Bijlage 3 – Programma van Eisen

Europese openbare aanbesteding

IGA TOOL

ten behoeve van

Gemeente Haarlem

Kenmerk 2023 – 645264

Inhoud

1.1. Algemeen

1.1	De Inschrijving is in de Nederlandse taal gesteld en de gehanteerde tarieven zijn in euro's, exclusief BTW.
1.2	De Inschrijving heeft een gestanddoeningstermijn van minimaal 90 dagen na de datum waarop de Inschrijvingen uiterlijk ingediend dienen te worden. Tijdens deze periode heeft de Inschrijving het karakter van een onherroepelijk aanbod.
1.3	Opdrachtnemer gaat ermee akkoord dat de gestanddoeningstermijn van zijn Inschrijving, in het geval een kort geding wordt aangespannen, verlengd wordt tot minimaal twee (2) weken na de datum van de uitspraak in het kort geding.
1.4	Opdrachtnemer adresseert de factu(u)r(en) aan het algemene factuuradres van Opdrachtgever onder vermelding van het door Opdrachtgever aangereikte inkooporder nummer.
1.5	Voor de facturatie van de leveringen/diensten stuurt Opdrachtnemer hoogstens één (1) (verzamel)factuur per maand. In ieder geval moet op iedere factuur de volgende informatie worden vermeld: • Het inkooporder nummer dat in de Opdracht vermeld wordt; • De naam van de contactpersoon/besteller; • Het afleveradres; • Het Kamer van Koophandelnummer van uw onderneming; • Bankrekeningnummer en indien van toepassing SWIFT/BIC en IBAN-code.
1.6	Opdrachtnemer richt alle facturen digitaal aan crediteuren@haarlem.nl.
1.7	Indien Opdrachtnemer zijn verbintenissen, voortvloeiend uit de Overeenkomst, niet geheel of niet behoorlijk is nagekomen, heeft Opdrachtgever het recht de betaling op te schorten.
1.8	Facturen die niet de geëiste informatie bevatten, zullen niet door Opdrachtgever in behandeling genomen worden.
1.9	Opdrachtnemer conformeert zich volledig en onvoorwaardelijk aan de bijgevoegde Algemene Inkoopvoorwaarden GIBIT 2020 en de Algemene inkoopvoorwaarden Diensten van Opdrachtgever. Dit betekent dat uitsluitend de door Opdrachtgever gehanteerde voorwaarden van toepassing zijn. Door de Inschrijver gehanteerde voorwaarden van welke aard dan ook worden expliciet van de hand gewezen.
1.10	Inschrijver dient akkoord te gaan met de inhoud van de concept Overeenkomst, toegevoegd bij deze aanbesteding en zoals deze eventueel gewijzigd is door middel van een Nota van inlichtingen.

1.11	Opdrachtnemer is in het bezit van alle vergunningen die nodig zijn voor het uitvoeren van de in de Aanbestedingsleidraad genoemde activiteiten.
1.12	Het uitvoeren van werkzaamheden in onderaanneming is alleen toegestaan als Opdrachtgever daarvoor schriftelijk toestemming heeft gegeven.
1.13	Als hoofdaannemer draagt Opdrachtnemer volledige verantwoordelijkheid voor de activiteiten van zijn onderaannemers. Opdrachtnemer verzorgt de communicatie namens en naar de onderaannemer(s). Facturering van werkzaamheden die in onderaanneming worden uitgevoerd, wordt door de hoofdaannemer verzorgd.
1.14	Elk jaar vindt er een evaluatiegesprek plaats tussen de accountmanager van Opdrachtnemer en de contractmanager van Opdrachtgever. In dit gesprek wordt de voortgang van de Overeenkomst besproken. De uitvoering dient te worden opgenomen in de SLA.
1.15	Gedurende het verificatiegesprek zal er een nadere afstemming plaatsvinden over de definitieve aantallen en fasering van de licenties tijdens contractperiode.

