Bijlage B - Programma van eisen

Uitleg Programma van eisen voor de inschrijvers:
- U dient kennis te nemen van de gestelde eisen van deze bijlage. Door inschrijving gaat u akkoord met de gestelde eisen.
  Deze bijlage wordt niet voor akkoord ondertekend.
- Als u niet akkoord gaat met één van de eisen, wordt u uitgesloten van verdere deelname aan de aanbestedingsprocedure.
- Voor verzoeken tot wijzigingen van de gestelde eisen kunt u een vraag stellen voor de nota van inlichtingen.

Eisen

Nummer	Onderwerp	Omschrijving
Algemene eisen		
EA001	Wet- en regelgeving	Opdrachtnemer garandeert dat de volledige Oplossing voldoet aan geldende nationale- en internationale wet- en regelgeving, standaarden voor koppelingen en archiefafspraken.
EA002	Bewezen applicatie	De te leveren oplossing is een bewezen applicatie en heeft voor de WIJ geen ontwikkelaanpassingen benodigd groter dan €10.000,- om volgens eisen te kunnen werken (standaardoplossing). Met ontwikkelkosten wordt bedoeld, alle 'te coderen' / ontwikkelen software.
EA003	SaaS-oplossing	De volledige oplossing wordt geleverd als SaaS-oplossing inclusief noodzakelijke en beveiligde verbindingen.
EA004	Front- en BackOffice	De oplossing biedt zowel een FrontOffice oplossing (toegankelijk op mobiel Telefoon en/of Ipad) en een BackOffice oplossing voor analysedoeleinden en ondersteuning van het werkproces.
EA005	Informatiearchitectuur en technisch ontwerp	Opdrachtnemer levert, na definitieve gunning en voor de start van het implementatietraject, een informatiearchitectuur en technisch ontwerp in Archimate of Visio voor de nieuwe situatie waarin de voorzieningen, alle koppelvlakken met andere applicaties en programma van eisen, wensen en vragen aanbestedingen, afhankelijkheden met andere informatievoorzieningen in kaart zijn gebracht en beschreven. Ook de beveiliging van elk koppelvlak moet hierin mee worden genomen. Uitgangspunt is om gebruik te maken van Koppelingen op basis van webservices.
EA006	Deadline implementatie	Opdrachtnemer dient de oplossing uiterlijk in Q4 2025 volledig te hebben geïmplementeerd bij WIJ Groningen, met als startdatum van het implementatieproject uiterlijk Q3 2025. In het geval dat deze termijn niet haalbaar blijkt te zijn, treden partijen hierover tijdig in overleg.
EA007	Testomgeving	Opdrachtnemer stelt tijdens de implementatieperiode kosteloos een testomgeving ter beschikking waarin het proces geaccepteerd wordt. Deze testomgeving is enkel voor op Opdrachtgever en dient te voorzien in alle relevante koppelingen. Alle data in deze testomgeving is fictief. De testomgeving moet gelijk zijn aan de productie.
EA008	Saas aansluitvoorwaarden	Door het inschrijven op deze aanbesteding verklaart Opdrachtnemer te voldoen aan de eisen uit Bijlage L - Saas aansluitingsvoorwaarden. Daarbij geldt de tekst die binnen de kolom “Implementatie” is genoemd als eisen.
EA009	Gestanddoening	Alle door Opdrachtnemer in het kader van deze aanbesteding overgelegde gegevens en gedane verklaringen zijn door Opdrachtnemer naar waarheid ingevuld en kunnen te allen tijde gestand worden gedaan.
EA010	Schadevergoeding	Opdrachtgever behoudt zich het recht op schadevergoeding voor, in het geval van onjuiste en/of onvolledige informatie en/of het niet kunnen nakomen van wat door Opdrachtnemer is aangeboden.
EA011	Overdracht	Bij beëindiging of ontbinding van de overeenkomst dient de Opdrachtnemer kosteloos alles in het werk te stellen om te komen tot een effectieve en geruisloze overdracht van werkzaamheden aan een (eventueel) nieuwe Opdrachtnemer. Alle gegevens welke Opdrachtnemer met betrekking tot de overeenkomst van Opdrachtgever in bezit heeft, worden op eerste verzoek direct digitaal aan Opdrachtgever ter beschikking gesteld.
EA012	Exitplan	Opdrachtnemer stelt kosteloos uiterlijk 2 maanden na implementatie van de Oplossing een exitplan op. Het exitplan dient te voldoen aan de eisen uit Bijlage M - Beschrijving Exit Scenario.
EA013	Verwerking van persoonsgegevens	Alle verwerking van persoonsgegevens vindt plaats binnen de Europese Economische Ruimte (EER). Dat wil onder andere zeggen dat alle personeel, apparatuur, gegevensopslag en netwerkverbindingen die voor de Opdrachtgever worden gebruikt, zich binnen de EER bevinden.
EA014	Updates en upgrades	Binnen de onderhoudsovereenkomst vallen ook de updates en upgrades van software, besturingssystemen en eventuele firmware, ongeacht de versie(s) en (nieuwe/extra) functionaliteiten.
EA015	Proactieve partner	Opdrachtnemer stelt zich op als proactieve partner. Dit houdt in dat zij acteert op wijzigingen/verbeteringen of andere zaken welke betrekking hebben op de aangeboden oplossing. Hierbij kan gedacht worden aan, echter niet limitatief, kennisdeling en doorontwikkeling van de dienstverlening en de geboden oplossing.
EA017	SROI	De SROI-inzet bedraagt 2% van de financiële omvang van de opdracht.
