Bijlage 5. Programma van Eisen en Wensen

Leveren, implementeren en onderhouden van een Identity en Access Managementsysteem

Nummer aanbesteding: 2026-198

Gemeente Zaanstad
Cluster Bedrijfsvoering
Afdeling Informatie, Beheer en Techniek (IBT)

Postbus 2000
1500 GA Zaandam

Bezoekadres:
Stadhuisplein 100
1506 MZ ZAANDAM

Datum: 31-08-2026
Status: Definitief

Inhoud

1 Inleiding

In deze bijlage vindt u het Programma van Eisen en Wensen. De eisen (aangeduid met een ‘E’) zijn uitsluitende criteria; het niet onvoorwaardelijk voldoen aan deze eisen heeft uitsluiting van verdere deelname aan deze aanbestedingsprocedure tot gevolg. Met inschrijving op de aanbesteding geven inschrijvers aan onverkort aan alle eisen te voldoen bij de uitvoering van de opdracht.

De wensen (aangeduid met ‘W’) zijn sub-subgunningscriteria. Per wens kan een vastgesteld maximaal aantal punten worden behaald (zie paragraaf 5.3 van de Offerteleidraad). Afhankelijk van de beoordeling wordt 0 - 100% van deze punten toegekend. Voor wens 1 t/m 5 maakt naast de schriftelijke inschrijving ook de demonstratie onderdeel uit van de beoordeling.

Voor een goed begrip van de inhoud van de eisen en wensen wordt geadviseerd eerst de begrippen- en afkortingenlijst (*bijlage 2*) zorgvuldig door te nemen. De daarin gedefinieerde termen worden consequent gebruikt in de beschrijving. Een eenduidig begrip is essentieel om een gedeeld beeld te waarborgen en misverstanden te voorkomen.

Omdat in deze aanbesteding de Oplossing zowel als Software as a Service (SaaS) als On-Premise wordt aangeboden, is dit Programma van Eisen en Wensen zodanig opgesteld dat het van toepassing is op beide leveringsmodellen.

Waar in het Programma van Eisen en Wensen expliciet onderscheid wordt gemaakt naar leveringsmodel (bijvoorbeeld door middel van formuleringen als “indien de Oplossing als SaaS wordt geleverd”), zijn deze eisen en wensen uitsluitend van toepassing op het betreffende leveringsmodel. Dit laat onverlet dat inschrijver – conform de Offerteleidraad – zowel een SaaS- als een On-Premise leveringsmodel dient aan te bieden.

Indien een eis of wens geen onderscheid maakt naar leveringsmodel, wordt deze geacht van toepassing te zijn ongeacht het leveringsmodel.

2 Omschrijving Oplossing

De Oplossing betreft een moderne ‘Identity en Access Management’(IAM)-systeem dat de volledige lifecycle van identiteiten en Autorisaties binnen de gemeente ondersteunt en grotendeels automatiseert. Het systeem beheert centraal de registratie van identiteiten, verwerkt instroom-, doorstroom- en uitstroommutaties en kent op basis daarvan automatisch de juiste Autorisaties toe of trekt deze tijdig in. Daarbij faciliteert het een gestandaardiseerd aanvraag- en goedkeurproces voor Procesrollen en zelfstandig los aan te vragen Autorisaties, waarin medewerkers en Rolhouders via gebruiksvriendelijke interfaces hun verantwoordelijkheden uitvoeren.

Daarnaast draagt de Oplossing bij aan risicobeheersing en informatieveiligheid door continue monitoring, proactieve signalering van afwijkingen en volledige reproduceerbaarheid van wijzigingen. Het systeem biedt inzicht en sturingsmogelijkheden voor Rolhouders en beheerders, ondersteunt zowel automatische als handmatige processen, en borgt dat toegangsrechten gecontroleerd, compliant en toekomstvast worden beheerd, zodat bedrijfscontinuïteit, rechtmatige gegevensverwerking en security gewaarborgd blijven.

3 Eisen en wensen

3.1 Algemene eisen

Nr.	Omschrijving
E1	Op elke factuur wordt onze referentie vermeld (inkooporder), de vakafdeling en het factuuradres: Gemeente Zaanstad, t.a.v. Crediteurenadministratie, Postbus 2000, 1500 GA Zaandam. Opdrachtnemer verzendt de factu(u)r(en) maandelijks na afloop van een kalendermaand slechts eenmaal toe (bij voorkeur via e-facturatie) aan de Gemeente Zaanstad, onder vermelding van alle wettelijke en bijzondere door de Gemeente Zaanstad gestelde eisen naar facturen@zaanstad.nl. Alle prijzen zijn inclusief de CAO wijzigingen; Alle prijzen zijn inclusief eventuele opslagen; Alle prijzen dienen exclusief BTW te worden opgegeven; Alle prijzen zijn inclusief alle kosten voor dienstverlening en kosten van derden die door Opdrachtnemer worden ingeschakeld.
E2	De Opdrachtnemer is in staat om de aangeboden functionaliteiten tijdens de demonstratie live te tonen, met uitzondering van externe koppelingen. De getoonde functionaliteiten zijn representatief voor de daadwerkelijk aangeboden Oplossing.
E3	De Oplossing past eventuele algoritmische toepassingen uitsluitend toe met een ondersteunend en adviserend karakter. Het gebruik hiervan is optioneel en vormt geen randvoorwaarde voor het functioneren van de kernfunctionaliteit van de Oplossing. Indien er algoritmische toepassingen worden ontwikkeld met een ander doel dan “ondersteunend of adviserend” dan is toestemming van Opdrachtgever vereist. Onder algoritmische toepassingen wordt verstaan: software waardoor op geautomatiseerde wijze voorspellingen worden gedaan, beslissingen worden genomen en/of adviezen worden gegeven op basis van data-analyse, statistiek, generatieve AI en/of zelflerende logica. Per algoritmische toepassing wordt inzicht geboden in het doel, de werking, de gebruikte gegevens binnen de IAM-context, alsmede de belangrijkste aannames, modellen en keuzes die aan de uitkomsten ten grondslag liggen. Daarbij wordt tevens inzicht gegeven in de betrokken partijen, waaronder eventuele subverwerkers. De door de gemeente aangeleverde gegevens blijven te allen tijde eigendom van de gemeente en worden uitsluitend gebruikt voor de uitvoering van de overeenkomst. Deze gegevens worden niet gebruikt voor het trainen, verbeteren of hergebruiken van algoritmische toepassingen buiten de context van de overeenkomst, tenzij de gemeente hiervoor vooraf expliciet schriftelijke toestemming heeft verleend. Op verzoek van de gemeente worden de gegevens verwijderd dan wel beschikbaar gesteld in een gangbaar en overdraagbaar formaat. Het gebruik van gegevens binnen algoritmische toepassingen vindt plaats conform de geldende wet- en regelgeving en de binnen deze aanbesteding gestelde eisen ten aanzien van informatiebeveiliging en privacy, waaronder in ieder geval de AVG, BIO2 en NIS2.

3.2 Functionele Eisen en wensen

3.2.1 Identity Lifecycle Management

Zie bijlage 13 Functioneel Ontwerp: Hoofdstuk 2 IDU.

Nr.	Omschrijving

E4	De Oplossing ondersteunt de geautomatiseerde afhandeling van instroom-, doorstroom- en uitstroomprocessen (IDU) van Identiteiten uit het HR-systeem of via handmatige invoer.
	
	Nieuwe Identiteiten en wijzigingen in Identiteitskenmerken van bestaande Identiteiten, zoals organisatorische eenheid, arbeidsrelatie, roltoewijzing en dienstverband, leiden op basis van configureerbare regels tot het automatisch toekennen of intrekken van HR-attributen. Tevens worden, indien van toepassing, aanvullende synchronisatieacties aangestuurd richting aangesloten Doelsystemen.
	
	Aan een HR-attribuut zijn één of meerdere Autorisaties gekoppeld. Identiteiten waaraan het betreffende HR-attribuut is toegekend, ontvangen de bijbehorende Autorisaties automatisch. De HR-attributen worden beheerd binnen het autorisatiebeheer.
	
	Opdrachtgever verlangt dat de geautomatiseerde IDU-keten binnen de Oplossing wordt ingericht op basis van een eenmalige, consistente configuratie van regels, waarvan de werking overeenkomt met het Functioneel Ontwerp (*bijlage 13*) en die voorspelbaar en beheersbaar functioneert.
	
	Dit omvat minimaal de volgende geautomatiseerde acties:
	• Het toevoegen, wijzigen en verwijderen van HR-attributen, inclusief het automatisch verstrekken en intrekken van bijbehorende Autorisaties en bedrijfsmiddelen.
	• Het activeren en inactiveren van:
	  ○ IAM-persoonskaart
	  ○ Topdesk-persoonskaart.
	• Het versturen van relevante notificaties en signaleringen bij instroom en uitstroom.
	• Indien het leveren van een Domeinaccount en/of toegangspas onderdeel is van het HR-attribuut *BML*, ondersteunt de Oplossing aanvullend:
	  ○ Een door IAM gegenereerde unieke accountnaam en e-mailadres in de Active directory bij aanvang van ieder Contract of bij heractivatie.
	  ○ Het afhandelen van contractbeëindiging, waarbij:
	  ▪ het AD-account wordt gedeactiveerd;
	  ▪ gebruikersaccounts en Autorisaties in applicaties na een configureerbare termijn worden ingetrokken;
	  ▪ het AD-account na 30 dagen automatisch wordt verwijderd.

E5	De Oplossing moet ondersteunen dat één natuurlijke persoon gelijktijdig meerdere Identiteiten kan hebben, indien deze werkzaamheden verricht voor meerdere Organisaties binnen de Oplossing, bijvoorbeeld voor de gemeente Zaanstad en één of meerdere Partnerorganisaties. In deze situaties wordt per Organisatie een afzonderlijke Identiteit vastgelegd binnen een eigen Identiteitscontainer Dit betreft expliciet geen scenario waarin één Identiteit meerdere rollen, Autorisaties of HR-attributen heeft binnen één Organisatie, maar een bewuste scheiding van Identiteiten per Organisatie.