1.2. Architectuur

2.1	Het systeem moet primair worden geleverd als Software as a Service. Voor integratie met interne identity stores en SaaS-applicaties waarvoor de IAM-applicatie niet een eigen proprietary connector heeft, wordt gebruik gemaakt van een door opdrachtnemer te leveren, bij opdrachtgever on-premise geplaatste agent of connector. De beveiligde verbinding tussen deze agent of connector en de SaaS-omgeving wordt geïnitieerd vanuit deze agent of connector om listeners aan de edge van ons netwerk onnodig te maken. Voor andersoortige koppelingen met systemen van opdrachtgever wordt gebruik gemaakt van de servicegateway van opdrachtgever.
2.2	Alle Systeemcomponenten (inclusief koppelingen met externe applicaties) die door Opdrachtnemer beschikbaar worden gesteld en alle ondersteunende applicaties, zoals web-browser en Java, worden bijgehouden op het laatste security- en servicepack-level.
2.3	Er moet gebruik worden gemaakt van vaste, specificeerbare (niet random) poorten (TCP/UDP) voor data-verkeer tussen opdrachtnemer en opdrachtgever.
2.4	Er moet gebruik gemaakt worden van Open Standaarden (https://www.forumstandaardisatie.nl) en - indien niet mogelijk - algemeen geldende en veelgebruikte closed standaarden. Bijvoorbeeld het gebruik van TLS 1.3 of 1.2 voor encryptie van dataverkeer.

2.5	Opdrachtnemer garandeert de werking van de via het publieke internet beschikbare functionaliteit op recente versies van de gangbare platforms/browsers zonder de installatie van extra plugins: • Windows, MacOS; • Microsoft Edge, Apple Safari, Google Chrome, Mozilla Firefox; • Android, IOS; • Het Systeem moet bruikbaar zijn via desktop, laptop, smartphone en tablet (responsive website).
2.6	Het Systeem mag geen issues geven met bekende antivirussoftware. Bij eventuele issues zal Opdrachtnemer bijdragen bij trouble-shooting processen en ondersteuning bieden waar nodig. Opdrachtgever is bij dergelijke processen regiehouder.
2.7	Het Systeem moet voldoen aan de overheidstoegankelijkheidseisen uit hoofdstuk 9 van de Europese standaard EN 301 549. Deze zijn identiek aan toegankelijkheidsnorm WCAG 2.1 A + AA.
2.8	Het systeem voldoet aan de GIBIT Eisen D1 en D2 t.a.v. Dataportabiliteit (Gemeentelijke ICT-kwaliteitsnormen).
2.9	Indien het systeem op container-technologie is gebaseerd, voldoet het aan de vereisten van de Haven-compliancy van de VNG.
2.10	De performance van het Systeem in de productieomgeving - gemeten naar de gemiddelde ‘page load time’ - is gemiddeld kleiner dan twee seconden. De ‘page load time’ is de tijd dat een gebruiker een pagina aanroept in het Systeem via een klik op een link of knop totdat de volledige pagina in de webbrowser is geladen. Pagina's waarop een aantoonbaar zwaar achtergrondproces wordt gestart - bijvoorbeeld een zoekopdracht of berekening - zijn uitgezonderd van deze eis. In die situaties moet de gebruiker wel terugkoppeling krijgen over de voortgang van het proces. Indien een pagina niet voldoet aan de geëiste ‘page load time’ dan moet Opdrachtnemer de performance van deze pagina verbeteren binnen een met Opdrachtgever overeengekomen tijdsperiode.
2.11	Het systeem ondersteunt een multi-tenant inrichting. Samenwerking met meer gemeenten en ketenpartners zal leiden tot een behoefte om in een enkele applicatie meerdere organisaties te kunnen ondersteunen, waarbij de data van deze organisaties (deels) strikt gescheiden blijft.
2.12	Het systeem past strikte scheiding van tenants toe op alle niveaus.
2.13	Het Systeem heeft zowel een ipv4 als ipv6 adres of Opdrachtnemer overlegt een planning wanneer dit is gerealiseerd.