Eisen ten aanzien van de functionaliteiten		
Registreren van signalen (FrontOffice)		
EF001	Mogelijkheden FrontOffice	De FrontOffice oplossing moet voldoen aan minimaal de onderstaande mogelijkheden: - Registratie van signalen direct op straat worden ingevoerd (telefoon / mobiel). Met signalen wordt bedoeld wat de medewerkers van de WIJ zien op straat (overlast, armoede, etc.) om vervolgens vast te leggen als signaal, om vervolgens gebundeld acties op te zetten in de Back-office. - Registratie kan laagdrempelig uitgevoerd worden (1 scherm met minimaal invoer van locatie en selecteren / invoeren van een paar velden, zie hieronder) - Registratie voorziet erin dat gekozen kan worden om te registreren op locatie van bestemming of op gekozen locatie - Registratie op niveau van straat / postcode (zonder huisnummer of namen van inwoners) of de keuze op een hoger niveau (wijk, buurt of stadsbreed) - Kan worden geregistreerd met (vrij in te richten) categorisering, labels als leefgebied en thema's
EF002	Uploaden documenten signaal	Bij registratie van signalen is het mogelijk om documenten up te loaden (foto's of bestanden, in de standaard format van foto's en Office-applicaties als Word en Excel).
EF003	Vaste gegevensvelden signaal	De Oplossing biedt onderscheid tussen verplichte en optionele invoer velden bij het registeren van een signaal.

EF004	Verplichten gegevensvelden signaal	Gegevensvelden bij het registreren van een signaal moeten een verplichting tot invullen kunnen krijgen. In samenspraak met Opdrachtgever worden deze verplichte velden nader bepaald.
EF005	Uploaden documenten na vastlegging signaal	Via de BackOffice is het ook mogelijk om documenten up te loaden bij reeds vastgelegde signalen.
EF006	Inloggegevens	Iedere FrontOffice gebruiker heeft persoonlijke inloggevens, waarvan deze gegevens opvraagbaar moeten kunnen zijn.
EF007	Overzicht geregistreerde signalen	Iedere FrontOffice gebruiker kan zijn geregistreerde signalen terugvinden en gegevens in ieder signaal kunnen aanpassen, zodat foutieve gegevens of onnodige gegevens achteraf alsnog verwijderd kunnen worden.
EF008	Koppelen aan medewerker	Door registratie worden de signalen automatisch gekoppeld aan de desbetreffende medewerker van de WIJ die het heeft vastgelegd. Hierop is ook te selecteren tijdens de analyse in de BackOffice. Tevens is het mogelijk om in de BackOffice andere medewerkers te koppelen aan het signaal.
EF009	Inactieve medewerkers	Medewerkers die niet meer actief zijn, kunnen in de applicatie op inactief gezet worden. Het is tevens mogelijk in de applicatie om signalen en aanpakken/activiteiten van inactieve medewerkers over te zetten naar actieve medewerkers.
Workflow en inzicht in werkvoorraad (BackOffice)		
EF009	Status signaal	Medewerkers kunnen inzien op welke signalen al actie op is ondernomen en waar nog actie op genomen moet worden (werkvoorraad). Signalen kunnen worden gemarkeerd als zijnde 'Openstaand, 'ter kennisgeving', 'On-hold' en 'Afgehandeld' om op te kunnen filteren in de werkvoorraad. Dit kan ook bulksgewijs uitgevoerd worden.
EF010	Berichtgeving status signaal	Van (te lang, door opdrachtgever te bepalen) openstaande signalen waarop acties nodig zijn, dient de applicatie een signaal in de vorm van mail en/of alert uit te sturen naar de (programma)medewerker, zodat die de medewerker hierop kan aanspreken. Dit signaal is te configuren zodat het uit of aan gezet kan worden.
EF011	Verdeling signalen	Signalen kunnen worden gedistribueerd naar andere medewerkers, of team in de oplossing van de BackOffice. Deze medewerkers en/of Teams hebben tevens inzicht in hun werkvoorraad.
Analyseren gebieden (BackOffice)		
EF012	Mogelijkheden BackOffice	De BackOffice oplossing voorziet in een werkende digitale oplossing en moet minimaal de onderstaande mogelijkheden bevatten: - Geografisch inzicht in geregistreerde signalen - Filtermogelijkheden om 'datasets/data-lagen' uit en aan te zetten - Geeft inzicht in de gehele Gemeente Groningen en kan inzoomen op verschillende geografische entiteiten (Gemeente, Plaats, Wijk, Buurt, Straat) - Filtermogelijkheden op vlak van inhoud (Thema's, Leefgebieden, Etc.) - Bevat mogelijkheden om ook aan te tonen welke voorzieningen / activiteiten zijn geregistreerd voor welk thema, leefgebied. - Geeft duidelijk inzicht in aantallen (Aantal geregistreerde signalen op vlak van categorie of soort signaal)
EF013	Configureren datasets	De oplossing bevat mogelijkheden om andere datasets te configureren (en daarmee importeren) zonder dat de leverancier hoeft te ontwikkelen.
EF014	Grafische monitor	De oplossing kan in één integraal geografische monitor, inzichten geven op vlak van verschillende datasets inclusief de eigen geregistreerde signalen en vastgelegde aanpakken/activiteiten.
EF015	Aan en uitzetten datasets	De oplossing bevat de mogelijkheid om andere datasets (OpenData als politiegegevens, of omgevingsgegevens) aan en uit te zetten voor verschillende gebruikers.
EF016	Filters	De oplossing biedt mogelijkheden om in de geografische oplossing zelf filters te configureren, van velden die door eigen inrichting toegevoegd zijn.
Aanpakken / activiteiten registreren (BackOffice)		
EF017	Aanpakken bibliotheek	De oplossing bevat de mogelijkheid om een bibliotheek van aanpakken / activiteiten vast te leggen in de BackOffice oplossing. - Filtermogelijkheden op vlak van geografisch (Gemeente, Wijk, Buurt, Straat) - Filtermogelijkheden op vlak van inhoud (Thema's, Leefgebieden, Etc.) - Filtermogelijkheden op vlak van datum, medewerkers en status.
EF018	Gegevens registratie aanpak	Bij het registreren van de aanpakken / activiteiten wordt vastgelegd; een startdatum en einddatum, met een selecteerbare status. Tevens een mogelijkheid om een aanpak of activiteit te kopieren en hergebruiken in een nieuwe aanpak/activiteit.
EF019	Kenmerken registratie aanpak	Bij het registreren van deze aanpakken / activiteiten kunnen kenmerken meegegeven worden, waarop in de BackOffice gefilterd kan worden (Thema's, doelen, onderwerp).