	Voor iedere afzonderlijke Identiteit geldt dat: - een eigen IAM-persoonskaart wordt aangehouden; - een eigen lifecycle voor instroom, doorstroom en uitstroom (IDU) wordt toegepast; - Autorisaties uitsluitend binnen de betreffende Identiteitscontainer worden toegekend en beheerd; wijzigingen in de ene Identiteit geen automatische gevolgen hebben voor andere Identiteiten van dezelfde natuurlijke persoon.
E6	De Oplossing detecteert afwijkingen en fouten in brongegevens (uit het HR-systeem of handmatige invoer) vóór verwerking en synchronisatie, zodat onjuiste of onvolledige gegevens niet automatisch worden doorgevoerd.
E7	De Oplossing moet het toekennen of intrekken van HR-attributen loggen, inclusief datum/tijdstip, oude en nieuwe waarde en actietype (toegevoegd / verwijderd). Deze logging is op Medewerker-niveau inzichtelijk (bijvoorbeeld via de IAM-persoonskaart) en kan gebruikt worden voor het traceren van de verstrekkings- en intrekkingshistorie van automatisch verstrekte Autorisaties.
E8	De Oplossing biedt de mogelijkheid voor een geautoriseerde groep Medewerkers om AD-accountbeheer uit te voeren. Deze Medewerkers kunnen wachtwoorden resetten, accounts ontgrendelen en handmatig Autorisaties toekennen aan Medewerkers. Deze handelingen worden vastgelegd in het auditlog en zijn inzichtelijk via de IAM-persoonskaart.
W1	**Identity Lifecycle Management** Opdrachtgever wenst een Oplossing voor Identity Lifecycle Management (IDU-keten) die na een eenmalige configuratie stabiel, voorspelbaar en beheersbaar functioneert. De Oplossing biedt inzicht in de werking van de IDU-keten en ondersteunt functioneel beheerders bij het monitoren, bijsturen en gecontroleerd wijzigen van configuraties, zodat de werking ook bij wijzigingen voorspelbaar blijft. Daarnaast biedt de Oplossing tijdig en Rolhoudergericht inzicht in relevante wijzigingen van Identiteiten en HR-gegevens, maakt zij snelle interventie mogelijk bij beveiligings- en integriteitsrisico's en valideert zij de kwaliteit van brongegevens en wijzigingen voorafgaand aan verwerking, inclusief het detecteren van afwijkingen, het inzichtelijk maken van de impact van wijzigingen en het gecontroleerd verwerken van uitsluitend gevalideerde en gewenste mutaties. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Identity Lifecycle Management' en ga daarbij in ieder geval in op: **A. Inrichting en wijzigbaarheid van IDU-regelconfiguratie** Beschrijf hoe de eenmalige inrichting van de IDU-regelconfiguratie (zie eis E4) wordt uitgevoerd door de leverancier en hoe deze inrichting zodanig wordt opgezet dat zij langdurig stabiel en voorspelbaar functioneert. Tevens beschrijven op welke wijze na de configuratie beperkte wijzigingen kunnen worden doorgevoerd, zelfstandig door functioneel beheer. **B. Signalering en inzicht bij wijzigingen in identiteiten en HR-attributen** Beschrijf welke signalerings- en inzichtmechanismen de Oplossing biedt om Leidinggevenden en Proceseigenaren tijdig te attenderen op relevante wijzigingen in identiteiten en HR-attributen, zoals doorstroom of functiewijzigingen. Beschrijf hoe deze signaleringen bijdragen aan eenduidig, laagdrempelig en controleerbaar autorisatiebeheer.

	C. Snel intrekken en pauzeren van rechten bij risico's Beschrijf hoe de Oplossing snelle en efficiënte maatregelen ondersteunt om gebruikersrechten direct in te trekken of te pauzeren bij beveiligings- of integriteitsrisico's. Hierbij wordt toegelicht hoe individuele Gebruikers met één actie kunnen worden geblokkeerd, waarbij dit leidt tot het direct inactief zetten van het AD-account en de toegangspas, zodat verdere toegang tot systemen en gegevens wordt voorkomen. **D. Detectie en validering van brongegevens vóór synchronisatie** Beschrijf hoe de Oplossing voorafgaand aan synchronisatie afwijkingen of fouten in HR-gegevens (zoals ongeldige startdata, ontbrekende gegevens of dubbele Medewerkers) detecteert en inzichtelijk maakt. Beschrijf daarnaast hoe de Oplossing de impact van wijzigingen in configureerbare regels vooraf inzichtelijk maakt. Geef aan hoe beheerders deze bevindingen kunnen beoordelen, synchronisaties of wijzigingen kunnen pauzeren, correcties kunnen doorvoeren en vervolgens gecontroleerd kunnen vrijgeven, zodat alleen gevalideerde en gewenste wijzigingen worden verwerkt.

3.2.2 Handmatige invoer identiteiten Partnerorganisaties

Zie bijlage 13 Functioneel Ontwerp: Hoofdstuk 2 IDU.

Nr.	Omschrijving
E9	De Oplossing biedt functionaliteit waarmee geautoriseerde Gebruikers identiteiten van Partnerorganisaties handmatig kunnen aanmaken, aanpassen en beheren. Hierbij gaat het om vergelijkbare Identiteitskenmerken als die in het HR-systeem worden vastgelegd.
E10	De Oplossing moet ondersteunen dat voor handmatig geregistreerde identiteiten het automatische Identity Lifecycle Management (IDU-keten) gelijkwaardig functioneert (zie voorgaande eisen *Identity Lifecycle Management*) als voor identiteiten uit het HR-systeem.
E11	De Oplossing voorkomt het handmatig aanmaken van dubbele Identiteiten binnen één Identiteitscontainer en waarborgt dat iedere natuurlijke persoon binnen deze Identiteitscontainer eenduidig en slechts éénmaal als Identiteit wordt vastgelegd.
E12	De Oplossing zorgt dat Identiteiten en bijbehorende persoonsgegevens uitsluitend zichtbaar en benaderbaar zijn voor geautoriseerde Medewerkers, op basis van toegekende Procesrollen en de daarbij behorende Autorisaties.
W2	**Handmatige invoer identiteiten Partnerorganisaties** Opdrachtgever wenst dat in de toekomst (gedeeltelijk) gedecentraliseerd beheer dan Identiteiten mogelijk is voor medewerkers in de Partnerorganisaties, bijvoorbeeld via gedelegeerd beheer of selfservicefunctionaliteit, waarbij de handmatige invoer en het beheer van identiteiten op een gebruiksvriendelijke wijze kunnen plaatsvinden. De beheersbaarheid van handmatig ingevoerde identiteiten staat voorop. Eventuele decentralisatie betreft uitsluitend het beheer van Identiteiten van Medewerkers die werkzaam zijn voor de betreffende Partnerorganisatie; alle overige identiteiten blijven gescheiden onder beheer van de gemeente Zaanstad of andere Partnerorganisaties. Beschrijf hoe Opdrachtnemer invulling geeft de wens 'Handmatige invoer identiteiten Partnerorganisaties' en ga daarbij in ieder geval in op:

	A. Gedelegeerd en/of self-service identiteitsbeheer Beschrijf hoe de Oplossing het (gedeeltelijk) gedelegeerd en/of self-service aanmaken, wijzigen en beheren van Identiteiten van Partnerorganisaties ondersteunt, zodanig dat dit op een gebruiksvriendelijke wijze kan plaatsvinden en tegelijkertijd leidt tot een beheersbare en controleerbare inrichting van het identiteitsbeheer. Ga daarbij in op de wijze waarop Partnerorganisaties Identiteiten handmatig kunnen invoeren en beheren, hoe de afbakening van verantwoordelijkheden, rollen en bevoegdheden is ingericht en hoe wordt geborgd dat Partnerorganisaties uitsluitend Identiteiten binnen hun eigen Identiteitscontainer kunnen beheren. Beschrijf tevens welke controles en validatiemechanismen beschikbaar zijn bij het correct invoeren en wijzigen van Identiteiten.

3.2.3 Aanvragen, intrekken en goedkeuren van Procesrollen en autorisaties, en beheer van mandaten

Zie bijlage 13 Functioneel Ontwerp: Hoofdstuk 3 Aanvragen en goedkeuren.

Nr.	Omschrijving
E13	De gebruikersinterfaces van de Oplossing (inclusief beheer-, selfservice- en Rolhouderportalen) zijn volledig webgebaseerd.
E14	De Oplossing maakt geen gebruik van browserplug-ins of lokale softwarecomponenten en is geschikt voor alle gangbare browsers (waaronder Chrome, Edge, Firefox en Safari).
E15	De Oplossing biedt afzonderlijke gebruikersportalen voor Medewerkers en Rolhouders, waarin zij – passend bij hun verantwoordelijkheden – Procesrollen en los aan te vragen Autorisaties kunnen aanvragen, toekennen en intrekken. Aanvragen van Procesrollen en los aan te vragen Autorisaties doorlopen een configureerbaar goedkeuringsproces, waarbij wordt bepaald welke Rolhouders betrokken zijn bij de beoordeling en besluitvorming. De Oplossing ondersteunt tevens dat bevoegde Rolhouders, zoals Proceseigenaren en Autorisatie-eigenaren, Procesrollen en Autorisaties direct kunnen toekennen zonder voorafgaande goedkeuring. Intrekkingen van Procesrollen en los aan te vragen Autorisaties worden direct doorgevoerd, zonder voorafgaande goedkeuring.
E16	De Oplossing ondersteunt het proces van aanvragen, goedkeuren, toekennen en intrekken van Procesrollen en Autorisaties door het verzenden van statusberichten aan de aanvrager en/of de Medewerker voor wie de aanvraag is gedaan. Deze statusberichten bevatten de actuele status en, indien van toepassing, de motivatie, inclusief de naam van de Proces- of Autorisatie-eigenaar die het besluit heeft genomen.
E17	De Oplossing logt elke stap in het proces van aanvragen, goedkeuren, toekennen en intrekken van Procesrollen en Autorisaties, en maakt deze informatie inzichtelijk voor functioneel beheer, zodat volledige traceerbaarheid, controleerbaarheid en auditbaarheid van Autorisaties is geborgd en ongewenste of verouderde Autorisaties worden voorkomen.
E18	De Oplossing ondersteunt dat Leidinggevenden tot minimaal 14 dagen vóór de startdatum van een nieuwe Medewerker Procesrollen en los aan te vragen Autorisaties voor deze Medewerker kunnen aanvragen, zodat alle benodigde Autorisaties op de startdatum actief zijn.

W3	**Aanvragen, goedkeuren, toekennen en intrekken van Procesrollen en Autorisaties, en beheer van mandaten** Opdrachtgever wenst dat de Oplossing Medewerkers en Rolhouders ondersteunt in het proces van het aanvragen, goedkeuren, toekennen en intrekken van Procesrollen en los aan te vragen Autorisaties, en dat dit proces transparant, veilig, consistent en beheersbaar verloopt. Deze wens richt zich in het verlengde van eis E17 op de gebruiksvriendelijkheid en beheersbaarheid van de inrichting en werking daarvan. Daarbij is het proces ingericht als selfservice en rolgebaseerde regie, waarbij na goedkeuring de toekenning en intrekking van Autorisaties automatisch en zonder handmatige tussenkomst wordt uitgevoerd richting de Doelsystemen. De goedkeuringsflows zijn configureerbaar door functioneel beheer. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Aanvragen, goedkeuren, toekennen en intrekken van Procesrollen en Autorisaties, en beheer van mandaten' en ga daarbij in ieder geval in op: **A. Navigatie en vindbaarheid van aanvraagbaar aanbod** Beschrijf hoe de Oplossing Medewerkers en Rolhouders ondersteunt met een intuïtieve gebruiksvriendelijke navigatie- en zoekfunctionaliteit, waarmee Procesrollen en los aan te vragen Autorisaties eenvoudig vindbaar en aan te vragen zijn. Beschrijf tevens hoe het aanvraagbare aanbod dynamisch wordt afgestemd op de Identiteitscontainer van de Medewerker, zodat uitsluitend de voor de betreffende Organisatie relevante Procesrollen en Autorisaties zichtbaar en beschikbaar zijn. **B. Configureerbaarheid en beheer van goedkeuringsproces** Beschrijf hoe de Oplossing het inrichten, aanpassen en beheren van goedkeuringsprocessen ondersteunt, zodanig dat functioneel beheer deze processen zelfstandig kan configureren zonder technische tussenkomst. Beschrijf daarnaast hoe functioneel beheer laagdrempelig inzicht heeft de de logging van alle acties die plaats vinden binnen het goedkeuringsproces, zodat eenvoudig kan worden vastgesteld wat er is gebeurd en waar eventuele acties of mutaties zich bevinden. **C. Regie en inzicht voor Medewerkers** Beschrijf hoe Medewerkers een compleet en samenhangend overzicht krijgen van de HR-attributen, Procesrollen en Autorisaties waarover zij beschikken, inclusief de status van lopende aanvragen. Beschrijf daarnaast hoe Medewerkers Procesrollen en los aan te vragen Autorisaties op een intuïtieve en gebruiksvriendelijke kunnen aanvragen of intrekken (zie ook *A.*). Zodanig dat Medewerkers in staat worden gesteld vast te stellen over welke HR-attributen, Procesrollen en Autorisaties zij beschikken, welke wijzigingen lopen en in hoeverre deze aansluiten bij hun werkzaamheden.