1.3. Informatiebeveiliging

3.1	Het systeem voorziet in Single Sign-On binnen het domein van Opdrachtgever. Het systeem wordt daartoe aangesloten op Microsoft Entra ID (voorheen Azure AD) van Opdrachtgever. De te gebruiken technieken (zoals SAML, OAuth2.0, OpenID Connect) voldoen aan de standaarden van Forum Standaardisatie. Motivatie: Onbevoegde toegang tot systemen en toepassingen voorkomen. Regie houden op accounts en accountpolicies. Multi factor authenticatie is geborgd. Bron: BIO 9.4.2
3.2	De autorisaties dienen rol gebaseerde autorisaties te zijn. Motivatie: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. Bron: BIO 9.2.2
3.3	De autorisaties kunnen per gebruikersrol, per groep, per team en per medewerker ingericht worden. Er dient verschil te worden gemaakt tussen creëren, raadplegen, wijzigen en verwijderen. Motivatie: Onbevoegde toegang tot systemen en toepassingen voorkomen. Bron: BIO 9.4.1
3.4	Functiescheiding wordt toegepast: beheer en gebruik zijn volledig gescheiden. Motivatie: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. Bron: BIO 9.2.2.2
3.5	Er dient onderscheid gemaakt te worden tussen technisch beheer en functioneel beheer. Motivatie: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. Bron: BIO 9.2.3
3.6	Het systeem bevat een audit-trail, welke niet muteerbaar is. Motivatie: Gebeurtenissen vastleggen en bewijs verzamelen. Bron: BIO 12.4.1
3.7	De audit-trail bevat wie, wat, waar, wanneer informatie aangaande: • Alle bewerkingen: het inloggen, wijzigen, afsluiten, aanmaken en verwijderen van zaken, informatieobjecten en (meta-)gegevens; • Alle activiteiten van beheerders: het aanmaken, wijzigen, beëindigen, verwijderen van autorisaties of rollen, informatieobjecten en (meta-)gegevens; Motivatie: Gebeurtenissen vastleggen en bewijs verzamelen. Bron: BIO 12.4
3.8	Bij beëindiging van een bepaalde autorisatie is herleidbaar dat deze autorisatie ooit bestaan heeft, inclusief bijbehorende audit-trail. Motivatie: Gebeurtenissen vastleggen en bewijs verzamelen. Bron: BIO 12.4

3.9	Indien een rol, groep of functie beëindigd wordt, is herleidbaar dat deze ooit bestaan heeft, inclusief bijbehorende audit-trail. Motivatie: Gebeurtenissen vastleggen en bewijs verzamelen. Bron: BIO 12.4
3.10	Alle benodigde verbindingen van en naar het te leveren Cloud product zijn beveiligd en encrypted volgens geldende voorschriften van de NCSC en Forum Standaardisatie. Motivatie: De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen. Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit. Bron: BIO 13.1 en 13.2 (De BIO verwijst naar NCSC en Forum Standaardisatie).
3.11	Alle informatie in de Cloud is encrypted volgens geldende voorschriften van de NCSC (National Cyber Security Centrum) en Forum Standaardisatie. Motivatie: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. Bron: BIO 10.1.1 (De BIO verwijst naar NCSC en Forum Standaardisatie).
3.12	Uitwisseling van gegevens tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware. Motivatie: Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware. Bron: BIO 12.2.1
3.13	Opdrachtnemer garandeert dat gegevens van verschillende klanten van elkaar zijn geïsoleerd. Motivatie: Voorkomen van ongewenste toegang tot en ongewenste wijziging van informatie. Bron: NCSC - WhitepaperCloudcomputing"
3.14	E-mails worden altijd volgens standaarden 'DKIM', 'SPF', 'DMARC', 'STARTTLS' en 'DANE' verstuurd. Dit gebeurt ofwel met behulp van de infrastructuur van Opdrachtgever (d.m.v. mailrelay via onze MX server) ofwel via e-mail servers van de leverancier (deze worden opgenomen in SPF-record van Opdrachtgever en krijgen een separate DKIM selector binnen het domein van Opdrachtgever). E-mails hebben ten alle tijden "@haarlem.nl" als e-mail domein. Alle DNS records van e-mail componenten bij de leverancier worden beschermd d.m.v. DNSSEC. Motivatie: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit. Bron: BIO 13.2.3.1 en Forum Standaardisatie: Verplichte lijst met Open Standaarden
3.15	Patch management is aantoonbaar ingericht. Systeemupdates worden tijdig uitgevoerd volgens overeengekomen afspraken opgenomen in de SLA. Motivatie: De integriteit van operationele systemen waarborgen. Benutting van technische kwetsbaarheden voorkomen. Bron: BIO 12.5.1
3.16	Vulnerability management is aantoonbaar ingericht. Zodra kwetsbaarheden aan het systeem bekend worden ontvangt opdrachtgever daar direct een melding