EF020	Uploaden documenten aanpak	Bij de aanpakken / activiteiten is het mogelijk om bestanden / documenten te koppelen. Deze zijn in te zien voor de gebruikers die toegang hebben tot de aanpakken / activiteiten. De bestanden / documenten (standaard formats voor foto's en Office applicaties als Word en Excel) zijn ook te openen vanuit de applicatie.
EF021	Signalen koppelen aanpak	Bij de aanpakken / activiteiten is het mogelijk om meerdere signalen te koppelen aan de desbetrefende aanpak / activiteit. Hierbij maakt het niet uit welke medewerker van de WIJ het signaal heeft vastgelegd.
EF022	Mailing	De Oplossing biedt de mogelijkheid om op het niveau van een aanpak mailingen te versturen naar deelnemers van die aanpak.
EF023	Aanmelden bij aanpak	Via een ander pad, kunnen andere medewerkers deelnemers aan laten melden bij een bepaalde aanpak (bv. een training).
EF024	Afschermen deelnemerslijst	Deze deelnemerslijst van een bepaalde aanpak met privacygevoelige gegevens is af te schermen van andere gebruikers.
Eisen ten aanzien van gebruiksvriendelijkheid		
EG001	Taal	De Oplossing moet Nederlandstalig zijn, zowel FrontOffice als BackOffice.
Eisen ten aanzien van data en rapportages		
ED001	Exports Excel	De oplossing beschikt over de mogelijkheid om exports naar Excel te draaien van zowel de signalen als de aanpakken. Dit met filtermogelijkheden van de desbetreffende genoemde velden en datums.
ED002	Configureren open- of publieke data	De oplossing is te configureren aan open- of publieke data (zoals OpenData van Politie of CBS gegevens) zodat in de analyse ook hier rekening mee gehouden kan worden. Hiermee is het dan mogelijk dat er extra op gefilterd (uit en aan) kan worden in de Backoffice applicatie. Dit kan ingericht worden zonder dat er daadwerkelijk ontwikkeld hoeft te worden door de leverancier (geen maatwerk).

ED003	Exportmogelijkheden	De oplossing beschikt over exportmogelijkheid in Excel of CSV om de gegevens over te halen naar een Datawarehouse t.b.v. rapportage / data-integratie doeleinden.
ED004	Data	Data van de WIJ Groningen mag niet toegankelijk zijn voor andere klanten van de Opdrachtnemer en is daarom ook volledig gescheiden van andere klanten.
ED005	Data	De data in de Oplossing wordt ontsloten voor frontofficecomponenten (klantcontact- en webformulierenfunctionaliteit). Denk hierbij bijvoorbeeld aan zogenaamde pre-fill van webformulieren.
ED006	Opslagcapaciteit	De oplossing dient voldoende opslagcapaciteit te hebben, zodat de verwerking van data niet tegen beperkingen aanloopt. Hierbij rekening houdend met een juiste schaalgrootte welke van toepassing is voor de WIJ Groningen.
ED007	Eigenaarschap data	Eigenaarschap van data betekent dat de WIJ Groningen toegang heeft tot eigen data voor o.a. het onderhouden van rapportages vanuit het datawarehouse, kwaliteitscontroles doen op data, input voor rapportages en om procesanalyses uit te voeren. Opdrachtnemer stelt voor opdrachtgever de data beschikbaar voor het datawarehouse van WIJ Groningen, en zorgt voor een duurzame en geautomatiseerde oplossing zodat het datawarehouse periodiek gevuld wordt vanuit de SaaS-oplossing. Mogelijkheid 1 Toegang tot database tot de eigen data en alle tabellen en views van de oplossing (of een kopie hiervan). Mogelijkheid 2 Dagelijks geautomatiseerd bestanden overdragen. Het gaat hierom een back-up file of export middels CSV van alle records inclusief historie van de database van de Oplossing.
Eisen ten aanzien van het Service Level Agreement		
ES001	SLA	Opdrachtnemer biedt een SLA aan dat volledig aansluit bij de eisen uit dit PvE. Indien Opdrachtnemer hierbij gebruik maakt van een standaard SLA, kan deze gehandhaafd blijven en aangevuld worden met een addemdum om bovenstaande te bewerkstelligen.
ES002	Strategisch overleg	Opdrachtnemer heeft jaarlijks een strategisch overleg met Opdrachtgever. In dit overleg worden strategische/beleidskwesties besproken.
ES003		Opdrachtnemer heeft elk kwartaal (minimaal 4 keer per jaar) tactisch overleg met de Opdrachtgever.
ES004	Agenda overleg	Opdrachtnemer stelt in overleg met de Opdrachtgever de agenda op, werkt de notulen uit en draagt zorg voor de planning van de overleggen.
ES005	Inhoud SLA	De SLA dient te worden voorzien van een escalatieprocedure en -ladder.
ES006	Taal helpdesk	Opdrachtnemer verzorgt een deskundige Nederlandstalige helpdesk in spraak en geschrift, voor zowel technische als functioneel ondersteuning, telefonische, via e-mail en/of een webportaal. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/inzicht in de afhandeling daarvan.
ES007	Bereikbarheid helpdeesk	De helpdesk is telefonisch bereikbaar op werkdagen tussen 8:00 en 18:00.
ES008	Reactietijd categorieën	De reactietijd is gebaseerd op drie categorieën prioriteiten: Prio 1, 2, 3 en 4.
ES009	Bereikbaarheid	Voor het plaatsen van meldingen is Opdrachtnemer bereikbaar op werkdagen tussen 8:00 en 18:00. Opdrachtnemer werkt tussen deze tijden ook aan de oplossingen.
ES010	Prioritering bij melding	Opdrachtgever geeft bij het melden de prioriteit aan, de uiteindelijke prioritering wordt vastgesteld op onderstaande prioriteitesbepaling. Bij verschil met de opgegeven prioriteit informeert Opdrachtnemer Opdrachtgever hierover.