	D. Regie en inzicht voor Leidinggevenden Beschrijf hoe Leidinggevenden een compleet en samenhangend overzicht krijgen van de Medewerkers waarvoor zij HR-verantwoordelijk zijn, met per Medewerker inzicht in de HR-attributen, Procesrollen en Autorisaties waarover deze beschikt. Beschrijf daarnaast hoe Leidinggevenden op een intuïtieve en gebruiksvriendelijke wijze Procesrollen en los aan te vragen Autorisaties voor Medewerkers kunnen aanvragen of intrekken (zie ook A.). Zodanig dat Leidinggevenden in staat worden gesteld vast te stellen over welke HR-attributen, Procesrollen en Autorisaties een Medewerker beschikt, welke wijzigingen lopen en in hoeverre deze aansluiten bij de werkzaamheden van de Medewerker. **E. Regie en inzicht van Proceseigenaren en Autorisatie-eigenaren:** Beschrijf hoe Proceseigenaren en Autorisatie-eigenaren (voor los aan te vragen Autorisaties) een compleet en samenhangend overzicht krijgen van de Procesrollen en Autorisaties waarvoor zij verantwoordelijk zijn, met per Procesrol of Autorisatie inzicht in welke Medewerkers hierover beschikken. Beschrijf daarnaast hoe Proceseigenaren en Autorisatie-eigenaren op een intuïtieve en gebruiksvriendelijke wijze Procesrollen en Autorisaties voor Medewerkers kunnen toekennen of intrekken, en aanvragen kunnen goedkeuren of weigeren, waarbij een motivatie wordt vastgelegd (zie ook *A.*). Zodanig dat Proceseigenaren en Autorisatie-eigenaren in staat worden gesteld vast te stellen welke Procesrollen en Autorisaties actief zijn, voor wie deze gelden en in hoeverre deze aansluiten bij de beoogde werkzaamheden. **F. Mandatering van bevoegdheden (goedkeuren en beheer)** Beschrijf hoe het 'regie en inzicht' van Rolhouders tijdelijk kan worden gemandateerd aan maximaal twee Medewerkers binnen dezelfde Identiteitscontainer. Beschrijf daarnaast hoe functioneel beheer te allen tijde een actueel en volledig overzicht kan raadplegen van de mandateringen, waarin per Rolhouder inzichtelijk is aan welke Medewerkers bevoegdheden zijn gemandateerd en wat de einddatum van deze mandateringen is. Waarbij de handelingen van Rolhouders rondom mandateren worden gelogd en raadpleegbaar zijn.

3.2.4 Autorisatiebeheer

Zie bijlage 13 Functioneel Ontwerp: Hoofdstuk 4 IAM-beheer.

Nr.	Omschrijving
E19	De Oplossing ondersteunt het beheren van Autorisaties, waarbij Autorisaties kunnen worden aangemaakt, gewijzigd en verwijderd. Een Autorisatie bestaat uit één of meerdere Resources en kunnen aan Autorisaties worden toegevoegd en verwijderd. De Oplossing biedt inzicht in de relaties tussen Autorisaties, Procesrollen en HR-attributen, zodat per Autorisatie zichtbaar is waar deze onderdeel van uitmaakt.
E20	De Oplossing ondersteunt het beheren (aanmaken, wijzigen en verwijderen) van Resources, waarbij iedere Resource is gekoppeld aan een Doelsysteem. Het Doelsysteem bepaalt de wijze van provisioning. De Oplossing ondersteunt daarbij de volgende vormen van provisioning: • Active Directory: geautomatiseerde provisioning door het toevoegen en verwijderen van Medewerkers aan respectievelijk uit AD-groepen. • Overige Doelsystemen (TOPdesk en e-mail): provisioning door middel van een opdracht (ticket-based) ten behoeve van verdere verwerking.

E21	De Oplossing is in staat om bij het toekennen van Autorisaties een delta te bepalen ten opzichte van de reeds toegekende Resources, waarbij op het niveau van individuele Resources wordt vastgesteld waarover een Medewerker reeds beschikt. Indien sprake is van overlap, worden uitsluitend de Resources die onderdeel uitmaken van de delta (een Medewerker nog niet beschikt) opgenomen in de provisioningopdracht richting het Doelsysteem
E22	De Oplossing ondersteunt het beheren van HR-attributen, Procesrollen en los aan te vragen Autorisaties, waaronder het aanmaken, wijzigen en deactiveren daarvan. Bij het aanmaken van een Procesrol of een los aan te vragen Autorisatie wordt deze gekoppeld aan een verantwoordelijke Proceseigenaar respectievelijk Autorisatie-eigenaar t.b.v. het goedkeuringsproces (zie ook eis *E15*). De Oplossing ondersteunt daarbij dat Autorisaties kunnen worden gekoppeld en ontkoppeld aan zowel Procesrollen als HR-attributen. Bij deactivering van een Procesrol of HR-attribuut worden de bijbehorende Autorisaties automatisch ingetrokken. Daarnaast biedt de Oplossing functioneel beheer een actueel en volledig overzicht van de Medewerkers en de HR-attributen, Procesrollen en Autorisaties waarover zij beschikken.
E23	De Oplossing waarborgt volledige transparantie, controleerbaarheid en auditeerbaarheid van het autorisatiebeheer. Alle wijzigingen in Resources, Autorisaties, Procesrollen en HR-attributen worden vastgelegd, inclusief de doorwerking van deze wijzigingen in de toegekende Autorisaties op het niveau van Medewerkers. De logging maakt inzichtelijk welke handelingen zijn uitgevoerd, welke wijzigingen zijn doorgevoerd en welke impact deze hebben gehad op de Autorisaties van Medewerkers.
W4	**Beheer van autorisatiestructuren en provisioning** Opdrachtgever wenst dat de Oplossing voorziet in een laagdrempelige en gebruiksvriendelijke beheerinterface voor autorisatiebeheer. Binnen deze interface kunnen Resources, Autorisaties, Procesrollen en HR-attributen eenvoudig worden ingericht, beheerd en onderhouden. Autorisaties vormen hierbij de bouwstenen en bestaan uit één of meerdere Resources. Procesrollen en HR-attributen bestaan uit één of meerdere Autorisaties. Het toekennen of intrekken van Autorisaties leidt tot provisioning naar Doelsystemen. Voor Active Directory vindt dit geautomatiseerd plaats, terwijl voor Topdesk en e-mail gebruik wordt gemaakt van ticket-based provisioning. De Oplossing ondersteunt volledige transparantie, herleidbaarheid en controleerbaarheid van het autorisatiebeheer, waarbij alle wijzigingen in Recources, Autorisaties, Procesrollen en HR-attributen inzichtelijk en herleidbaar zijn per Gebruiker, ten behoeve van analyse, kwaliteitscontrole en aantoonbare naleving van security- en compliance-eisen. De Oplossing ondersteunt volledige transparantie, herleidbaarheid en controleerbaarheid van het autorisatiebeheer. Wijzigingen in Resources, Autorisaties, Procesrollen en HR-attributen zijn inzichtelijk en herleidbaar tot op Gebruikersniveau m.b.t. de doorwerking van ingetrokken of toegekende Autorisaties, ten behoeve van analyse en kwaliteitscontrole. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens ‘Beheer van autorisatiestructuren en provisioning’ en ga daarbij in ieder geval in op: **A. Inrichting en beheer van autorisatiestructuren** Beschrijf hoe binnen de Oplossing Resources, Autorisaties, Procesrollen en HR-attributen op een laagdrempelige en gebruiksvriendelijke worden ingericht, beheerd en onderhouden.

	B. Impactanalyse en wijzigingsverwerking bij autorisatieaanpassingen Beschrijf hoe de Oplossing vooraf inzicht biedt in de impact van wijzigingen in Resources, Autorisaties, Procesrollen en HR-attributen en op welke wijze deze impact kan worden beoordeeld, goedgekeurd of tegengehouden. **C. Hergebruik en standaardisatie van een basisautorisatie in Autorisaties van een applicatie** Beschrijf hoe de Oplossing ondersteunt dat Autorisaties hiërarchisch of genest kunnen worden opgebouwd. Hierbij wordt bedoeld dat een basisautorisatie (een applicatieaccount en bijbehorende basis-AD-groepen) eenmalig kunnen worden ingericht en vervolgens automatisch worden opgenomen in alle functionele Autorisaties van diezelfde applicatie, zodat deze niet afzonderlijk per Autorisatie of Procesrol hoeven te worden beheerd.
W5	**Bundelticketmechanisme voor ticket-based Doelsystemen** Opdrachtgever wenst dat de Oplossing voor Doelsystemen zonder directe geautomatiseerde provisioning (ticket-based) een bundelticketmechanisme ondersteunt richting Functioneelbeheergroepen. De Oplossing genereert middels een eenmalig te maken script per applicatie (Logisch Doelsysteem) en per verantwoordelijke Functioneelbeheergroep Bundeltickets, gericht op het verwerken van autorisatiewijzigingen (toekennen en intrekken van Resources). Deze Bundeltickets bevatten de relevante wijzigingen (delta) ten opzichte van de bestaande situatie (zie ook *E21*) Zowel de wijziging als de reeds toegekende rechten worden opgenomen, zodat een volledig en actueel beeld ontstaat van de autorisatiesituatie per Gebruiker. Het bundelticketmechanisme draagt bij aan consistente, controleerbare en efficiënte verwerking van autorisatiewijzigingen binnen applicaties (Logisch Doelsystemen) waar handmatige verwerking plaatsvindt. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Bundelticketmechanisme ticket-based Doelsystemen' en ga daarbij in ieder geval in op: **A.** Beschrijf hoe de Oplossing Bundeltickets genereert per applicatie voor een Functioneelbeheergroep richting Topdesk voor het toekennen of intrekken van Resources, en hoe binnen deze Bundeltickets de relevante wijzigingen (delta) en de actuele situatie worden opgenomen. **B.** Beschrijf hoe de informatie in het Bundelticket overzichtelijk, gebruiksvriendelijk en begrijpelijk wordt gepresenteerd, zodat functioneel beheerders snel kunnen vaststellen welke wijzigingen moeten worden doorgevoerd; **C.** Beschrijf hoe eenmalig een script gemaakt kan worden en vervolgens geautomatiseerd tickets voor nieuwe applicaties verstuurd worden naar Topdesk zonder tussenkomst van een functioneel beheer.

3.2.5 Integraties

Voor een overzicht van de informatie die er gesynchroniseerd moet worden zie bijlage 13 Functioneel Ontwerp en daarbinnen bijlage 3 (AD), bijlage 4 (Youforce) en bijlage 5 (Topdesk).