	van. Kwetsbaarheden worden met de urgentie die past bij de risico inschatting van de IBD/NCSC (CVE score) tijdig verholpen. Dit volgens overeengekomen afspraken opgenomen in de SLA. Motivatie: Benutting van technische kwetsbaarheden voorkomen. Bron: BIO 12.6.1.1
3.17	Opdrachtnemer garandeert de werking van het systeem op de meest recente versies van de meest gangbare webbrowsers op Windows, Apple en Android systemen. Motivatie: De integriteit van operationele systemen waarborgen. Benutting van technische kwetsbaarheden voorkomen. Bron: BIO 12.5.1
3.18	Het systeem mag geen gebruik maken van add-ons (extensies) in de webbrowser. Motivatie: De integriteit van operationele systemen waarborgen. Benutting van technische kwetsbaarheden voorkomen. Bron: BIO 12.5.1
3.19	Indien in het systeem wachtwoorden worden opgeslagen dient dat versleuteld gedaan te worden volgens geldende voorschriften van de NCSC. Wachtwoorden moeten altijd eenwegsvercijferd worden opgeslagen door gebruik van hashing in combinatie met salts. Motivatie: Zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit. Bron: ICT-Beveiligingsrichtlijnen voor Webapplicaties van NCSC, richtlijn U/TV.01
3.20	Opdrachtgever blijft eigenaar van de informatie en kan die te allen tijde opvragen. Motivatie: Bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers. Bron: BIO 15.1.2
3.21	Informatie moet op verzoek van Opdrachtgever vernietigd, verwijderd of overschreven kunnen worden met gebruikmaking van technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen. Bijvoorbeeld als gevolg van een wettelijke verplichting of na het beëindigen van het contract. Motivatie: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die is opgeslagen voorkomen. Bron: BIO 11.2.7 en BIO 8.3.2

1.4. Privacy

4.1	Privacy by Design en Privacy by Default worden toegepast in de ontwikkeling en doorontwikkeling van het Systeem. Dit betekent dat uitsluitend die persoonsgegevens mogen worden verwerkt die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt.

4.2	Opdrachtnemer waarborgt de integriteit van de te gebruiken persoonsgegevens in het Systeem.
4.3	Verwerking van persoonsgegevens mag uitsluitend plaatsvinden binnen de Europese Economische Ruimte (EER). Verwerking van persoonsgegevens in de Verenigde Staten is niet toegestaan.
4.4	Van gerepliceerde gegevens is altijd bekend wat de authentieke registratie is (single point of control).
4.5	Autorisaties voor het verwerken van persoonsgegevens moeten op grond van de Algemene Verordening Gegevensbescherming (AVG) worden beperkt tot die functies, die absoluut noodzakelijk zijn voor het behandelen van een case.
4.6	Beveiligingsincidenten die de beschikbaarheid en/of betrouwbaarheid van het Systeem of mogelijk de betrouwbaarheid of juistheid van de gegevens kunnen aantasten, moeten direct worden gemeld aan de Opdrachtgever. Tevens moet vermeld worden wat de maatregelen zijn die genomen worden (zijn genomen) en binnen welke termijn een incident opgelost zal zijn (is).
4.7	Opdrachtnemer sluit een standaard verwerkersovereenkomst (VNG-model) met de voorlopige gegunde partij af die voldoet aan de eisen die de AVG daaraan stelt (https://www.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/).
4.8	~~Indien in het Systeem wachtwoorden worden opgeslagen, moet dat versleuteld gedaan worden volgens geldende voorschriften van de NCSC. Wachtwoorden moeten altijd eenwegsvercijferd worden opgeslagen door gebruik van hashing in combinatie met een salt (ICT-Beveiligingsrichtlijnen voor Webapplicaties van NCSC, richtlijn U/TV.01).~~

1.5. Geautomatiseerde besluitvorming en documentatie

5.1	Het Systeem moet worden geleverd met documentatie en instructiemateriaal voor eindgebruikers in de Nederlandse taal. Overige documentatie, zoals technische- en functionele beheerdocumentatie, moet in het Nederlands of in het Engels zijn opgesteld.