ES011	Prioritering definities	De prioritering is als volgt: Prio 1: De Oplossing is volledig niet beschikbaar. Prio 2: De Oplossing is deels niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers. Prio 3: Kleine verstoringen. Prio 4: Gebruikers / beheerdersvraag. De helpdesk van Opdrachtnemer draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen met betrekking tot de Oplossing.
ES012	Reactietijd	De reactietijd is onderverdeeld in twee aspecten: responsetijd en oplostijd. - Responsetijd: De tijd vanaf de melding tot het contact met Opdrachtgever over het incident. - Oplostijd: Gemiddelde tijd van een oplossing vanaf het moment van het contact met Opdrachtgever over het incident (Mean time to resolve - MTTR)
ES013	Escalatieprocedure	Vervolgens wordt het incident met de vastgestelde prioriteit afgehandeld. Indien geen overeenstemming wordt bereikt over de prioriteit treedt de escalatieprocedure in werking. - Prio 1: 60 minuten responsetijd en 8 uur oplostijd - Prio 2: 4 uur responsetijd en 16 uur oplostijd - Prio 3: 24 uur responsetijd en 40 uur oplostijd - Prio 4: 24 uur responsetijd en 40 uur oplostijd
Eisen ten aanzien van de KPI's		
EK001	Beschikbaarheid	De uptime van de Oplossing is 99% op jaarbasis. Hierbij is gepland onderhoud uitgezonderd van de beschikbaarheidsberekening wat tussen opdrachtgever en opdrachtnemer is afgestemd.
EK002	Rapportages	Opdrachtnemer zal de volgende standaard rapportages leveren: a.Realtime rapportage b.Management rapportage Deze rapportages, dan wel de inzet van een Service Delivery Manager om de rapportages vorm te geven, zullen zonder aanvullende kosten worden verstrekt.
EK003	Inhoud rapportages	De inhoud van de standaard rapportages kunnen op verzoek van Opdrachtgever worden aangepast. De inhoud van de aanpassingen wordt vastgesteld tijdens het Half-jaarlijksoverleg tussen Opdrachtgever en Opdrachtnemer.
EK004	Gepland onderhoud	Gepland onderhoud vindt 's nachts na 01:00 uur plaats en mag maximaal 2 uur per keer en maximaal 6 uur per kwartaal duren.
EK005	Aankondigen onderhoud	Gepland onderhoud is minimaal 1 week van tevoren bij de primaire contactpersoon van Opdrachtgever aangekondigd.
Privacy eisen		
EP001	AVG signalen	De te registereren signalen mogen geen AVG technische gegevens bevatten.
EP002	AVG aanpakken	Bij aanpakken / activiteiten is het mogelijk om deelnemers/inwoners te registreren met naam, emailadres en adres zodat er inzicht is in een deelnemerslijst. De Oplossing moet dan voldoen aan de AVG.

EP003	Privacy Impact Analyse	Opdrachtnemer gaat akkoord met het jaarlijks uitvoeren van een Privacy Impact Analyse op de applicatie en werkt mee aan het realiseren van de minimale maatregelen die hieruit voortvloeien.
EP004	Backups bewaartijd	Na afloop van de retentieperiode worden de backups verwijderd.
EP005	VOG	Opdrachtnemer zorgt voor VOG medewerkers op een door Opdrachtgever te controleren wijze.
EP006	DR en BC-plan	Opdrachtnemer heeft voor hetgeen zij verantwoordelijk is op het gebied van Disaster Recovery/Business Continuity plan een DR en BC-plan opgesteld en periodiek getest.
Commerciële en administratieve eisen		
EC001	Taal en valuta	De inschrijving van Opdrachtnemer is in de Nederlandse taal gesteld en de gehanteerde tarieven zijn in euro's, exclusief btw.
EC002	Indexering	De inschrijving bevat een volledig ingevuld prijsinvulformulier. Alle genoemde prijzen staan gedurende het eerste jaar van de overeenkomst vast. De prijzen kunnen na het eerste contractjaar éénmaal per jaar per 1 januari conform GIBIT 2023 artikel 9.6 worden bijgesteld. Aanpassingen van de prijzen naar aanleiding van de indexatie, zowel verlagingen (verplicht) als verhogingen, dienen uiterlijk één maand voorafgaande aan de ingangsdatum (lees: 1 januari) van de prijswijziging schriftelijk, gespecificeerd en rekenkundig onderbouwd, voorgesteld te worden aan de contractmanager van Opdrachtgever. Wanneer het voorstel tot prijsaanpassing niet voor 1 december is ingediend, vervalt het recht op indexering. Bij het niet melden van een prijsverlaging is Opdrachtnemer verplicht deze prijsverlaging met terugwerkende kracht door te voeren. Overige tariefstijgingen, buiten de genoemde indexatie om, worden uitdrukkelijk van de hand gewezen.
EC003	Geldende prijzen	Opdrachtnemer is bij haar inschrijving uitgegaan van geldende prijzen voor de dienstverlening en/of levering. Niet genoemde kosten kunnen onder geen geval alsnog in rekening worden gebracht bij de Opdrachtgever. Hetgeen door Opdrachtnemer wordt uitgewerkt in het kwalitatief gunningscriterium is in de opgegeven prijs van Opdrachtnemer inbegrepen.
EC004	Kosten implementatie	Kosten van Opdrachtnemer voor de implementatie worden separaat in het prijzenblad door inschrijver geduid en door de opdrachtnemer gefactureerd.
EC005	Factuuregevens	Opdrachtnemer factureert de jaarlijkse kosten per factuur achteraf. De factuur dient voldoende gespecificeerd te zijn met daarop alle kosten. Op de factuur dient minimaal vermeld te worden: 1. Door belastingdienst gestelde eisen 2. Ordernummer 3. Factuurnummer 4. Factuurperiode 5. Gericht aan de Gemeente Groningen, met adres van een van de locaties of pustbusnummer 6. Digitaal aangeleverd worden via facturendigitaal@groningen.nl 7. Factuur moet in PDF, evenals eventuele Bijlagen Betaling zal binnen 30 dagen door Opdrachtgever plaatsvinden.