<table>
<tr><th>Nr.</th><th>Omschrijving</th></tr>
<tr><td>E24</td><td>De Oplossing ondersteunt dat koppelingen met systemen kunnen worden gerealiseerd via een door de Opdrachtgever voorgeschreven ESB en/of API-gateway (zoals OpenTunnel), indien dit een vereiste is om systemen te ontsluiten.
De Oplossing stelt geen beperkingen aan het gebruik van dergelijke integratievoorzieningen en is in staat om via deze voorzieningen te communiceren met andere systemen.
De beveiliging van koppelingen wordt ingericht conform de daarvoor geldende eisen en in afstemming met de Opdrachtgever.</td></tr>
<tr><td>E25</td><td>De Oplossing moet zorgen voor een betrouwbare en consistente verwerking van gegevensuitwisseling tussen de Oplossing en de gekoppelde systemen. Wijzigingen en synchronisaties moeten correct en volledig worden doorgevoerd.</td></tr>
<tr><td>E26</td><td>De Oplossing moet voorzien in mechanismen voor automatische herverwerking (retry-mechanismen), waarbij bij een fout of time-out de verwerking automatisch opnieuw wordt uitgevoerd totdat deze succesvol is afgerond of totdat een beheerbare en inzichtelijke foutmelding wordt gegenereerd.</td></tr>
<tr><td>E27</td><td>De Oplossing moet alle integratie-, synchronisatie- en provisioning-acties loggen, inclusief status, tijdstip en eventuele foutmeldingen actief signaleren, zodat beheer tijdig kan ingrijpen bij mislukte of onvolledige verwerkingen en herstelacties kan uitvoeren.</td></tr>
<tr><td>E28</td><td>De Opdrachtnemer levert de adapter en verzorgt de werkzaamheden die aan de kant van de Oplossing noodzakelijk zijn om de koppeling te laten functioneren:
<table>
<tr><th>Systeem</th><th>Koppeling</th><th>Minimale functionaliteit</th></tr>
<tr><td>SSO</td><td>ADFS / Azure AD (Entra Id)</td><td>De Oplossing ondersteunt de volgende functionaliteiten:
- SSO-authenticatie via ADFS en Azure AD (Entra id)
- Uitvoeren van de authenticatie op basis van AD-accounts (username/password) of Azure AD-identiteit.</td></tr>
<tr><td>HR-systeem
Voor Zaanstad betreft dit YouForce.</td><td>BINT-bestand = Beaufort Interface bestand (technisch XML) en in de toekomst mogelijk Rest-Api</td><td>De Oplossing ondersteunt de volgende functionaliteiten:
- Synchronisatie van Medewerkers en bijbehorende Identiteitskenmerken vanuit het HR-bronsysteem naar de IAM-persoonskaart.
Zie bijlage 13 Functioneel ontwerp en daarbinnen bijlage 4 voor een overzicht van de Identiteitskenmerken.</td></tr>
<tr><td>Doelsystemen:</td><td></td><td></td></tr>
<tr><td>1. ITSM
Voor Zaanstad betreft dit Topdesk.</td><td>Rest-Api’s</td><td>De Oplossing ondersteunt de volgende functionaliteiten:
- aanmaken Topdesk-persoonskaart eerste Contract in IAM (5);</td></tr>
</table>
</td></tr>
</table>

			- inactiveren Topdesk-persoonskaart bij einde Contract en verwijderen Domeinaccount en emailadres (6); - reactiveren van de Topdesk-persoonskaart bij nieuw Contract en vastleggen nieuw Domeinaccount en emailadres (7); - Synchroniseren telefoonnummers van Topdesk-persoonskaart naar de IAM-persoonskaart (8); - Synchroniseren Identiteitskenmerken vanuit de IAM-persoonskaart naar het Topdesk-persoonskaart (9); - Wijzigingssjabloon aanmaken met een ticket voor functioneerbeheergroepen. *Voor de nummering en een schematische weergave van de werking zie in Bijlage 13 Functioneel ontwerp figuur 5.* *Voor de informatie die gesynchroniseerd moet worden zie in Bijlage 13 Functioneel Ontwerp en daarbinnen bijlage 5.*
	2. Email	Voorkeur heeft SPF+ DKIM boven Exchange (OAD2): Oplossing verstuurd mail vanuit eigen mailserver uit naam van Zaanstad	De Oplossing ondersteunt e-mailverzending namens Zaanstad, via een eigen mailvoorziening of de gemeentelijke mailomgeving, inclusief TLS, correcte SPF/DKIM/DMARC-configuratie en benodigde authenticatie. Verzend- en reply-adres zijn configureerbaar. De Oplossing ondersteund het mailen: - van (bundel)tickets naar een algemene mailbox; - van signaleringen en notificaties aan Leidinggevenden en/of Proceseigenaren bij lifecycle-gebeurtenissen, zoals instroom, doorstroom en uitstroom; - van status- en attenderings-meldingen aan Medewerkers bij goedkeuring, afwijzing en statuswijzigingen van aanvragen. - Van welkomstboodschappen op de eerste werkdag.

	3. Active Directory (AD)	Beveiligde LDAP(S)-verbinding + Service account. Indien de Oplossing als SaaS wordt geleverd, wordt Microsoft Entra ID als koppellaag tussen de Oplossing en Active Directory geplaatst, zodat de keten Oplossing - Microsoft Entra ID - Active Directory wordt gevolgd. Geautomatiseerde provisioning naar Active Directory blijft in dat geval onderdeel van de vereiste functionaliteit. Bij een On-Premise-levering mag voor de beveiligde LDAP(S)-koppeling en voor de functionaliteit uit eis 8 een specifiek technisch AD-serviceaccount worden gebruikt, dat uitsluitend voor die koppeling wordt gebruikt en niet over meer rechten beschikt dan noodzakelijk	De Oplossing ondersteunt de volgende functionaliteiten: • Aanmaken AD-account met een Domeinaccount en e-mailadres bij elk nieuw IAM-Contract (1). • Intrekken en verwijderen (clearen) van AD-account (Domeinaccount en emailadres) en homedirectory binnen een vastgestelde termijn (bijvoorbeeld 30 dagen) na einde dienstverband (2). • Synchroniseren telefoonnummers van in het AD-account basis van wijzigingen in de IAM-persoonskaart (3). • Toevoegen en verwijderen van Medewerkers aan/uit directory-groepen op basis van autorisatietoekenningen. *Voor de nummering en een schematische weergave van de werking zie in Bijlage 13 Functioneel ontwerp figuur 5.* *Voor de informatie die gesynchroniseerd moet worden zie in Bijlage 13 Functioneel Ontwerp en daarbinnen bijlage 3.* Daarnaast biedt de Oplossing volledig inzicht in: • alle directory-groepen en vertaald naar Resources; • de Gebruikers die aan deze groepen zijn gekoppeld.
	Datapakhuis	Databestanden SFTP of Data-API	De Oplossing ondersteunt dat alle data beschikbaar gesteld wordt via één van de twee varianten: **1. Datadumps via SFTP** - Data wordt beschikbaar gesteld in afzonderlijke databestanden per dataset, in de formaten CSV of XLS(X).

			- Bestanden worden dagelijks geactualiseerd en aangeboden via een beveiligde SFTP-server van Zaanstad of van de leverancier. - Zaanstad initieert het datatransport via een pull-mechanisme. - Datadumps bevatten de volledige populatie aan records per dataset. **2. Data-API** - De Oplossing biedt een data-API waarmee Zaanstad periodiek, minimaal één keer per dag, alle tabellen met de volledige dataset kan ophalen. - De API ondersteunt stabiele en veilige gegevensoverdracht. - Het volledig ophalen van alle data via de API kan plaatsvinden binnen een tijdsbestek van maximaal 5 minuten.
W6	**Integraties** Opdrachtgever wenst dat de Oplossing robuuste en toekomstbestendige integraties ondersteunt met het bestaande en toekomstige IT-landschap, waarbij betrouwbaarheid, beheersbaarheid en flexibiliteit centraal staan. De Oplossing waarborgt een consistente en controleerbare verwerking van identiteiten en Autorisaties richting Doelsystemen, inclusief het omgaan met tijdelijke uitval, foutafhandeling en herstel van synchronisaties. Daarnaast ondersteunt de Oplossing een gestructureerde en beheersbare implementatie en inpassing van integraties, in samenwerking met de Opdrachtgever en eventuele derde partijen, passend binnen het gevraagde leveringsmodel (SaaS en/of on-premise). Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Integraties' en ga daarbij in ieder geval in op: **A. Retry-mechanisme bij synchronisatieproblemen** Beschrijf hoe de Oplossing omgaat met het herstellen van synchronisatieprocessen wanneer Doelsystemen tijdelijk niet beschikbaar zijn, zowel gepland als ongepland. Ga daarbij in op: • de wijze waarop mislukte verwerkingen worden gedetecteerd en geregistreerd • retry- en/of wachtrijmechanismen (queueing) • maximale hersteltermijnen en gedrag bij langdurige uitval • inzicht en sturing voor beheer bij herstelacties **B. Implementatie van koppelingen en samenwerking** Beschrijf hoe koppelingen met externe systemen worden gerealiseerd en hoe een succesvolle implementatie wordt geborgd. Ga daarbij in op: • de gehanteerde werkwijze en fasering (bijvoorbeeld ontwerp, realisatie, test en inbeheername)		

- de rolverdeling en samenwerking tussen Opdrachtnemer, gemeente en betrokken derde partijen
- de wijze waarop afhankelijkheden en risico's in de keten worden beheerst

C. Ontwerp en inpassing van integraties in de IT-omgeving

Beschrijf op welke wijze de Opdrachtnemer, in samenwerking met de Opdrachtgever en relevante derde partijen, invulling geeft aan het ontwerp van integraties tussen de Oplossing en het bestaande IT-landschap, rekening houdend met het gevraagde leveringsmodel (SaaS en/of on-premise).
Ga daarbij in op:

- de gehanteerde aanpak voor het opstellen en uitwerken van functionele en technische ontwerpen;
- voorbeelden van functionele en technische ontwerpen en/of referentie-architecturen uit vergelijkbare implementaties;
- een beschrijving van de functionele werking van de Oplossing (productlogica), inclusief de samenhang tussen identiteiten, Autorisaties, lifecycleprocessen en integraties;
- de wijze waarop de samenhang met de bestaande architectuur en het integratielandschap wordt geborgd;
- de rolverdeling tussen Opdrachtnemer, Opdrachtgever (waaronder architecten en beheerders) en eventuele derden;
- de mate waarin standaardisatie, herbruikbaarheid en beheersbaarheid van integraties worden ondersteund;
- Indien de Oplossing als SaaS wordt geleverd, beschrijf op welke wijze de Opdrachtnemer de hosting van de Oplossing heeft ingericht, inclusief de geografische locatie(s) en de betrokken hosting- of cloudleverancier, en welke consequenties dit heeft voor de integratie met het bestaande IT-landschap;

De mate waarin deze aanpak concreet, onderbouwd en aantoonbaar uitvoerbaar is binnen de gevraagde implementatievorm, wordt meegewogen in de beoordeling.