1.6. Implementatie

6.1	Opdrachtnemer beschrijft in een implementatieplan de technische en functionele implementatie en hoe de migratie van bestaande functionaliteit wordt uitgevoerd.
6.2	Opdrachtgever stelt voorafgaand aan het ondertekenen van de overeenkomst samen met Opdrachtnemer een acceptatieplan op waarmee partijen voorafgaan aan (gefaseerde) livegang toetsen of de geboden oplossing voldoet aan alle eisen in dit PvE.
6.3	Opdrachtnemer verzorgt aan functioneel beheerders en key-users beheerderstrainingen en gebruikerstrainingen op basis van train-de-trainer. De trainingen worden gegeven via Microsoft Teams of incompany.

1.7. Service Level Agreement

7.1	Opdrachtnemer dient bij de inschrijving een Service Level Agreement (SLA) in. Daarin komen minimaal de volgende onderdelen terug: Service levels, Service management (bereikbaarheid/helpdesk/piketnummer), Processen rond storingen, onderhoud en wijzigingen, Communicatie en escalatie en Rapportages en overleg. De SLA moet tegelijkertijd met de overeenkomst worden ondertekend.
7.2	Opdrachtnemer gaat ermee akkoord dat over de invulling van de onderwerpen in de SLA nadere afspraken kunnen worden gemaakt.
7.3	De volgende onderwerpen dienen in de SLA aan bod te komen: • Opdrachtnemer zorgt gedurende de duur van de contractperiode dat het Systeem blijft voldoen aan relevante landelijke wet- en regelgeving. • Opdrachtnemer zorgt gedurende de duur van de contractperiode voor het operationeel houden van het Systeem en de bijbehorende Koppelingen. • Opdrachtnemer heeft ten behoeve van storingen een Nederlandstalige helpdesk ingericht die bereikbaar is op maandag tot en met vrijdag van 8:30 uur tot 17:30 uur en ten minste bereikbaar is via e-mail en telefoon. ~~Buiten kantoortijden stelt Opdrachtnemer een piketnummer beschikbaar. Daar waar de Opdrachtnemer aantoonbaar een betere dienstverlening garandeert dan het gestelde minimum, leidt dit tot een betere beoordeling.~~ • Geef duidelijk aan op welke wijze de afhandeling van incidenten, problemen en wijzigingen (te bezien als P1, P2, P3, of P4) via 1e, 2e en 3e lijns support is ingericht en hoe de afhandeling is geborgd. Wat zijn de standaard response- en oplostijden die hierbij in acht worden genomen?

	• Geef aan hoe Opdrachtnemer de supportprocessen ten behoeve van de Gemeente Haarlem inregelt. • Opdrachtnemer levert een accountmanager die fungeert als “Single point of Contact” voor de Opdrachtgever. De volgende drie communicatie en escalatie niveaus worden minimaal onderkend: 1 operationeel (serviceniveau: procescoördinatie en 1e escalatie), 2 tactisch (service/contract management) en 3 strategisch (directie/afdelingsmanagement). • Opdrachtnemer geeft bij het niet behalen van de afgesproken dienstverlening (service levels) dit direct en gemotiveerd per e-mail door aan Opdrachtgever. • Opdrachtgever krijgt periodiek een rapportage met daarin een overzicht van de behaalde servicelevels, afgehandelde storingen/wijzigingen en eventuele beveiligingsincidenten. Deze rapportage wordt in een periodiek overleg tussen Opdrachtnemer en Opdrachtgever besproken.

1.8. Onderhoud en continuïteit

8.1	Bij upgrades en updates van het Systeem documenteert de Opdrachtnemer de belangrijkste wijzigingen en consequenties voor het functioneren van het Systeem en de Koppelingen en stelt deze beschikbaar aan de Opdrachtgever in de vorm van release notes.
8.2	De beschikbaarheid van de SaaS-oplossing is minimaal 99,0% over een 24/7 - 365 dagen per jaar termijn. Gepland onderhoud wordt daarbij niet meegerekend. Per kwartaal moet de year-to-date performance worden gerapporteerd door Opdrachtnemer.
8.3	Opdrachtnemer beschikt over certificeringen ISO27001 en ISO900x(gelijkwaardig+beschrijving) en de aangeboden dienst valt binnen de scope van deze certificeringen.