EC006	Opschorten betaling	Indien blijkt dat een factuur onjuistheden bevat, behoudt de Opdrachtgever zich het recht voor de betaling op te schorten, totdat overeenstemming is bereikt tussen beide partijen.
EC007	Foutieve facturen	Foutieve facturen, bijvoorbeeld het gebruik van een onjuist werkordernummer, worden niet in behandeling genomen.
EC008	Wijze facturering	Op verzoek van de Opdrachtgever kan de wijze van de facturering worden aangepast. Het omschakelen naar een andere wijze van facturering geschiedt in overleg en kosteloos.
EC009	Factureren implementatiekosten	De implementatiekosten worden separaat gefactureerd aan de hand van onderstaande facturatieschema: a. 30% bij definitieve opdrachtverstrekking b. 40% bij start implementatie c. 30% na afronding implementatie en acceptatie door Opdrachtgever
Overige eisen		
EO001	Training FrontOffice	Opdrachtnemer maakt een e-learning voor het gebruik van de FrontOffice Oplossing. Deze e-learning dient beschikbaar te zijn voor de gehele looptijd van de Overeenkomst, zodat nieuwe medewerkers van Opdrachtgever deze e-learning op een later moment ook kunnen maken.
EC002	Training BackOffice	Opdrachtnemer biedt een training aan voor in totaal 100 medewerkers met een BackOffice licentie. In groepen van 10 medewerkers worden deze medewerkers in één training wegwijs gemaakt met de BackOffice Oplossing.
EC003	Gebruiksbeheer	Het gebruiksbeheer kan door Opdrachtgever zelf worden uitgevoerd. Dit betekent minimaal het toevoegen, wijzigen, kopiëren en verwijderen van gebruikers/rollen en het toekennen van de rechten en wachtwoorden.
Eisen ten aanzien van security		
Risicobeheer - algemeen		
SRA001	Vaststellen BIV-classificatie	Via een Business Impact Analyse (BIA) wordt de Beschikbaarheids-, Integriteits- en Vertrouwelijkheidsclassificaties door de lijnorganisatie vastgesteld. Een BIA wordt uitgevoerd als onderdeel van of voorafgaand aan het APM-traject of een grote wijziging op een bestaande applicatie. Op basis van deze BIV-classificatie is 'automatisch' bepaald welke maatregelen (minimaal) moeten worden meegenomen in de ontwikkeling en implementatie van de applicatie.
SRA002	Frequentie BIV-classificatie herzien	Periodiek wordt een Business Impact Analyse uitgevoerd om te toetsen of de BIV-classificaties nog correct is. Frequentie: Minimaal 1x per 3 jaar.
SRA003	Periodiek moet de BIV-classificatie herzien worden	Op basis van de (periodieke) herziening van de BIV-verificatie wordt een gapanalyse uitgevoerd. Hierbij wordt vastgesteld in hoeverre de daadwerkelijke inrichting van de applicatie hieraan voldoet.
SRA004	Borging dat informatiebeveiligings maatregelen zijn toegepast conform BIV-classificatie bij externe leveranciers	Wanneer de applicatie gehost wordt door een derde partij zijn informatiebeveiligingsmaatregelen vastgelegd in het contract en in onderliggende stukken.
SRA005	Frequentie toetsen of maatregelen zijn toegepast conform BIV-classificatie bij externe leveranciers	De informatiebeveiligingsmaatregelen moeten periodiek getoetst worden om vast te stellen of deze nageleefd worden. Frequentie: Minimaal 1x per jaar.

SRA006	Afhandeling informatiebeveiligingsrisico's	Alle informatiebeveiligingsrisico's worden geregistreerd in het centrale risicoregister en geclassificeerd. Bij de afhandeling van de risico's wordt de risicoclassificatie meegenomen in de prioriteitstelling / bepaling van de volgorde.
SRA007	Acceptatie risico's is niet langer dan toegestane periode	Na beoordeling van een risico kan besloten worden om het (rest-)risico te accepteren. De termijn van acceptatie is afhankelijk van de BIV-classificatie. Frequentie: Risicoclassificatie: Kritiek = geen RAO mogelijk Hoog = 3 maanden Midden = 6 maanden Laag/Informatief = maximaal 1 jaar
SRA008	Uitvoeren penetratietest	Geldt alleen voor *nieuwe* applicaties met functionaliteiten die via publieke netwerken ontsloten zijn.
SRA009	Periodiek worden penetratietesten uitgevoerd	Geldt alleen voor *bestaande* applicaties met functionaliteiten die via publieke netwerken ontsloten zijn. Frequentie: 1x per jaar en bij significante wijziging een test door een onafhankelijke partij.
Inrichting en applicatiebeheer - algemeen		
SIA001	Toegang tot applicatie via netwerk	Elke (interne en externe) applicatie dient voor de gebruikers uitsluitend benaderbaar te zijn via het netwerk van de gemeente Groningen.
SIA002	Configuratiebeheer op orde	In de configuratiebeheerapplicatie zijn de componenten, behorende bij de applicatie, en de onderlinge relaties vastgelegd conform het datamodel.
SIA003	Frequentie verificatie configuratie	Periodiek wordt gecontroleerd of de registratie in de configuratiebeheerapplicatie nog een juiste weergave is van de werkelijke inrichting. Frequentie: Minimaal 1x per jaar.
SIA004	Prioritering incidenten bij hoge impact	In het incidentbeheerproces worden incidenten bij eerste vastlegging geprioriteerd. De prioriteit wordt vastgesteld op basis van de impact en urgentie. De urgentie is gelijk aan de classificatie. Bij impact Hoog gelden de volgende prioriteringen. Frequentie: Prioriteit 1 (Hoog).
SIA005	Prioritering incidenten bij middel impact	In het incidentbeheerproces worden incidenten bij eerste vastlegging geprioriteerd. De prioriteit wordt vastgesteld op basis van de impact en urgentie. De urgentie is gelijk aan de classificatie. Bij impact Middel gelden de volgende prioriteringen. Frequentie: Prioriteit 1 (Midden).