D. Integratie met Microsoft Entra ID

De gemeente maakt gebruik van een hybride directorylandschap waarbij het merendeel van de identiteiten en Autorisaties via Active Directory wordt beheerd en gesynchroniseerd met Microsoft Entra ID.
Voor een beperkt deel van de Autorisaties (bijvoorbeeld specifieke beheerrechten) vindt toekenning momenteel rechtstreeks plaats in Microsoft Entra ID, waarbij deze niet via de bestaande synchronisatie wordt ontsloten.
De gemeente wenst inzicht in de mogelijkheden om het beheer van deze Autorisaties verder te automatiseren en te integreren binnen de Oplossing.
Beschrijf:

- op welke wijze de Oplossing integratie met Active Directory en Microsoft Entra ID ondersteunt;
- in hoeverre de Oplossing het beheer van accounts en Autorisaties binnen het hybride landschap ondersteunt, inclusief de volledige lifecycle (aanmaken, wijzigen, verwijderen) en Autorisaties buiten de standaard synchronisatie;
- in hoeverre de Oplossing ondersteuning biedt voor het beheer van toegangsgegevens (zoals wachtwoorden en One-Time Passwords) en bijdraagt aan het verminderen van handmatige beheerhandelingen.

4 Niet functionele eisen

4.1 Security

4.1.1 Logging & Audit

Nr.	Omschrijving
E29	De Oplossing logt alle relevante gebeurtenissen volledig, reproduceerbaar en herleidbaar, waarbij loggegevens voldoen aan eisen van kwaliteit, betrouwbaarheid en bruikbaarheid voor monitoring, audit en beveiligingsdoeleinden. Dit omvat minimaal: Scope van logging: • Alle systeemwijzigingen (automatisch en handmatig), volledig vastgelegd en reproduceerbaar, conform de loggingvereisten zoals beschreven bij de functionele eisen *E7, E8, E17, E23, E27;* • Alle inlogpogingen van Gebruikers en systemen (geslaagd en mislukt), waarbij minimaal wordt vastgelegd: accountnaam, locatie, tijdstip en resultaat van de poging; • Alle data-uitwisselingen via koppelingen (indien van toepassing), waarbij minimaal wordt vastgelegd: account- of systeemnaam, tijdstip, soort data, transportnummer en resultaat van de uitwisseling; Kwaliteit en inhoud van logging: • Loggegevens bevatten minimaal: gebeurtenis; resultaat van de handeling; tijdstip (timestamp); herleidbaarheid tot Gebruiker, proces of handeling; Loggegevens zijn niet muteerbaar (onveranderbaar/audit-proof). • Loggegevens zijn leesbaar zonder aanvullende tooling; • Logging heeft geen negatieve invloed op de performance van de Oplossing; • Logging vindt minimaal plaats op gebruikers-, object- (zoals dossier-) en veldniveau; • Loggegevens zijn exporteerbaar ten behoeve van externe analyse (SIEM-Oplossingen zoals Splunk); • Mogelijkheid tot rapportage op basis van loggegevens.
E30	Indien de Oplossing als SaaS wordt geleverd, waarborgt het dat loggegevens gedurende een passende periode beschikbaar blijven voor incidentonderzoek, compliance, audit en rapportage, waarbij bewaartermijnen risicogebaseerd worden toegepast. Dit omvat minimaal: Bewaartermijnen van loggegevens: • Logbestanden worden minimaal 2 jaar bewaard, tenzij anders overeengekomen of noodzakelijk (bijvoorbeeld bij een (vermoed) beveiligingsincident); • Voor security- en risicoanalyse wordt, op basis van een expliciete en aantoonbare risicoafweging, een minimale bewaartermijn van 5 jaar toegepast; Randvoorwaarden voor bewaartermijnen: • Loggegevens blijven gedurende de bewaartermijn volledig, integer en beschikbaar voor analyse en audit; • Loggegevens blijven raadpleegbaar en reproduceerbaar gedurende de volledige bewaartermijn; • Verlenging van bewaartermijnen is mogelijk indien dit noodzakelijk is voor incidentonderzoek, juridische verplichtingen of compliance-doeleinden.

E31	Indien de Oplossing als SaaS wordt geleverd, waarborgt deze dat bevoegde Medewerkers loggegevens efficiënt kunnen raadplegen, doorzoeken en analyseren, en dat logging zodanig is ingericht dat beheeracties afzonderlijk en controleerbaar inzichtelijk zijn. Dit omvat minimaal: Toegankelijkheid en doorzoekbaarheid: • Logbestanden zijn volledig en integraal doorzoekbaar; • De Oplossing beschikt over filtermogelijkheden om loggegevens gericht te kunnen analyseren; • Loggegevens kunnen zodanig worden geraadpleegd dat efficiënte analyse en interpretatie mogelijk is; Logging van beheeracties: • Alle beheeracties worden gelogd en logisch gescheiden van gebruikerslogins, zodat onderscheid gemaakt kan worden tussen regulier gebruik en beheerhandelingen. Export en analyse: • Alle loggingtabellen kunnen minimaal dagelijks worden geëxporteerd ten behoeve van nadere analyse.

4.1.2 Security & Compliance

Nr.	Omschrijving
E32	Continuïteit van certificering en verantwoording: • Opdrachtnemer waarborgt gedurende de volledige looptijd van de overeenkomst dat zowel Opdrachtnemer als de door hem ingeschakelde softwareleverancier, cloudleverancier(s) en/of hostingpartij(en) blijven voldoen aan de certificeringen die in de Offerteleidraad zijn vereist en die bij inschrijving zijn overgelegd. • Opdrachtnemer stelt jaarlijks, en op eerste verzoek van Opdrachtgever, een geldige assuranceverklaring (SOC 2 Type II of ISAE 3000 Type II) van een Register EDP-Auditor over de softwareleverancier beschikbaar. Deze verklaring dient aan te tonen dat blijvend wordt voldaan aan de overeengekomen beveiligings- en beheersingsmaatregelen. Verantwoordelijkheid Opdrachtnemer: • Opdrachtnemer overlegt op verzoek van Opdrachtgever de relevante certificeringen en verstrekt jaarlijks de vereiste assuranceverklaring (SOC 2 en/of ISAE 3000) van de softwareleverancier. • Opdrachtnemer informeert Opdrachtgever onverwijld over wijzigingen, schorsingen, intrekkingen of het verlopen van certificeringen die van invloed kunnen zijn op de overeengekomen beveiligings- en beheersingsmaatregelen.
E33	De Cyber Beveiligingswet (CBW), de BIO2 en de maatregelen uit de meest actuele versie van de "ICT-beveiligingsrichtlijnen voor webapplicaties" van het Nationaal Cyber Security Centrum (NCSC), geldt als basis voor informatiebeveiliging. Indien de Oplossing als SaaS wordt geleverd dan is deze volledig in lijn met BIO2, NIS2 en AVG.
E34	Indien de Oplossing als SaaS wordt geleverd dan voldoet deze aantoonbaar aan de meest actuele OWASP richtlijnen: https://owasp.org/Top10/.
E35	Indien de Oplossing als SaaS wordt geleverd dan voert Opdrachtnemer minimaal jaarlijks een onafhankelijke penetratietest uit op de applicatie en de bijbehorende infrastructuur. Opdrachtgever ontvangt een samenvatting van de bevindingen, verbetermaatregelen en opvolging. Volledige penetratietestrapporten hoeven niet te worden verstrekt.
E36	De Opdrachtgever heeft het right to audit (o.a. door het laten uitvoeren van pentesten) waaraan de Opdrachtnemer zijn volledige medewerking verleent.

heeft verwijderd: Register EPD-Auditor

heeft verwijderd: dan voldoet deze aantoonbaar aan de meest actuele

E37	De Opdrachtnemer waarborgt een snelle detectie en beheersing van beveiligingsincidenten om schade te beperken en impact te minimaliseren. Dit omvat minimaal: Beheer en respons op beveiligingsincidenten: • De Opdrachtnemer beschikt over een aantoonbaar en uitgewerkt protocol voor het detecteren, beheersen en afhandelen van beveiligingsincidenten en cyberaanvallen, inclusief maatregelen om schade te beperken en herstel gestructureerd en adequaat uit te voeren; • Opdrachtnemer maakt inzichtelijk hoe kwetsbaarheden in de software tijdig worden gesignaleerd, geanalyseerd en verholpen, inclusief het beheer daarvan gedurende de ontwikkel- en onderhoudsfase. Meldplicht en communicatie: • De Opdrachtnemer meldt beveiligingsincidenten en relevante kwetsbaarheden die impact hebben (of kunnen hebben) op de Oplossing of gegevensverwerking onverwijld aan Opdrachtgever, inclusief aard, impact en genomen of voorgenomen maatregelen;
E38	Indien de Oplossing als SaaS wordt geleverd dan waarborgt deze dat e-mailverkeer en digitale communicatie adequaat worden beveiligd tegen spoofing, phishing, malware en afluisteren, conform geldende standaarden voor overheden. Dit omvat minimaal: E-mail- en communicatiebeveiliging: • Bij het verzenden en ontvangen van e-mails wordt gebruik gemaakt van alle relevante, voor overheden verplichte beveiligingsstandaarden, waaronder in ieder geval SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE, IPv4 en IPv6, HTTPS en HSTS; • De correcte implementatie van deze standaarden is aantoonbaar en toetsbaar via gangbare validatietools (zoals www.internet.nl); Beveiliging van content en bestanden: • Bestanden die worden geüpload, worden gecontroleerd op malafide code, waaronder virussen, trojans en spam.
E39	Indien de Oplossing als SaaS wordt geleverd dan ondersteunt deze de Zero Trust-principes van de Opdrachtgever en maakt integraal gebruik van de centrale identity provider (IdP), waarbij uitsluitend geautoriseerde Gebruikers en apparaten toegang krijgen. Dit omvat minimaal: Identity en authenticatie: • De Oplossing werkt uitsluitend met geautoriseerde Gebruikers en apparaten; • De Oplossing maakt integraal gebruik van de identity provider (IdP) van de Opdrachtgever voor authenticatie; • De Oplossing vereist geen lokale wachtwoorden of bypass-mechanismen; Single Sign-On en standaarden: • De Oplossing ondersteunt standaard centrale authenticatie via Single Sign-On (SSO); • Bij voorkeur wordt gebruikgemaakt van OpenID Connect (OIDC) en OAuth 2.0; • Optioneel wordt SAML 2.0 ondersteund indien OIDC niet beschikbaar is; Beleid en integratie: • De Oplossing ondersteunt volledig de door de Opdrachtgever ingestelde Conditional Access Policies; • De Oplossing mag geen aanvullende of afwijkende authenticatie- of beveiligingsmechanismen afdwingen die in conflict zijn met deze policies.