1.9. Wijziging/doorontwikkeling

9.1	Opdrachtgever belegt de ondersteuning voor doorontwikkeling van de oplossing binnen de Gemeente Haarlem en Zandvoort bij de Opdrachtnemer. Hiertoe kan de Opdrachtgever een strippenkaart van 120 uur in opdracht geven. De resterende strippenkaart uren blijven beschikbaar bij jaarovergang. Het soort werkzaamheden waarvoor de Opdrachtgever deze strippenkaart wenst te kunnen inzetten is (niet limitatief): • aanmaken en wijzigen van systeemkoppelingen;

	• technische ondersteuning bij afhandeling van storingen en wijzigingen;
	• advies ten aanzien van effectieve inzet van de oplossing;
	  • hulp bij migratie van bestaande IAM gerelateerde processen;
	  • enzovoort.

1.10. Autorisatiebeheer

10.1	Organisatierollen: Mogelijkheid om organisatierollen met per rol bijbehorende autorisaties in één of meer systemen te modelleren ten behoeve van handmatige (via een IAM portaal) en geautomatiseerde (op basis van business rules) toekenning.
10.2	Rollen toekennen: Mogelijkheid dat leidinggevenden aan een (ondergeschikte) medewerker een of meer organisatierol(len) toekennen of goedkeuren. De accounts en autorisaties die bij die rol horen worden automatisch in de betreffende systemen aangebracht.
10.3	Toekenbare rollen Leidinggevende kan alleen rollen toekennen en zien, waartoe hij bevoegd is.
10.4	Workflow Mogelijkheid aanvraag- en goedkeuringsprocessen te modelleren. Het moet mogelijk zijn om processen handmatig en geautomatiseerd in te richten, waarbij onder meer de risicoklasse van een autorisatie of de licentiekosten medebepalend zijn voor de keuze handmatig goedkeuren of geautomatiseerd toekennen.
10.5	Applicatierollen Mogelijkheid om in gekoppelde systemen applicatierollen te definiëren en via het portaal en aan businessrollen beschikbaar te stellen voor toekenning.
10.6	Birthright autorizations Mogelijkheid bieden om geautomatiseerd op basis van business rules rollen aan natuurlijke personen toe te kennen of in te trekken en geautomatiseerd de bijbehorende autorisaties aan te brengen of af te nemen in gekoppelde systemen.
10.7	Distributielijsten Mogelijkheid om e-maildistributielijsten in Exchange on-premise automatisch bij te werken vanuit de rollenbeheerprocessen (via birthright of toegekende businessrollen).
10.8	Functiescheiding De mogelijkheid moet bestaan om functiescheiding te kunnen realiseren. Het systeem moet dus voorzien in een mogelijkheid om conflicterende rollen te signaleren en registreren.
10.9	Conflicterende rollen goedkeuren De mogelijkheid om toekenning van bepaalde conflicterende rollen alleen mogelijk te maken onder expliciete goedkeuring voor een bepaalde tijd.
10.10	Conflicterende rollen kunnen blokkeren De mogelijkheid om toekenning van bepaalde conflicterende rollen te blokkeren.

10.11	Inzicht in rollen De mogelijkheid om binnen de hiërarchie medewerkers, managers en functioneel applicatie beheerders snel inzicht te geven in de toegekende rollen en autorisaties via het self-service portaal en via rapportages.
10.12	Toegang Office 365 Mogelijkheden om groepslidmaatschappen en distributielijsten toe te kennen of te ontnemen.
10.13	Notificaties Het toekennen of intrekken van autorisaties moet worden gemeld aan gebruikersgroepen zoals functioneel beheerders van doelsystemen.

