyclus beveiligd communiceert met instanties (zoals het Landelijk Meldpunt Afvalstoffen).
5.4	Cyclus koppelt met andere softwaresystemen (zowel intern als extern) op basis van webservices. Het uitwisselen van bestanden (txt, csv en xls) is niet wenselijk.
5.5	ISO27001 : Het betreft hier een principe uitgangspunt. Het gaat niet specifiek om de certificering maar om het feit dat de leverancier informatiebeveiliging actief onder de aandacht heeft. Op basis van de verklaring van toepasselijkheid van de leveranciers beoordeelt Cyclus dit.
5.6	Als uitgangspunt geldt dat alle gegevens binnen de Europese Economische Ruimte (EER) opgeslagen worden.
5.7	Logbestanden van gebeurtenissen die gebruiksactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Een logregel bevat minimaal: - de gebeurtenis; - de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; - het gebruikte apparaat; - het resultaat van de handeling; - datum en tijdstip van de gebeurtenis
5.8	Gebruikers mogen géén mogelijkheid hebben om hun wachtwoord op te slaan, dit zodat zij altijd hun wachtwoord moeten intypen waardoor de veiligheid wordt verhoogd (tenzij SSO via AzureAD).
5.9	Foutieve inlogpogingen moeten worden gelogd met datum, tijdstip, ingevoerde gebruikersnaam en ip-adres zodat er bevestigd kan worden dat iemands account is geblokkeerd door te veel foutieve inlogpogingen en waar de inlogpogingen hebben plaatsgevonden

6. Techniek

6.1	Software dient te voldoen aan de laatste of voorlaatste versie en ondersteund te zijn door de leverancier. Hardware dient vervangen te worden als de gewenste dienstverlening vervanging vereist.

6.2 Software dient geautomatiseerd voorzien te kunnen worden van een licentie. Software die per individueel werkstation voorzien moet worden van een unieke licentie (bijvoorbeeld door middel van e-mail of een internet verbinding) is niet toegestaan. Software voor gebruik in combinatie met flexwerken mag niet worden gelicenseerd op basis van het aantal apparaten dat toegang geeft tot deze software.

6.3 Voor browser gebaseerde applicaties geldt dat er geen gebruik gemaakt mag worden van plugins. Gangbare browsers moeten worden ondersteund.

6.4 Koppelingen tussen applicaties moeten gebaseerd zijn op open standaarden. Applicaties mogen niet afhankelijk zijn van het gebruik van andere applicaties, tenzij hiervoor open standaarden worden gebruikt.

6.5 Voor toegang tot applicaties buiten Active Directory om is two factor authentication (twee-factor-authenticatie) vereist.

7. Koppelingen

7.1 De leverancier levert de volgende koppelingen inclusief documentatie op, op basis van de relevante standaard voor de volgende systemen:

7.2 Tbv Basis- en kerngegevens
- BAG gegevens via postcodetabel.nl
- V-Consyst (Dynamics) voor ledigingsgegevens en black list
- Ortec OWS
- XL Waste
- Exact (import)

7.3 Tbv authenticatie
- Microsoft (Azure) Active Directory tbv Single Sign On;
- eHerkenning

7.4 Domeinspecifiek
- STOSAG
- EBA

7.5 Uw applicatie voorziet standaard in functionaliteit om weeggegevens, handmatig gestart of automatisch in batch, in te lezen Gedurende de contractperiode kunnen tevens automatische koppelingen worden gemaakt met de individuele weegbruggen.

8. Leveranciers management

8.1 Afspraken over beschikbaarheid, incidentafhandeling en wijzigingsprocedures worden vastgelegd in een SLA (Service Level Agreement) en een DAP (Dossier Afspraken en Procedures).

8.2 De kosten van nieuwe major en minor releases, updates, patches, fixes (et cetera) en installatie daarvan zijn opgenomen in de aanbieding. Hieronder tevens inbegrepen wijzigingen naar aanleiding van wetswijzigingen. De regelmatige verversing van de Testomgeving is inbegrepen in de aanbieding.