E40	Indien de Oplossing als SaaS wordt geleverd dan waarborgt deze dat toegang tot systemen en gegevens plaatsvindt op basis van persoonlijke accounts en moderne, door de Opdrachtgever aangestuurde authenticatiemechanismen. Dit omvat minimaal: Persoonlijke accounts en beheer: • Iedere Gebruiker, inclusief beheerders, gebruikt een persoonlijk account dat via de IdP wordt gevalideerd; • Generieke not-named accounts zijn niet toegestaan; • Serviceaccounts voor koppelingen worden uitsluitend via de IdP ingericht (bijv. service principals); • Lokale accounts zijn standaard uitgeschakeld en uitsluitend toegestaan voor noodprocedures (break-glass), onder strikte logging en monitoring; Moderne authenticatie: • De Oplossing ondersteunt moderne authenticatieprincipes zoals door de IdP van de Opdrachtgever afgedwongen; • De Oplossing ondersteunt Multi-Factor Authentication (MFA) zoals aangestuurd vanuit de IdP; • De Oplossing ondersteunt het toepassen van phishing-resistente authenticatie (zoals FIDO2/passkeys) als aanvullende factor (step-up authentication) bij hoog-risico toepassingen; • De Oplossing kan signalen uit risk-based access verwerken en benutten voor aanvullende beveiligingsmaatregelen; Randvoorwaarde: • Single Sign-On is het uitgangspunt; de Opdrachtnemer hoeft zelf geen MFA of FIDO2 te leveren, maar de Oplossing moet dit wel ondersteunen en mag geen eigen authenticatie afdwingen die hiermee conflicteert.
E41	• • • • • Vervallen. Zie het antwoord op vraag 5 van de 1e Nota van Inlichtingen.
E42	Indien de Oplossing als SaaS wordt geleverd dan waarborgt Opdrachtnemer dat authenticatiegegevens, cryptografische sleutels en andere gevoelige secrets zodanig worden verwerkt en beschermd dat deze niet toegankelijk zijn voor de Opdrachtnemer en uitsluitend onder strikte voorwaarden kunnen worden gebruikt. Dit omvat minimaal: Bescherming van secrets: • Wachtwoorden worden uitsluitend opgeslagen als gehashte en gesalte waarden (bijvoorbeeld bcrypt of argon2); • Private keys van FIDO2/WebAuthn worden nooit opgeslagen of ingezien door de Opdrachtnemer; • De Opdrachtnemer heeft geen toegang tot TOTP-seeds, recovery codes of andere MFA-secrets;

heeft verwijderd: Indien de Oplossing als SaaS wordt geleverd dan waarborgt Opdrachtnemer dat gevoelige gegevens zodanig worden beschermd dat uitsluitend de Opdrachtgever (tenant) toegang heeft tot de inhoud en dat de Opdrachtnemer deze gegevens niet kan ontsleutelen (Zero Knowledge-principe). De Opdrachtnemer past dit principe toe op alle componenten waarbij dit technisch mogelijk is en toont dit aantoonbaar aan. Dit omvat minimaal:

heeft verwijderd: Zero Knowledge en encryptie:

heeft verwijderd: De Opdrachtnemer past een Zero Knowledge-model toe voor alle componenten waar dit technisch mogelijk is;

heeft verwijderd: Gevoelige data is, waar toepasbaar, encrypted en niet ontsleutelbaar door de Opdrachtnemer;

heeft verwijderd: Identity & Access Management gebruik van Customer Managed Keys (CMK);

heeft verwijderd: Sleutelbeheer en cryptografie:

heeft verwijderd: De Oplossing ondersteunt het gebruik van cryptografische sleutels die beheerd worden door de Opdrachtgever;

heeft verwijderd: Indien cryptografische hardware wordt gebruikgemaakt van gangbare en erkende standaarden (zoals FIPS 140-2 gecertificeerde HSM's).

	Toegang door Opdrachtnemer: • Toegang tot gevoelige gegevens door de Opdrachtnemer is alleen mogelijk indien dit strikt noodzakelijk is en technisch niet anders kan worden ingericht; • Break-glass toegang door de Opdrachtnemer is uitsluitend tijdelijk, wordt expliciet geautoriseerd door de Opdrachtgever en vindt plaats onder strikte logging en monitoring.
E43	De Oplossing waarborgt dat tijdelijke en gevoelige toegangsrechten gecontroleerd worden toegekend, beperkt in duur zijn en auditbaar blijven, zodat risico's op ongeautoriseerde toegang worden geminimaliseerd. Dit omvat minimaal: Tijdgebonden en gecontroleerde toegang: • De Oplossing biedt functionaliteit voor het beheer van tijdelijke of beperkte toegang tot gevoelige functies; • Accounts en gebruikersrechten kunnen tijdgebonden worden toegekend, waarbij een duidelijke begin- en einddatum instelbaar is; • Toegang tot gevoelige of hoog-risico functies kan worden afgebakend en beperkt tot een vooraf gedefinieerde en afdwingbare periode; Inrichting en toepasbaarheid: • De functionaliteit voor tijdelijke en gevoelige toegangsrechten is realiseerbaar binnen de standaard IAM-functionaliteit van de Oplossing; • De Oplossing ondersteunt, indien gewenst, toekomstige integratie met een Privileged Access Management (PAM)-Oplossing.
E44	Indien de Oplossing als SaaS wordt geleverd dan waarborgt deze dat API's worden beveiligd tegen misbruik, datalekken en ongeautoriseerde toegang, conform moderne beveiligingsstandaarden en bewezen authenticatie- en autorisatiemechanismen. Dit omvat minimaal: Authenticatie en beveiligingsstandaarden: • Alle API's maken gebruik van OAuth 2.0 en/of OpenID Connect (OIDC), inclusief Proof Key for Code Exchange (PKCE) waar van toepassing; • Voor machine-to-machine communicatie wordt bij voorkeur gebruikgemaakt van wederzijdse TLS-authenticatie (mTLS); Secretless en veilige authenticatie: • De Oplossing ondersteunt moderne, secretless authenticatiepatronen voor productieomgevingen, waaronder managed identities, certificate-based authentication, private key JWT/client assertions of vergelijkbare mechanismen; • Het gebruik van langdurige gedeelde client secrets wordt vermeden; • Indien het gebruik van client secrets technisch noodzakelijk is, toont Opdrachtnemer aan dat de beveiliging hiervan aantoonbaar en adequaat is geborgd door passende maatregelen. Bescherming tegen misbruik: • De Oplossing ondersteunt API throttling en anti-abuse mechanismen om misbruik en overbelasting te voorkomen.
E45	De Oplossing waarborgt de beveiliging van data in rust en tijdens transport en borgt datalekpreventie, sleutelbeheer en integriteit van gegevensverwerking. Dit omvat minimaal: Encryptie en transportbeveiliging: • Alle data in transit wordt beveiligd met TLS 1.2+ of hoger (bij voorkeur TLS 1.3); • Data in rust wordt versleuteld met minimaal AES-256 encryptie;

	Indien de Oplossing als SaaS wordt geleverd geldt sleutelbeheer en cryptografie: • Ondersteuning voor Customer Managed Keys (CMK). Indien cryptografische hardware wordt toegepast, geldt FIPS 140-2 Level 3 gecertificeerde HSM's als referentieniveau en niet als verplichte certificering of voorgeschreven technische implementatie; Opdrachtnemer mag een gelijkwaardige of betere oplossing aanbieden, mits aantoonbaar wordt voldaan aan een vergelijkbaar of hoger niveau van beveiliging en sleutelbeheer; Detectie en preventie: • Indien de Oplossing als SaaS wordt geleverd geldt dat alle data-uitwisselactiviteiten worden gemonitord en gecontroleerd door Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS); Integriteit en foutdetectie: • De Oplossing bevat controlemechanismen waarmee transactie- en verwerkingsfouten aantoonbaar kunnen worden gedetecteerd.

E46	De Opdrachtnemer waarborgt dat persoonsgegevens worden verwerkt conform de geldende privacywetgeving en dat transparantie, datalokalisatie en continuïteit van gegevensverwerking zijn geborgd. Dit omvat minimaal:
	
	Indien de Oplossing als SaaS wordt geleverd geldt voor privacy en compliance:
	• Data wordt verwerkt conform de AVG-richtlijnen;
	• De Opdrachtnemer biedt volledige transparantie in de verwerking van persoonsgegevens;
	• De Opdrachtnemer werkt aantoonbaar mee aan een Data Protection Impact Assessment (DPIA) indien vereist, waarbij een volledige DPIA verplicht kan worden gesteld door de Opdrachtgever;
	
	Datalokalisatie en transparantie:
	• Data in transport en in rust wordt versleuteld conform eis 44.
	• Indien de Oplossing als SaaS wordt geleverd geldt
	  ○ De Opdrachtnemer host de data van de Oplossing binnen de Europese Economische Ruimte (EER);
	  ○ Het is te allen tijde inzichtelijk op welke geografische locaties de gegevens zich bevinden; Continuïteit en beschikbaarheid:
	  ○ De Opdrachtnemer neemt passende maatregelen om bij grote continuïteitsverstoringen de toegang tot data en functionaliteit te waarborgen;
	  ○ De Opdrachtnemer beschrijft op welke wijze de continuïteit van de Oplossing en toegang tot data wordt geborgd.

heeft verwijderd: Ondersteuning voor Customer Managed Keys (CMK), FIPS 140-2 Level 3 gecertificeerde HSM's;

4.2 Dienstverlening

4.2.1 Oplevering en doorontwikkeling

Nr.	Omschrijving
E47	De Opdrachtnemer verzorgt training en kennisoverdracht aan de functioneel beheerders, zodat de Opdrachtgever de Oplossing zelfstandig kan beheren en gebruiken. De training en kennisoverdracht bestaat minimaal uit één of meer fysieke bijeenkomsten in Zaandam, ondersteuning on-the-job bij livegang en het verstrekken van naslagdocumentatie.
E48	Indien de Oplossing wordt geleverd als Software as a Service (SaaS), geldt dat de Opdrachtnemer integraal verantwoordelijk is voor de levering en het beheer van de dienst. Hieronder valt minimaal: • het beschikbaar stellen en onderhouden van het platform (inclusief hardware, software en licenties); • het uitvoeren van onderhoud (waaronder updates, security patches en releases); • het technisch beheer en monitoring van de Oplossing, waaronder beschikbaarheid, performance, capaciteit, beveiliging en data-integriteit; • het borgen van informatiebeveiliging conform geldende standaarden, wet- en regelgeving, en onze aanvullende securityeisen; • het leveren van adequate en beveiligde connectiviteit naar de Oplossing, waarbij de Opdrachtnemer één of meerdere vaste (statische) IP-adressen beschikbaar stelt ten behoeve van IP-filtering door de gemeente, zodat toegang tot de Oplossing kan worden beperkt op basis van netwerktoegang.
E49	Indien de Oplossing als on-premise wordt geleverd, is de Opdrachtgever verantwoordelijk voor het onderliggende platform en de infrastructuur. De Opdrachtnemer is verantwoordelijk voor de Oplossing als softwarecomponent, inclusief het leveren van updates, patches en beveiligingsmaatregelen, en ondersteunt de Opdrachtgever bij beheer, monitoring en optimalisatie van de Oplossing.
E50	Indien de Oplossing wordt geleverd als Software as a Service (SaaS), is de Oplossing aantoonbaar geschikt voor gebruik in een Zaanstad IT-omgeving waarin SSL-inspectie wordt toegepast op netwerkverkeer tussen on-premises systemen van de gemeente en de Oplossing (SaaS-On-premise integraties). De Oplossing functioneert in deze situatie zonder verstoringen van functionaliteit. Voor koppelingen tussen de Oplossing en SaaS-systemen buiten de Zaanstad IT-infrastructuur van de gemeente beschrijft de Opdrachtnemer op welke wijze het beveiligde netwerkverkeer is ingericht.
E51	De Oplossing voorziet in een productieomgeving en ten minste één niet-productieomgeving (voor test- en acceptatiedoeleinden). Afhankelijk van het leveringsmodel (SaaS of on-premise) worden deze omgevingen respectievelijk door Opdrachtnemer geleverd of door Opdrachtnemer ondersteund bij inrichting en beheer.
E52	De Opdrachtnemer borgt dat bij oplevering: • bestaande gegevens uit het conversiebestand (*zie bijlage 15*) worden ingelezen of handmatig worden ingevoerd; • de configuratie voor de werking overeenkomt met het functioneel ontwerp (*zie bijlage 13*) en als geheel in beheer wordt genomen; • de inrichting volledig en consistent is bij ingebruikname.
E53	De Oplossing waarborgt dat administratieve accounts veilig, traceerbaar en auditeerbaar zijn ingericht en dat toegang tot deze accounts adequaat wordt beschermd met sterke authenticatie en passende beveiligingsmaatregelen. Dit omvat minimaal: Identificeerbaarheid en auditability:

	• Alle administratieve accounts hebben een duidelijke en herkenbare naamgeving, zodat acties volledig herleidbaar zijn voor beheer en auditdoeleinden; Notificatie en recovery: • Administratieve accounts ondersteunen minimaal één e-mailadres voor notificaties en recovery; • Ondersteuning voor meerdere e-mailadressen; Sterke authenticatie: • Toegang tot administratieve accounts vereist sterke Multi-Factor Authentication (MFA), waarbij de Oplossing aansluit op de Identity Provider (IdP) van de Opdrachtgever; • De Oplossing ondersteunt het gebruik van door de Opdrachtgever voorgeschreven authenticatiemiddelen, waaronder in ieder geval Microsoft Authenticator (of gelijkwaardige IdP-gebaseerde authenticatie); • De Oplossing ondersteunt aanvullende sterke authenticatiemechanismen, zoals phishing-resistente authenticatie (bijvoorbeeld FIDO2 hardware tokens), indien door de Opdrachtgever toegepast; Gebruiksgemak en implementatie: • De MFA-Oplossing vereist geen aanvullende software-installaties op het apparaat van de Gebruiker, tenzij dit aantoonbaar noodzakelijk is voor de gekozen authenticatiemethode en door de Opdrachtgever expliciet is geaccepteerd.
E54	Opdrachtgever wordt gedurende de contractperiode voorzien in onderhoud en doorontwikkeling van de Oplossing. Afhankelijk van het leveringsmodel (SaaS of on-premise) worden deze activiteiten respectievelijk uitgevoerd door Opdrachtnemer of uitgevoerd door Opdrachtgever met ondersteuning van Opdrachtnemer. Onder onderhoud wordt minimaal verstaan: Correctief-onderhoud, Preventief-onderhoud en Adaptief-onderhoud. Deze vormen van onderhoud maken integraal onderdeel uit van de dienstverlening en zijn inbegrepen in de aangeboden Oplossing. Configuraties en ingerichte functionaliteit die onderdeel uitmaken van de implementatie blijven na updates en wijzigingen van de Oplossing behouden en functioneren naar behoren.
E55	De Opdrachtnemer waarborgt dat bij beëindiging van de overeenkomst of bij faillissement de continuïteit van de dienstverlening en de overdraagbaarheid van de Oplossing zijn geborgd, voor zover betrekking hebbend op de door de Opdrachtnemer geleverde Oplossing en dienstverlening. Dit houdt in dat: • alle data, configuratiegegevens en relevante documentatie volledig, actueel en in een gangbaar en leesbaar formaat beschikbaar worden gesteld aan de Opdrachtgever; • deze gegevens tijdig en op een wijze worden aangeleverd die een gecontroleerde migratie naar een andere Oplossing mogelijk maakt; • de Opdrachtnemer gedurende een overeengekomen periode ondersteuning biedt bij migratie of exit; • De Oplossing is zodanig ingericht dat een overgang naar een alternatief systeem mogelijk is zonder onomkeerbaar verlies van data of essentiële functionaliteit.
W7	**Uitbreiding met andere HR-bronnen** Opdrachtgever wenst dat de Oplossing uitbreiding met meerdere HR-bronnen kan ondersteunen, zodanig dat identiteiten eenduidig worden verwerkt binnen hetzelfde IDU-proces en conform dezelfde lifecycle-regels.

	Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Uitbreiding met andere HR-bronnen' en ga daarbij in ieder geval in op: **A.** Op welke wijze de Oplossing meerdere HR-bronnen ondersteunt binnen één integraal IDU-proces, inclusief de verwerking van identiteiten en lifecycle-events. **B.** Welke impact het toevoegen van een extra HR-bron heeft op de inrichting van het IDU-proces, de autorisatiestructuur en de governance. **C.** In hoeverre bestaande koppelingen of referentie-implementaties beschikbaar zijn met de gangbare HR-systemen (bijvoorbeeld Youforce, Afas).
W8	**Adoptie, training en borging** Opdrachtgever wenst dat de Oplossing effectief wordt toegepast binnen de Organisatie en dat gebruik en beheer duurzaam worden geborgd. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Adoptie, training en borging' en ga daarbij in ieder geval in op: **A. Opleidingen en doelgroepen** Beschrijf welke trainingsmiddelen beschikbaar zijn voor Servicedesk Medewerkers, Proceseigenaren en eindGebruikers,, inclusief de opzet, vorm (bijvoorbeeld klassikaal, online of blended), omvang en fasering van de trainingen. Beschrijf daarbij expliciet: • welke uitgangspunten worden gehanteerd ten aanzien van groepsgrootte, trainingsduur en frequentie; • hoe de trainingen aansluiten op de omvang en samenstelling van de Organisatie; • hoe wordt geborgd dat de Opdrachtgever na implementatie zelfstandig beheer en gebruik kan uitvoeren. **B. Documentatie en kennisvoorziening** Beschrijf welke documentatie en hulpmiddelen beschikbaar zijn en hoe deze actueel worden gehouden. **C. Adoptie en veranderaanpak** Beschrijf hoe Opdrachtgever wordt ondersteund bij het uitdragen van de Oplossing aan eindgebruikers en hoe adoptie wordt bevorderd.
W9	**Doorontwikkeling en releasebeheer** Opdrachtgever wenst dat de Oplossing toekomstvast is en gestructureerd wordt doorontwikkeld, met een gecontroleerd en voorspelbaar releaseproces, waarbij de Opdrachtgever aantoonbaar invloed kan uitoefenen op de prioritering en inhoud van nieuwe functionaliteit. Voor SaaS-Oplossingen geldt dat de Opdrachtnemer verantwoordelijk is voor doorontwikkeling en releasebeheer. Voor on-premise implementaties beschrijft de Opdrachtnemer op welke wijze de Opdrachtgever wordt ondersteund, inclusief de verdeling van verantwoordelijkheden. Beschrijf hoe de Opdrachtnemer invulling geeft aan de wens 'Doorontwikkeling en releasebeheer' en ga daarbij in ieder geval in op: **A. Doorontwikkeling en roadmap** Beschrijf hoe de Oplossing wordt doorontwikkeld, hoe nieuwe functionaliteiten worden bepaald en hoe rekening wordt gehouden met gebruikersbehoeften, wet- en regelgeving en marktontwikkelingen. **B. Releaseproces en frequentie** Beschrijf hoe releases worden gepland, getest en uitgerold, in samenhang met het gehanteerde wijzigingsbeheerproces (zie ook eis *E54)*.

	C. Regie en beïnvloedbaarheid Opdrachtgever Beschrijf via welke overlegstructuren de Opdrachtgever invloed heeft op de inhoud en prioritering van functionaliteit, inclusief de mogelijkheid om functionaliteit (bijv. tegen aanvullende kosten) versneld te realiseren. **D. Inspanning Opdrachtgever nieuwe releases** Beschrijf welke rol en inspanning van de Opdrachtgever wordt verwacht bij on-premise implementatie van nieuwe releases. Rolverdeling en ondersteuning die je krijgt. Bepaalde periode back-up.

4.2.2 Service Level Agreement

Nr.	Omschrijving
E56	De Oplossing en bijbehorende dienstverlening zijn beschikbaar en bruikbaar in de Nederlandse taal. Hieronder wordt minimaal verstaan: • alle gebruikersinterfaces (beheer-, selfservice- en workflowportalen); • meldingen, foutcodes, notificaties en helpteksten; • documentatie, handleidingen en releasenotes; • ondersteuning en communicatie vanuit de Opdrachtnemer.
E57	De Opdrachtnemer biedt een Nederlands sprekende supportOrganisatie: bereikbaar via minimaal e-mail en online klantportaal, zowel technische, functionele vragen, wijzigingen en incidenten.
E58	De Opdrachtnemer ondersteunt centrale registratie van incidenten, classificatie en prioritering en geregistreerde afhandeling en het kunnen volgen van de door Opdrachtgever aangemaakte tickets/ registraties.
E59	De Opdrachtnemer tijdens de POC een concept-SLA en een opzet voor het Document Afspraken en Procedures (DAP) aan, gebaseerd op de in dit PvE gestelde eisen en wensen. De Opdrachtnemer werkt de DAP na gunning en gedurende de implementatie nader uit en levert deze bij oplevering in definitieve vorm op ter borging van de inrichting en werking van de Oplossing.
E60	Indien de Oplossing als SaaS wordt geleverd, bedraagt de beschikbaarheid minimaal 99,9% per kalenderjaar, exclusief gepland onderhoud. Gepland onderhoud bedraagt maximaal 20 uur per kalenderjaar, wordt voorafgaand aan de uitvoering minimaal 5 werkdagen gecommuniceerd aan de Opdrachtgever en vindt buiten reguliere werktijden plaats, tenzij anders overeengekomen.
E61	De Opdrachtnemer hanteert een gestructureerd incidentmanagementproces voor incidenten die betrekking hebben op de Oplossing en de door Opdrachtnemer geleverde dienstverlening, ongeacht het leveringsmodel (SaaS of on-premise). Incidenten worden geclassificeerd naar prioriteit en impact op de dienstverlening. Voor incidenten met betrekking tot de Oplossing en de door de Opdrachtnemer geleverde dienstverlening gelden minimaal de volgende uitgangspunten:

	• Voor incidenten met de hoogste prioriteit, zijnde incidenten die leiden tot (nagenoeg) volledige onbeschikbaarheid van de Oplossing of ernstige verstoring van kernfunctionaliteit voor alle of het merendeel van de Gebruikers,, is ondersteuning buiten reguliere werktijden beschikbaar (24/7), met een maximale initiële reactietijd van 1 uur en het streven naar een werkbare Oplossing binnen 8 uur. De wijze waarop Opdrachtnemer deze bereikbaarheid en opvolging organisatorisch invult is aan Opdrachtnemer, mits tijdige opvolging, escalatie en herstel van deze incidenten buiten reguliere werktijden zijn geborgd en een dergelijk incident niet pas wordt opgepakt nadat Gebruikers of beheerders van Opdrachtgever de volgende werkdag melding maken van de uitval. • Voor overige incidentcategorieën worden reactietijden en oplostermijnen vastgelegd in de SLA; • De Opdrachtnemer beschrijft de gehanteerde prioritering, responstijden en oplostermijnen en onderbouwt hoe deze aansluiten bij de aard, inrichting en kritikaliteit van de Oplossing. Afwijkende classificatiesystematieken (bijvoorbeeld gebaseerd op BIV- of risicoclassificatie) zijn toegestaan, mits aantoonbaar een gelijkwaardig niveau van dienstverlening en responssnelheid wordt geborgd.
E62	De Opdrachtnemer treft aantoonbare maatregelen ter waarborging van de continuïteit van de Oplossing en beschikt over een ingericht en operationeel Business Continuity- en Disaster Recovery-proces. Afhankelijk van het leveringsmodel (SaaS of on-premise) worden deze maatregelen uitgevoerd door Opdrachtnemer, dan wel door Opdrachtgever met ondersteuning van Opdrachtnemer. Dit omvat minimaal: • een actueel en gedocumenteerd Business Continuity- en Disaster Recovery-plan, inclusief procedures voor escalatie en noodtoegang (break-glass); • vastgelegde Recovery Time Objective (RTO) en Recovery Point Objective (RPO), waarbij een RTO van maximaal 8 uur en een RPO van maximaal 24 uur als uitgangspunt gelden. • periodiek testen van herstelprocedures, , waarbij herstel gecontroleerd en reproduceerbaar kan worden uitgevoerd, met een frequentie van ten minste eenmaal per jaar. Indien de Oplossing als SaaS wordt geleverd, omvat dit tevens: • het maken van back-ups van productiedata uitsluitend voor continuïteitsdoeleinden, waarbij minimaal dagelijkse back-ups met een retentie van ten minste 30 dagen worden gehanteerd;
E63	De Opdrachtnemer hanteert een gestructureerd en aantoonbaar wijzigingsbeheerproces voor het doorvoeren van releases, updates en beveiligingsupdates, dan wel ondersteunt de Opdrachtgever hierbij bij on-premise implementaties. Dit proces borgt dat wijzigingen gecontroleerd, traceerbaar en reproduceerbaar worden uitgevoerd. De Oplossing ondersteunt dat wijzigingen en releases gecontroleerd kunnen worden teruggedraaid, waarbij de voorgaande situatie kan worden hersteld zonder verlies van integriteit van data en configuratie.
W10	**Beschikbaarheid en performance**

	Opdrachtgever wenst dat de Oplossing een hoge mate van beschikbaarheid en performance biedt, zodat IAM-processen betrouwbaar worden uitgevoerd. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Beschikbaarheid en performance' en ga daarbij in ieder geval in op: **A. Onderscheid tussen SaaS- en on-premise implementatie** Beschrijf het onderscheid tussen SaaS- en on-premise implementaties, inclusief een duidelijke afbakening van verantwoordelijkheden tussen Opdrachtnemer en Opdrachtgever. **B. Beschikbaarheid en onderhoud** Beschrijf het beschikbaarheidsniveau van de Oplossing, inclusief concrete SLA-waarden en behaalde prestaties in de praktijk, en hoe gepland onderhoud wordt uitgevoerd en gecommuniceerd. Onderbouw dit met concrete waarden, voorbeelden of gerealiseerde prestaties. **C. Verwerking en performance** Beschrijf hoe synchronisaties en provisioningacties worden uitgevoerd, inclusief concrete doorlooptijden, prestaties bij piekbelasting en de wijze waarop deze prestaties worden gemonitord en geborgd. Onderbouw dit met concrete waarden, voorbeelden of gerealiseerde prestaties. Ga hierbij in op: i. de verwachte en/of aantoonbaar gerealiseerde doorlooptijden voor verwerking van wijzigingen, uitgesplitst naar type proces (bijvoorbeeld individuele wijzigingen, bulkverwerkingen en piekbelasting); ii. een referentiescenario waarin een wijziging vanuit een HR-bronsysteem met een omvang van minimaal 300 identiteiten wordt verwerkt, inclusief de totale doorlooptijd tot en met doorwerking in aangesloten Doelsystemen; iii. de wijze waarop de Oplossing performance bewaakt, opschaalt en stabiliteit waarborgt bij toenemende belasting. De Gemeente behoudt zich het recht voor om de opgegeven prestaties te verifiëren in referenties.
W11	**Incidentmanagement en support** Opdrachtgever wenst dat incidenten en vragen efficiënt worden afgehandeld, met passende ondersteuning voor de Organisatie. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Incidentmanagement en support' en ga daarbij in ieder geval in op: **A. Onderscheid tussen SaaS- en on-premise implementatie** Beschrijf het onderscheid tussen SaaS- en on-premise implementaties, inclusief een duidelijke afbakening van verantwoordelijkheden tussen Opdrachtnemer en Opdrachtgever (bijvoorbeeld ten aanzien van 1e, 2e en 3e lijns support). **B. SupportOrganisatie en bereikbaarheid** Beschrijf hoe de supportOrganisatie is ingericht, via welke kanalen ondersteuning wordt geboden, op welke momenten en in welke mate ondersteuning buiten reguliere werktijden bereikbaar is. Onderbouw dit met concrete waarden (bijvoorbeeld openingstijden en bereikbaarheid), voorbeelden of gerealiseerde prestaties. **C. Incidentafhandeling, prioritering en responstijden** Beschrijf de classificatie en prioritering van incidenten (incl. categorieën en definities), de bijbehorende responstijden en oplostermijnen per categorie (inclusief wat standaard is en wat via aanvullende SLA's beschikbaar is) en het escalatieproces, evenals hoe inzicht wordt geboden in incidenten, prestaties en trends (bijv. via rapportages of dashboards). Onderbouw dit met concrete waarden (bijvoorbeeld SLA-tijden), voorbeelden of gerealiseerde prestaties.

	De mate waarin de beschrijving concreet, aantoonbaar en ondersteund met praktijkvoorbeelden of referenties is, wordt meegewogen in de beoordeling.
W12	**Continuïteit en herstel** Opdrachtgever wenst dat de continuïteit van de Oplossing is geborgd en dat herstel bij verstoringen snel, gecontroleerd en aantoonbaar kan plaatsvinden. Beschrijf hoe de Oplossing invulling geeft aan de wens 'Continuïteit en herstel' voor zowel SaaS- als on-premise implementaties en ga daarbij in ieder geval in op: **A. Onderscheid tussen SaaS- en on-premise implementatie** Beschrijf het onderscheid tussen SaaS- en on-premise implementaties, inclusief: • een duidelijke afbakening van verantwoordelijkheden tussen Opdrachtnemer en Opdrachtgever en de afhankelijkheden tussen beide • de mate waarin de gevraagde continuïteits- en herstelmaatregelen daadwerkelijk door Opdrachtgever gerealiseerd kunnen worden **B. Continuïteitsmaatregelen** Beschrijf welke maatregelen zijn getroffen om de continuïteit van de dienstverlening te waarborgen en onderbouw dit met concrete voorbeelden of referenties. Beschrijf daarnaast de impact van (tijdelijke of langdurige) uitval van de Oplossing op de uitvoering van IAM-processen en op welke wijze de Opdrachtgever in staat blijft om kritische werkzaamheden voort te zetten. Ga hierbij in op mogelijke werkprocessen of voorzieningen waarmee essentiële handelingen, zoals het verwerken van instroom of het toekennen van Autorisaties, tijdelijk (handmatig) kunnen worden uitgevoerd. **C. Herstelprocessen en disaster recovery** Beschrijf hoe herstel bij calamiteiten is ingericht, inclusief procedures, verantwoordelijkheden en de mate van automatisering, en geef aan hoe herstelprocedures worden getest. Onderbouw dit met concrete testfrequenties, resultaten of praktijkvoorbeelden. **D. Back-up, databehoud en herstel** Beschrijf hoe back-ups en databehoud zijn ingericht (inclusief frequentie, retentie en beveiligingsmaatregelen) en hoe data wordt beschermd tegen verlies of corruptie. Geef aan hoe dit is ingericht bij SaaS- en on-premise implementaties en welke verantwoordelijkheden daarbij gelden voor Opdrachtnemer en Opdrachtgever. Beschrijf tevens de gehanteerde RTO en RPO, de onderbouwing daarvan, de wijze waarop deze worden gerealiseerd en hoe herstel en dataverlies worden getest. Onderbouw dit met concrete waarden (zoals RTO/RPO), voorbeelden of gerealiseerde prestaties.
W13	**Exit en overdraagbaarheid** Opdrachtgever wenst dat bij beëindiging van de dienstverlening een gecontroleerde, volledige en tijdige overdracht van data, configuratie en documentatie mogelijk is, waarbij continuïteit van dienstverlening gedurende de exitfase wordt geborgd. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Exit en overdraagbaarheid' en ga daarbij in ieder geval in op: **A. Onderscheid tussen SaaS- en on-premise implementatie** Beschrijf het onderscheid tussen SaaS- en on-premise implementaties, inclusief een duidelijke afbakening van verantwoordelijkheden tussen Opdrachtnemer en Opdrachtgever. **B. Exitstrategie en continuïteit** Beschrijf hoe beëindiging van de dienstverlening wordt ondersteund (incl. proces, stappen, doorlooptijden en rollen) en hoe continuïteit van dienstverlening en toegang tot data gedurende de exitfase wordt geborgd.

	C. Data, configuratie en overdraagbaarheid Beschrijf hoe data, configuratie en documentatie beschikbaar worden gesteld, in welke formaten en met welke mate van volledigheid, en hoe migratie naar een andere Oplossing wordt gefaciliteerd.

5 Bijzondere uitvoeringsvoorwaarden

5.1 Social Return on Investment

Deze opdracht leent zich niet voor het stellen van een SROI-verplichting. De werkzaamheden betreffen hoog specialistische inzet, waarvoor beperkt mogelijkheden bestaan om personen met een afstand tot de arbeidsmarkt in te zetten.

Daarnaast bestaat de opdrachtwaarde slechts voor een beperkt deel uit loonkosten. Het stellen van een SROI-eis wordt daarom niet als realistisch en proportioneel beschouwd.

5.2 Duurzaamheid

De gemeente Zaanstad wenst dat de Oplossing en de levering en het beheer daarvan op duurzame wijze worden uitgevoerd, met aandacht voor energiegebruik, grondstoffen en transparantie.

Nr.	Omschrijving
W14	Opdrachtgever wenst dan Opdrachtnemer invulling geeft aan duurzaamheid binnen de levering en exploitatie van de Oplossing. Beschrijf hoe Opdrachtnemer invulling geeft aan de wens 'Duurzaamheid' en ga daarbij in ieder geval in op: **A. Duurzaamheidsbeleid hosting en datacenters** Indien de Oplossing als Software as a Service (SaaS) wordt geleverd, beschrijf op welke wijze de hostingpartij invulling geeft aan duurzame hosting, waaronder het gebruik van hernieuwbare energie, energie-efficiënte datacenters en reductie van CO_2-uitstoot. Bij on-premise implementaties beschrijf hoe de Oplossing bijdraagt aan efficiënt gebruik van infrastructuur en welke maatregelen de Opdrachtnemer treft om energieverbruik en belasting van de IT-omgeving te beperken. **B. Circulaire bedrijfsvoering en lifecyclemanagement** Beschrijf welke maatregelen de Opdrachtnemer neemt op het gebied van circulaire economie, verantwoord gebruik van middelen, lifecyclemanagement en minimalisering van afvalstromen binnen de levering en het beheer van de Oplossing. **C. Transparantie en rapportage** Beschrijf welke certificeringen, rapportages of beleidsdocumenten beschikbaar zijn ten aanzien van duurzaamheid, ESG-, milieu- of CO_2-doelstellingen, en op welke wijze gedurende de contractperiode periodiek inzicht kan worden geboden en kan worden gestuurd op continue verbetering.

gemeente Zaanstad

Stadhuisplein 100, 1506 MZ Zaandam
Postbus 2000, 1500 GA Zaandam

T 14 075
antwoord@zaanstad.nl
www.zaanstad.nl