SIA006	Prioritering incidenten bij lage impact	In het incidentbeheerproces worden incidenten bij eerste vastlegging geprioriteerd. De prioriteit wordt vastgesteld op basis van de impact en urgentie. De urgentie is gelijk aan de classificatie. Bij impact Laag gelden de volgende prioriteringen. Frequentie: Prioriteit 1 (Laag).
SIA007	Inrichting OTAP-omgevingen	Aanwezigheid van een Test-/Acceptatie-omgeving is verplicht en is (logisch dan wel fysiek) gescheiden van de Productie-omgeving. Voordat nieuwe of aangepaste software in productie wordt genomen moet deze eerst getest worden.
SIA008	Er is een update- en patchbeheerproces vastgesteld en geïmplementeerd	Via dit proces worden updates en patches gesignaleerd en doorgevoerd. Dit proces is geïmplementeerd voor alle systeemonderdelen die onderdeel uitmaken van de oplossing (onder andere applicatie, OS, e-mailserver, database).
SIA009	Functionele/technische inrichting OTAP-omgevingen	De inrichting van de OTA- en P-omgevingen zijn identiek (versies, OS, patchniveau) aan elkaar en volgen dezelfde updates.
SIA010	Serviceniveau	Definitie van de serviceniveaus en daarmee ook de maatregelen die daar in meegenomen zijn, zijn elders beschreven.
SIA011	TPM-eis in contracten	De naleving van de overeengekomen maatregelen wordt vastgesteld op basis van een *jaarlijkse* TPM. Indien dit van toepassing is moet dit in het contract met de leverancier zijn opgenomen. Frequentie: Minimaal 1x per jaar.
Inrichting en applicatiebeheer - beschikbaarheid		
SIB001	Er is een uitwijkplan opgesteld voor de applicatie	In het uitwijkplan is beschreven welke acties ondernomen moeten worden indien uitwijk van de applicatie nodig is.
SIB002	Vaststelling uitwijkomgeving	De keuze voor de inrichtingswijze van de uitwijkomgeving is vastgelegd. Frequentie: Cold standby.
SIB003	Frequentie actualiseren uitwijkplan	Periodiek moet het uitwijkplan gecontroleerd en waar nodig geactualiseerd worden. Hierbij wordt voornamelijk de documentatie, waarin is vastgelegd wat te doen in geval van een uitwijk, gecontroleerd.
SIB004	Frequentie uitvoeren uitwijktest	Periodiek wordt de werking getoetst van het uitwijkplan. Hierbij wordt een daadwerkelijke uitwijk gedaan. Hierbij wordt zowel het proces geverifieerd als de werking van de applicatie op de uitwijkomgeving.
Inrichting en applicatiebeheer - integriteit		
SII001	Testen datakwaliteit back-ups	Periodiek wordt, via een vastgesteld schema, voor een back-up gecontroleerd of deze ingezet kan worden om de gegevens te herstellen. Frequentie: minimaal 1x per jaar.
SII002	Invoervalidatie	Via invoervalidatie wordt voorkomen dat gegevens opgevoerd kunnen worden die niet passen in het datamodel van de applicatie. Dit is verplicht bij webapplicaties.
SII003	Controle op datakwaliteit	Periodiek wordt de datakwaliteit expliciet gecontroleerd door vast te stellen of de vastgelegde data voldoet aan het vastgestelde datamodel.
Logging en monitoring - integriteit		
SLI001	Logging inloggen beheeraccounts	Beheeraccounts zijn accounts waar veel rechten aan toegekend zijn. Het gebruik van dit soort accounts is daarmee risicovol en dient te worden gelogd.
SLI002	Logging configuratiewijzigingen	Met behulp van configuratie-instellingen worden bepaalde maatregelen technisch afgedwongen. Wijzigingen die doorgevoerd worden aan deze instellingen kunnen deze gewenste technische maatregelen mogelijk wegnemen en dienen derhalve gelogd te worden.
SLI003	Monitoring van logging	Op basis van de logging van beheeraccounts en configuratiewijzigingen moet, vooraf bepaalde, periodieke monitoring ingeregeld worden.
SLI004	Periodieke controle op effectiviteit en volledigheid logging en monitoring	Vanwege wijzigende omstandigheden is het nodig om periodiek de logging [I-LenM-1/2/3] en daarop gebaseerde monitoring te controleren. Frequentie: Min. 1x per 2 jaar.

SLI005	Het wijzigen, creëren en verwijderen van gegevens wordt geregistreerd (gelogd) in een logbestand	Logging is nodig om achteraf te kunnen vaststellen welke acties zijn uitgevoerd en wie deze acties heeft uitgevoerd. Deze logging moet op gebruikersaccountniveau inzicht geven in de uitgevoerde acties. Te loggen acties en detail vast te stellen op basis van beheer behoefte.
SLI006	Vaststellen bewaartermijnen logbestanden	Voor logbestanden gelden (wettelijke minimale en maximale) bewaartermijnen. Voor iedere logging moet vastgesteld worden welke bewaartermijn van toepassing is. Waar geen wettelijk bewaartermijn is voorgeschreven geldt vanuit de BIG/BIO dat logging minimaal 3 maanden en maximaal 36 maanden (in het geval van een bijvoorbeeld een informatiebeveiligingsincident) bewaard moet worden.
SLI007	Naleving bewaartermijnen logbestanden	Voor logbestanden gelden (wettelijke minimale en maximale) bewaartermijnen. Periodiek moet gecontroleerd worden of deze bewaartermijnen nageleefd worden. Frequentie: Min. 1x per 2 jaar.
Risicobeheer - vertrouwelijkheid		
SRV001	Aanvullend een (D)PIA uitvoeren	Wanneer de applicatie persoonsgegevens bevat is het nodig om een Privacy Impact Analyse (PIA) uit te voeren. Hiermee wordt dieper ingegaan op de privacyrisico's van die specifieke verwerking van persoonsgegevens en de gewenste maatregelen.
