

Programma van eisen IAM

Bijlage A

Dossiernummer : 000009228

TenderNed kenmerk : 618459

Datum : 14 Oktober 2026



Veiligheidsregio
Utrecht

vru.nl



De door de opdrachtnemer te verrichten werkzaamheden dienen te geschieden conform de eisen als beschreven in dit programma van eisen en conform de voorwaarden genoemd in de offerte uitvraag. Door een Inschrijving in te dienen verklaart Inschrijver onvoorwaardelijk akkoord te gaan met alle eisen in het programma van eisen. Daar waar in dit programma van eisen wordt gesproken over een werkdag wordt hiermee bedoeld een kalenderdag behoudens zaterdagen, zondagen en algemeen erkende feestdagen in de zin van artikel 3 lid 1 Algemene termijnenwet.

1. Commercieel, contractueel en leveranciersmanagement

Nr.	Omschrijving eis
1.1	Aanpassingen / releases worden middels een vooraf afgestemd schema, goed gedocumenteerd uitgevoerd. opdrachtgever wordt ruim van te voren op de hoogte gesteld van de aanpassingen.
1.2	De opdrachtnemer borgt dat alle software, componenten, modules, diensten en cloudvoorzieningen van derden die worden gebruikt binnen of ter ondersteuning van de SaaS-dienst voldoen aan de eisen en voorwaarden uit dit Programma van Eisen. Dit geldt ongeacht of deze onderdelen zelfstandig of in combinatie met de eigen dienstverlening van de opdrachtnemer aan VRU beschikbaar worden gesteld. De opdrachtnemer blijft verantwoordelijk voor de naleving van deze eisen door derde partijen
1.3	De opdrachtnemer blijft gedurende de contractperiode onderhoud, ondersteuning en beveiligingsupdates leveren op de door VRU gebruikte SaaS-dienst. Indien de opdrachtnemer besluit de SaaS-dienst te vervangen door een nieuwe of opvolgende dienst, release of versie en het onderhoud op de bestaande SaaS-dienst te beëindigen, waarborgt de opdrachtnemer dat VRU zonder meerkosten kan overstappen naar en gebruik kan maken van de opvolgende dienst, release of versie. Daarbij blijven de overeengekomen functionaliteiten, servicelevels, koppelingen en contractuele afspraken onverkort van kracht.
1.4	Indien Opdrachtnemer zelf een storing constateert aan één van de onderdelen van het systeem, informeert Opdrachtnemer zo snel als mogelijk Opdrachtgever met een duidelijke omschrijving van het gevolg van het geconstateerde probleem.
1.5	Indien bij Opdrachtgever tijdens de looptijd behoefte ontstaat aan producten en aanvullende diensten welke binnen scope van de opdracht vallen, maar die niet in dit PVE omschreven staan, dient Opdrachtnemer hieraan mee te werken.
1.6	Dit wordt gezien als een aanvullende opdracht die Opdrachtnemer uitvoert als onderdeel van de opdracht. Opdrachtnemer neemt deze na overleg (en goedkeuring aanvullende offerte) op in de dienstverlening. Hierbij valt te denken aan, bijvoorbeeld maar niet uitsluitend, de koppeling met andere softwaresystemen.



Nr.	Omschrijving eis
1.7	De opdrachtnemer maakt bij de opslag van gegevens gebruik van fysieke opslag en verwerking binnen de Europese Economische Ruimte (EER) en zorgt ervoor dat doorgifte van gegevens naar landen buiten de Europese Economische Ruimte (EER) uitgesloten is.
1.8	De opdrachtnemer verleent bij beëindiging van de overeenkomst volledige medewerking aan een beheerste exit en overdracht van de SaaS-dienstverlening aan VRU of een door VRU aangewezen opvolgende partij, inclusief overdracht van data, configuratie, documentatie, koppelingen, autorisatiemodellen, workflows en benodigde kennis om de dienstverlening te kunnen voortzetten.
1.9	Opdrachtnemer is niet gerechtigd het gebruik van de SaaS-dienst door technische maatregelen te belemmeren of te blokkeren, behalve nadat Opdrachtnemer de VRU in gebreke heeft gesteld ten aanzien van een aan de VRU toerekenbaar tekortschieten in de nakoming van haar verplichtingen uit de Overeenkomst.
1.10	Opdrachtnemer/leverancier van het aan te kopen systeem werkt mee aan het uitvoeren van een Data Protection Impact Assessment (DPIA). Van opdrachtnemer wordt verwacht dat alle technische en organisatorische maatregelen genomen worden die naar de stand der techniek verwacht mogen worden, gebaseerd op de aard van de gegevens en de verwerking.
1.11	De Opdrachtnemer verplicht zich tot verbeteren / vernieuwen / bijhouden en tijdig realiseren van deze verbeteringen c.q. wijzigingen in de Oplossing naar aanleiding van nieuwe of gewijzigde wet- en regelgeving en landelijke standaarden voor overheden zonder hiervoor extra kosten in rekening te brengen.
1.12	De opdrachtnemer levert de oplossing compleet en bedrijfsvaardig op.
1.13	Informatieobjecten en bijbehorende metadata dienen onherstelbaar vernietigd te kunnen worden op basis van de als zoekcriteria (metadata) opgegeven waardering/vernietigingstermijn.
1.14	Opdrachtnemer en de oplossing voldoen aan alle eisen zoals gesteld in de privacywetgeving Algemene Verordening Gegevensbescherming (AVG/GDPR) en andere relevante wet- en regelgeving op het gebied van privacy en gegevensbescherming.