1.11. Identiteitenbeheer

11.1	Identificeren personeelsmutaties: Mogelijkheid bieden om personeelsmutaties in BCS HR Non-Profit automatisch te detecteren en op basis van de mutatie in een IAM-voorziening identiteitsgegevens op te voeren of bij te werken.
11.2	Selectie van te koppelen gegevens: Er kunnen meerdere bronsystemen gelijktijdig ontsloten worden en per systeem kan een andere koppeling nodig zijn. Mogelijkheid bieden om per bron in te stellen welke gegevens vanuit het HR systeem ontsloten moeten worden.
11.3	Koppeling: De IGA-oplossing ondersteunt de volgende koppelingsmogelijkheden voor de koppeling met bronsystemen: webservices, api's en import van csv-bestanden.
11.4	Real-time koppeling: De mogelijkheid moet bestaan om in real-time en op bepaalde momenten mutaties uit bronsystemen te kunnen verwerken.
11.5	IAM portaal: Mogelijk om persoonsgegevens buiten het HR systeem om binnen een IAM-portaal te beheren: opvoeren, wijzigen of afvoeren. Bij het handmatig opvoeren van identiteiten moet het systeem een eigen unieke identificatie hanteren om te voorkomen dat de unieke personeelsnummers worden gedoubleerd. Verplichte velden zijn onder andere organisatie, afdeling, locatie, team, functie/rol en/of leidinggevende.
11.6	Personeelsmutaties: Mogelijkheid bieden om workflows met business rules en rapportages te definiëren waarbij filtering op basis van één of meer attributen van identiteiten gebruikt kunnen worden. De volgende attributen zijn wenselijk als selectiecriterium: • Naam • Voornamen

	• Organisatie • Afdeling • Locatie • Team • Functie/rol • Leidinggevende • Personeelsnummer
11.7	Bepalen van leidinggevende: Mogelijkheid bieden om bij import vanuit het HR systeem op basis van de HR-attributen per afdeling en/of locatie vast te stellen wie de leidinggevende van een medewerker is
11.8	Wachtwoordenbeleid: Mogelijkheid om voor beheerde accounts wachtwoorden te genereren voor doelsystemen. Per doelsysteem moet het voor dat systeem geldende wachtwoordenbeleid toegepast kunnen worden.
11.9	Genereren accounts en e-mailadressen: Mogelijkheid om regels te definiëren voor het genereren en toekennen van accountnamen in Windows en andere systemen en e-mailadressen in Entra ID, Active Directory en Exchange (on premise en Exchange 365).
11.10	Provisionen van identiteiten naar doelsystemen: Mogelijkheid bieden van een geautomatiseerde provisioning van identiteitsgegevens naar Active Directory, Microsoft Entra ID, Exchange (on premise en Exchange 365), TOPdesk, Microsoft 365/Sharepoint Online/Teams, documentmanagementsysteem Verseon, Insite (Pleio intranet), Delinea Secret Server, kaartmanagementsysteem SIMS (SQLServer).
11.11	DIY-connector: Het moet voor gemeente Haarlem mogelijk zijn om zelf, zonder uitgebreide externe hulp, een connector met een doelsysteem in te richten, als een dergelijke connector niet bestaat (mits het doelsysteem dat toestaan).
11.12	Reconciliatie – Soll/Ist vergelijking: Het moet mogelijk zijn om van gekoppelde en niet-gekoppelde doelsystemen de accounts en autorisaties in te lezen ter verificatie van de huidige situatie, de zogenaamde reconciliatie of Soll-Ist vergelijking.
11.13	Workflow: Voor de besturing van de provisioningprocessen moet het eenvoudig (zonder externe consultancy) mogelijk zijn om zelf workflows te definiëren.
11.14	Cloud: De mogelijkheid moet bestaan om informatiesystemen in de cloud aan te kunnen sluiten. Daarvoor moeten in ieder geval provisioning protocollen als SCIM ~~en SPML~~ kunnen worden toegepast.
11.15	In en uit dienst: Mogelijkheid bieden om een personeelsmutatie in te plannen op het moment dat