Inrichting/applicatiebeheer - vertrouwelijkheid		
SIV001	Testomgeving bevat geen authentieke persoonsgegevens	In de productieomgeving wordt de toegang tot gevoelige data ingeperkt met behulp van autorisaties. De medewerkers die toegang krijgen hebben dit nodig voor het uitvoeren van hun functie. Voor het testen van aangepaste software is het wel nodig om testdata beschikbaar te hebben. Het is echter niet noodzakelijk dat dit dezelfde (authentieke) gegevens zijn als in de productieomgeving. De testdata moet wel representatief zijn om goed te kunnen testen. In het geval toch van authentieke (persoons)gegevens gebruik wordt gemaakt ligt hieraan een formele goedkeuring door de CISO aan ten grondslag. Alle naar een individu te relateren gegevens moeten zijn geanonimiseerd.
SIV002	Bescherming systeemdocumentatie	Systeemdocumentatie, met mogelijk vertrouwelijke informatie, wordt beschermd tegen onbevoegde toegang en is niet vrij toegankelijk.
Logische toegangsbeveiliging - vertrouwelijkheid		
SLV001	Goedgekeurde autorisatiematrix is aanwezig	Het ontwerp van de autorisatiestructuur is door de applicatie-eigenaar vastgelegd in een autorisatiematrix en deze is goedgekeurd door de *proces* eigenaar. Daarbij wordt minimaal rekening gehouden met gewenste scheiding tussen: - conflicteren rollen (functiescheiding en zo nodig 4-ogenprincipe voor het doorvoeren van kritische wijzigingen); - beheertaken en gebruikstaken; - autorisaties in de productie- en andere omgevingen (OTA).
SLV002	Registratie gebruikers derden	In de autorisatiematrix zijn de gegevens geregistreerd van gebruikers die gebruikt worden door derden. Het gaat hier voornamelijk om de gebruikers van externe leveranciers.
SLV003	Periodieke verificatie autorisatiematrix	Bij deze verificatie wordt de opzet van de autorisatiematrix geverifieerd. Hierbij worden minimaal de volgende zaken gecontroleerd: - zijn de beschreven applicatiefuncties nog conform inrichting van de applicatie; - komt de eigenaar overeen met de registratie in de CMDB (ServiceNow); - is het gedelegeerd eigenaarschap nog juist belegd en geregistreerd. Frequentie: Minimaal 1x per jaar.
SLV004	Periodieke verificatie daadwerkelijk toegekende autorisaties	Bij deze verificatie worden de daadwerkelijk toegekende autorisaties vergeleken met de structuur zoals in de autorisatiematrix is vastgelegd. Hierbij worden minimaal de volgende zaken gecontroleerd: - zijn gebruikers geautoriseerd die niet meer werkzaam zijn bij de organisatie; - sluiten de autorisaties aan bij de functie en afdeling van de gebruikers; - komen de autorisaties overeen met de autorisaties gekoppeld aan de applicatiefunctie die aangevraagd is voor de medewerker; - zijn de gebruikers voor derden nog in nodig. Frequentie: Minimaal 1x per kwartaal.
SLV005	Periodieke verificatie contactgegevens bekend bij leverancier	Met de leveranciers van applicaties worden afspraken gemaakt over de communicatie tussen de leverancier en WIJ Groningen. Het gaat hier bijvoorbeeld om de communicatie over verstoringen, rfc's, patches en updates. Periodiek moet geverifieerd worden of de contactgegevens die bekend zijn bij de leverancier nog juist zijn. Frequentie: Minimaal 1x per jaar.
SLV006	Authenticatie via centrale credential store van Gemeente Groningen	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar. Gebruikers worden geauthenticeerd via een beveiligde koppeling met de centrale identiteitenadministratie (via Azure AD, ADFS of LDAP).
SLV007	Wachtwoordinstelling en voldoen minimaal aan het wachtwoordbeleid	Indien de applicatie voor authenticatie niet aangesloten is op de centrale Active Directory of LDAP moet binnen de applicatie zelf een wachtwoordbeleid afgedwongen worden. Dit moet conform vastgesteld wachtwoordbeleid.
SLV008	Wachtwoorden worden gehashed opgeslagen	Indien wachtwoorden in de applicatie worden vastgelegd moet de opslag ervan gehashed worden. Hierbij gelden de volgende criteria. Elk wachtwoord heeft een eigen salt waarde (minimaal 64 bits) en wordt gehashed met een SHA-2 algoritme met minimaal 1000 iterations).
SLV009	Aantal authenticatiefactoren dat minimaal toegepast moet worden bij gebruik vanaf het interne netwerk	Authenticatie is het proces waarbij nagegaan wordt of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij/zij beweert te zijn. Bij gevoelige gegevens is er meer zekerheid nodig.

SLV010	Aantal authenticatiefactoren dat minimaal toegepast moet worden bij gebruik vanaf een extern of openbaar netwerk	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie. In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd.
SLV011	Goedkeuring autorisatieaanvragen	Autorisaties worden enkel verstrekt na goedkeuring door de (gedelegeerd) proces-of applicatie-eigenaar.
SLV012	Audittrail autorisatieaanvragen aanwezig	De audittrail geeft inzicht in de stappen die een autorisatieaanvraag heeft doorlopen van het moment van indienen tot en met het afhandelen van de aanvraag.
SLV013	Periodiek wordt gecontroleerd op niet gebruikte autorisatiecomponenten	Met deze verificatie wordt bepaald of alle autorisatiecomponenten zoals AD-groepen of autorisatiegroepen binnen de applicatie nog gebruikt worden/nog nodig zijn. Als dit niet het geval is moeten deze opgeruimd worden. Frequentie: Min. 1x per jaar.
SLV014	Blokkeren accounts na foutieve inlogpogingen	Accounts worden automatisch geblokkeerd na maximaal 5 foutieve inlogpogingen.
SLV015	Beëindigen openstaande sessies bij inactiviteit	Van de systemen die via het netwerk te bereikbare zijn en die niet actief worden gebruikt, worden de sessies automatisch dagelijks beëindigd. Na maximaal 15 minuten inactiviteit van een gebruiker dient deze zich opnieuw te authenticeren (blokkering door middel van beeldschermbeveiliging op het werkstation).