8.3 In het geval van het plotseling wegvallen van of een onvoorziene beëindiging van de dienstverlening door de leverancier, wordt de continuïteit van de oplossing en dienstverlening gegarandeerd door een derde partij (data-escrow, of een andere vorm van garantstelling zoals een beheerstichting of een tri-partite overeenkomst).

8.4 Leverancier verzorgt (na-)scholing bij veranderingen in haar diensten en/of producten, bijvoorbeeld bij grote veranderingen in releases en/of updates.

8.5 Ondersteuning en onderhoud wordt voor contractperiode verleend op tenminste de laatste en voorlaatste door de opdrachtgever geaccepteerde versie van de software.

8.6 De leverancier zorgt voor een volledige implementatie op de test- en productieomgeving (inclusief interfaces met andere producten/software) van de aangeboden ICT-oplossing.

8.7 Alle noodzakelijke medewerking zal worden verleend voor de uitvoering van (wettelijk verplichte) audits

8.8 Leverancier geeft inzicht in opgetreden beveiligingsincidenten. Beveiligingsincidenten zijn incidenten die inbreuk maken op beveiligingseisen betreffende de beschikbaarheid, integriteit en vertrouwelijkheid. De beveiligingsincidenten worden direct gemeld bij de daarvoor aangewezen contactpersoon van de opdrachtgever

9. Rapportage

9.1	Zowel de stamdata al de transactionele gegevens zijn ten allen tijde en zonder belemmering toegankelijk voor BI doeleinden
9.2	Er wordt minstens 2x dag een geautomatiseerde backup van de database gemaakt worden en ter beschikking gesteld voor BI-raadpleging
9.3	Reeds bij de inschrijving is inzicht te verkrijgen in de binnen de applicatie beschikbare standaard rapportages
9.4	Er is op voorhand inzicht in de rapportage omgeving, of deze een gescheiden rapportage omgeving betreft of zich rechtstreeks op productie bevindt
9.5	Er wordt gerapporteerd op 'harde data', ipv op onderliggende formules of berekende velden
9.6	De oplossing biedt de mogelijkheid om binnen de applicatie, zelf rapportages te ontwikkelen

10. Functioneel beheer

10.1	De applicatie wordt minimaal een keer per dag geback-upt en data kan op verzoek van opdrachtgever middels een door de leverancier beschreven standaard procedure worden teruggezet.
10.2	Uw applicatie moet kunnen omgaan met diakrieten.
10.3	Foutmeldingen die uw applicatie weergeeft, dienen in begrijpelijke taal aan te geven wat de reden van de foutmelding is en wat van de gebruikers verwacht wordt om het probleem op te lossen.
10.4	Er dient bij implementatie een overdracht te zijn bestaande uit minimaal een uitgebreide werkinstructie en handleidingen eventueel aangevuld met gebruiker specifieke trainingen.
10.5	Technisch beheer van de applicatie ligt bij de opdrachtnemer; hieronder valt ook het realiseren van updates en proactief onderhoud van de applicatie.
10.6	Functioneel beheer ligt vanaf de start van het gebruik van de oplossing bij de opdrachtgever
10.7	Automatisch updaten van de software gebeurt buiten werktijden

11. Exit plan

11.1	Na het einde van de overeenkomst krijgt de Opdrachtgever aansluitend minimaal 3 maanden tijd om met behulp van de hier aangeboden oplossing de administratie af te sluiten.
11.2	De leverancier stelt tijdig alle data inclusief documenten beschikbaar voor verder gebruik, al dan niet in een nieuwe oplossing. Leverancier stelt hier geen verdere eisen aan en brengt geen extra kosten (behoudens de genoemde kosten in deze aanbesteding) in rekening voor het beschikbaar stellen van bovengenoemde data aan opdrachtgever.
11.3	De leverancier maakt een exitplan die beschrijft hoe de exit-fase uitgevoerd gaat worden. Goedkeuring van exitplan door Opdrachtgever is voorwaardelijk voor de acceptatie.