	wordt bepaald door een mutatiedatum, een in dienst- of een uit dienst-datum. Toekomstmutaties moeten geïdentificeerd kunnen worden.
11.16	Ontslag op staande voet: Mogelijkheid dat een leidinggevende of een gedelegeerde een procedure voor ontslag op staande voet onverwijld in gang kan zetten, waarmee automatisch direct alle autorisaties worden afgenomen en alle accounts worden geblokkeerd.
11.17	Doorstroom: Mogelijkheid bieden om in geval van functiewijziging opvoer- en afvoermutaties op afzonderlijke momenten door te voeren, zodat iemand in een overgangsperiode naast de nieuwe functie ook voor een te bepalen tijd de oude functie (inclusief bijbehorende autorisaties en voorzieningen) kan houden.
11.18	Notificatie: Mogelijkheid bieden om op te bepalen momenten vóór de einddatum van een dienstverband of een contract een melding te doen naar manager en/of medewerker. Deze functionaliteit moet per bronsysteem in te stellen zijn.
11.19	Ontdubbelen: Mogelijkheid bieden om bij aankoppelen van bron- en doelsystemen te analyseren welke identiteiten al voorkomen en daarmee automatisch de identiteitsgegevens te ontdubbelen. Mogelijkheid bieden om de dubbele gegevens handmatig te corrigeren.
11.20	Basisautorisaties: Toekennen/muteren/intrekken
11.21	Mogelijkheid bieden om op basis van bedrijfsregels generieke autorisaties te muteren. Te denken valt aan: • genereren en intrekken e-mailadres • toekennen/intrekken groepslidmaatschappen, autorisaties en licenties in Office365 • toekennen toegang tot afdelingsdocumenten / groepen / shares • toekennen/intrekken (generieke) rollen in gekoppelde systemen, ten minste in Active Directory en Microsoft Entra ID, TOPdesk en SIMS De regels moeten onderscheid kunnen maken in afdeling, locatie, herkomstbron van identiteitsgegevens, functie, manager en diverse contexten etc
11.22	Werkorder/ticket: Mogelijkheid om een mutatie ten aanzien van een persoonsgegeven (accounts en autorisaties) als een werkorder te melden aan een functioneel beheerder van een niet aan IAM gekoppeld relevant systeem. Dit verloopt via een ticket in een servicemanagement tool (momenteel TOPdesk).
11.23	Tweerichtingsverkeer: Mogelijkheid bieden om koppelingen twee richtingen op te laten werken, zodat

	bijvoorbeeld ook bepaalde gegevens, zoals het bedrijfse-mailadres, gemuteerd kunnen worden in het HR systeem dat als primaire bron wordt gehanteerd.

1.12. Gebruiksgemak

12.1	Eindgebruikersportaal: Het eindgebruikers portaal moet Nederlandstalig kunnen worden ingesteld.

1.13. Governance

13.1	Rollenoverzicht: Mogelijkheid bieden aan rollenbeheerders om een overzicht te krijgen met de medewerkers en afdelingen per rol
13.2	Audittrail: Mogelijkheid bieden om van elke IAM transactie vast te leggen en real time te kunnen bekijken: • wie • wanneer • welke transactie (was-wordt) heeft uitgevoerd of heeft laten uitvoeren
13.3	Inzicht in autorisaties: Mogelijkheid om te kunnen constateren welke autorisatie/rol een persoon op enig moment heeft gehad.
13.4	Inzicht in autorisaties: Mogelijkheid bieden om alle natuurlijke identiteiten en autorisaties in kaart te brengen en op basis hiervan te bepalen of deze accounts rechten moeten krijgen of al dan niet verwijderd moeten worden. Deze kunnen alsnog de rechten krijgen of ingetrokken worden.
13.5	Functiescheidingsoverzicht: Mogelijkheid bieden om vast te stellen welke gedefinieerde conflicterende autorisaties/rollen aan een medewerker zijn toegekend, voor hoe lang en door wie.
13.6	Functiescheiding beoordeling: Mogelijkheid bieden om gedefinieerde rolconflicten over systemen heen te beoordelen.
13.7	Delegatie: Mogelijkheid bieden om taken van IAM rollen (lijnmanager, rolbeheerder etc.) te delegeren aan andere IAM-gebruikers en om de delegatie weer in te trekken.

13.8	Wachtwoordenbeleid: Mogelijkheid bieden om het op enig moment geldende wachtwoordenbeleid te presenteren aan gebruikers, beheerders en auditors.
13.9	Verplichte velden: Mogelijkheid om invoervelden in schermen verplicht te maken, bijvoorbeeld een toelichtingenveld bij een mutatie.
13.10	Beperking export van data: Mogelijkheid om export van data te beperken via configuratie van velden en doelgroepen of via standaard voor gedefinieerde rapporten.
13.11	Rapportages: Mogelijkheid dat in het portaal rapportages direct door gebruikers te genereren zijn als pdf, printbestand, xls en csv met zelf te selecteren attribuutvelden en query's.
13.12	Role based toegang tot IGA portaal: Het IGA portaal dient rol gebaseerde autorisaties te kennen zodat het mogelijk wordt om verschillende gebruikersgroepen verschillende gebruikersfuncties toe te kennen, bijvoorbeeld auditors die read-only toegang moeten hebben.