SLV016	Wachtwoord niet zichtbaar	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
Logging en monitoring - vertrouwelijkheid		
SLM001	Logging mutaties gebruikers	Het aanmaken en muteren van gebruikers wordt gelogd.
SLM002	Logging autorisatiegroepen	Wijzigingen van autorisatiegroepen worden gelogd.
SLM003	Logging toekennen of verwijderen autorisaties	Het toekennen of verwijderen van autorisatiegroepen aan gebruikers wordt gelogd.
SLM004	Inzien van gegevens wordt geregistreerd (gelogd) in een logbestand	Logging is nodig om achteraf te kunnen vaststellen welke acties zijn uitgevoerd en wie deze acties heeft uitgevoerd. Deze logging moet op het niveau van gebruikersaccount inzicht geven in de uitgevoerde acties.
SLM005	Monitoring op aanpassingen aan gebruikers en autorisaties	Monitoring moet ingeregeld worden om aanpassingen door onbevoegden te signaleren en af te handelen.
SLM006	Logging aanmaken van back-ups	Back-ups zijn een manier om grote hoeveelheden data uit databases te halen en daarmee aantrekkelijk om data diefstal op uit te voeren.
SLM007	Monitoring op manueel aangemaakte back-ups	Het aanmaken van een back-up wordt normaliter uitgevoerd door een systeem account. Wanneer dit door een ander account wordt gedaan wijkt dit af van dit uitgangspunt.
SLM008	Geen gevoelige gegevens in logging	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).
Hardening		
SH001	Periodiek worden vulnerabilityscans uitgevoerd	Vulnerabilityscans worden uitgevoerd op serverniveau. De classificatie van een server is gebaseerd op de classificatie van de applicatie die er op draait. Frequentie: 1x per jaar.
SH002	Registratie kwestbaarheden	Bevindingen uit vulnerability scans worden als rfc geregistreerd in het centraal meldingensysteem.
SH003	Periodieke controle patches	Periodiek wordt gecontroleerd of er patches zijn uitgebracht. Frequentie: Min. 1x per kwartaal.
SH004	Patches (met CVSS Low: 0.1 t/m 3.9)	Patches met CVSS Low (0.1 t/m 3.9) worden tijdig geinstalleerd. Frequentie: Binnen 1 jaar.
SH005	Patches (met CVSS Medium: 4.0 t/m 6.9)	Patches met CVSS Medium (4.0 t/m 6.9) worden tijdig geinstalleerd. Frequentie: Binnen 180 dagen.
SH006	Patches (met CVSS High: 7.0 t/m 8.9)	Patches met CVSS High (7.0 t/m 8.9) worden tijdig geinstalleerd. Frequentie: Binnen 24 dagen.
SH007	Patches (met CVSS Critical: 9.0 t/m 10)	Patches met CVSS Critical (9.0 t/m 10) worden tijdig geinstalleerd. Frequentie: Binnen 4 dagen.
Encryptie		
SE001	Encryptie van opslagsystemen (storage en back-up)	Gegevens die opgeslagen worden op storage systemen versleuteld opgeslagen.
SE002	Encryptie van databases	Gegevens op database worden vercijferd opgeslagen middels de door de leverancier geboden oplossingen.
SE003	Versleuteling inloggegevens	Inloggegevens worden alleen over versleutelde verbindingen verstuurd.
Eisen ten aanzien van informatiebeheer		
Archieffunctionaliteit		
AF001	archieffunctionaliteit	De Oplossing kan documenten en bijbehorende metadata opnemen, beheren en veilig opslaan en borgen dat ze, gedurende hun bewaartermijn (maximaal 5 jaar), toegankelijk en opvraagbaar blijven. De koppeling tussen metadata en informatieobject moet gedurende deze bewaartermijn in stand blijven.

AF002	archieffunctionaliteit	De Oplossing is in staat een overzicht te genereren van signalen en/of activiteiten die in aanmerking komen voor vernietiging op basis van de bewaartermijn en kan dit overzicht, 'de vernietigingslijst', exporteren naar een bruikbaar formaat, bij voorkeur excel.
AF003	archieffunctionaliteit	De Oplossing is in staat, op basis van bovengenoemd vernietigingsoverzicht, signalen en/of activiteiten en de bijbehorende documenten en metadata onherstelbaar te vernietigen.
AF004	archieffunctionaliteit	De Oplossing is in staat bewaartermijnen (bij voorkeur geautomatiseerd) toe te kennen aan een signaal/activiteit. Documenten overerven de bewaartermijn van het project waar zij onderdeel van zijn.
AF005	archieffunctionaliteit	De Oplossing is in staat bewaartermijnen te laten ingaan door middel van 1. Geautomatiseerde start van de bewaartermijn op basis van afhandeling van het het dossier en 2. op basis van een handmatige actie.
Overig		
OVG001	bestandsformaten	De Oplossing ondersteunt (de opname van) de volgende bestandsformaten: PDF A/1A en A/2A, PDFA/1B, PDF1.7, odt, docx, rtf, txt, tiff, png, jpeg, jpg, jp2, jpx, gif, bmp, eml, msg, odp, pptx, warc, ods, csv, xlsx.
OVG002	Documentbeheer	Documenten kunnen worden gefixeerd en zijn beveiligd tegen onbedoelde en onbevoegde wijzigingen.
OVG005	metadata	Het is niet mogelijk om documenten zonder de verplichte metadata te registreren.
OVG006	metadata	Metadata mag niet ongeautoriseerd verwijderd worden. Metadata moet geautoriseerd gewijzigd kunnen worden, bijvoorbeeld in het geval van onjuistheden. Wijzigingen in de metadata worden vastgelegd in een logging.
OVG009	metadata	Ieder te onderscheiden informatieobject (dossier en document) worden voorzien van een uniek identificatiekenmerk of -nummer.
OVG012	Zoekfunctie	De Oplossing heeft een zoekfunctie. Met deze zoekfunctie is alle informatie eenvoudig en binnen redelijke tijd terug te vinden.
OVG013	Zoekfunctie	Elk document kan in de applicatie binnen redelijke tijd en inspanning geopend en bekeken worden.