Nr.	Omschrijving eis
1.15	De in de applicatie opgeslagen data blijft duurzaam toegankelijk gedurende de looptijd van de overeenkomst, e.e.a. conform dit Programma van Eisen, behoudens conform protocol vernietigde data.
1.16	De opdrachtnemer dient aantoonbaar gecertificeerd te zijn volgens de ISO27001 of een gelijkwaardige norm voor informatiebeveiliging en maakt voor de VRU de bijbehorende SoA (Statement of Applicability) inzichtelijk.
1.17	De VRU heeft te allen tijde recht op het uitvoeren van een onafhankelijke externe audit op het gebied van informatiebeveiliging, of opdrachtnemer laat door een onafhankelijke externe partij een dergelijke audit uitvoeren (minimaal 1x per jaar) en deelt de uitkomst transparant met de VRU.
1.18	In het rapport of de bijlage bij de uitkomst van de audit zoals in E68 beschreven staat wat er is geconstateerd, welke maatregelen opdrachtnemer gaat nemen en binnen welke periode dit zal zijn uitgevoerd.
1.19	De opdrachtnemer borgt dat informatieobjecten en bijbehorende metadata die persoonsgegevens bevatten of kunnen bevatten, op basis van vastgelegde bewaartermijnen, vernietigingstermijnen en metadata-zoekcriteria onherstelbaar kunnen worden vernietigd. Vernietiging vindt plaats conform de AVG, het bewaarbeleid van VRU en de overeengekomen vernietigingsprocedure.
1.20	Opdrachtnemer heeft met alle onderaannemers een contract met hierin een clause informatiebeveiliging/geheimhouding.
1.21	Opdrachtnemer conformeert zich aan de eisen van de GIBIT 2025.
1.22	Voor het vastleggen van de afspraken m.b.t. de verwerking van gegevens wordt gebruik gemaakt van de verwerkersovereenkomst van de VRU. Deze verwerkersovereenkomst is ook van toepassing op eventuele onderaannemers van opdrachtnemer indien dit nodig mocht zijn als verwerker van vertrouwelijke (w.o. persoons-)gegevens. Opdrachtnemer is verantwoordelijk voor de naleving van de verwerkersovereenkomst door haar onderaannemers.
1.23	Alle gegevens binnen de oplossing, dan wel ter beschikking gesteld aan de opdrachtnemer ten behoeve van de opdracht blijven te allen tijde eigendom van de VRU.



Nr.	Omschrijving eis
1.24	De opdrachtnemer waarborgt dat alle in de SaaS-dienst opgeslagen data gedurende de looptijd van de overeenkomst duurzaam toegankelijk blijft voor VRU. De data blijft beschikbaar, leesbaar, integer, raadpleegbaar en exporteerbaar, conform de eisen uit dit Programma van Eisen en de overeengekomen bewaartermijnen. Data mag uitsluitend worden vernietigd op basis van een vooraf vastgesteld en met VRU afgestemd vernietigingsprotocol.
1.25	Alle door opdrachtnemer aangeboden diensten vallen binnen een door opdrachtnemer of zijn onderaannemers gebruikt ISMS (Information Security Management System), dat gecertificeerd is conform de ISO27001 of een gelijkwaardige norm.
1.26	De tarieven en prijzen dienen met een nauwkeurigheid van twee decimalen te worden ingevuld.
1.27	In geval van Onduidelijkheden in facturen behoudt Opdrachtgever zich het recht voor pas over te gaan tot betaling nadat Opdrachtnemer duidelijkheid heeft verstrekt.
1.28	Opdrachtnemer heeft een actieve procedure "meldplicht datalekken". Opdrachtnemer informeert de VRU hierover onmiddellijk na constateren en geeft aan welke eisen opdrachtnemer aan de VRU hierover stelt. Wanneer er sprake is van een datalek vanuit de oplossing door een lek in de software/programmatuur dan dient de opdrachtnemer hier direct actie op te ondernemen en de VRU hierop te attenderen. Indien de oorsprong van de oorzaak betrekking heeft op de infrastructuur van VRU dan zal de opdrachtnemer de VRU daarop direct moeten attenderen alsmede te adviseren wat de VRU daaraan kan doen.
1.29	Uw Inschrijving bevat gespecificeerde all-in tarieven voor de gevraagde dienstverlening, conform de eisen die vermeld staan in dit Beschrijvend document en alle bijbehorende Bijlagen. De geoffreerde tarieven zijn gebaseerd op genoemde specificaties. Alle gegeven antwoorden betreffende de gunningscriteria zijn onderdeel van de Inschrijving van de Inschrijver en zijn onderdeel van de aangeboden tarieven.
1.30	Meerwerk, conform een extra opdracht buiten de reguliere dienstverlening (bijvoorbeeld bij projecten of grote events), mag alleen na schriftelijke toestemming van de Opdrachtgever gefactureerd worden. Meerwerk dient separaat van de reguliere dienstverlening, op een aparte factuur, gefactureerd te worden.



Nr.	Omschrijving eis
1.31	Opdrachtnemer verplicht zich ondersteuning te bieden aan Opdrachtgever (m.n. functionele beheerders) rondom het beheer en onderhoud van de functionaliteit van de oplossing en de daarin gebruikte bedrijfsinformatie, d.w.z. het instellen van de (functionele) parameters en de inhoud van databases.
1.32	Opdrachtnemer stuurt maximaal één verzamel factuur per maand.
1.33	Opdrachtnemer is bereid medewerking te verlenen aan het factureren en afhandelen van facturen door middel van een geautomatiseerd systeem van Opdrachtgever, voor zover dit nog niet als eis is opgenomen in één of meer onderdelen van dit PVE.
1.34	De Opdrachtnemer garandeert, conform de Archiefwet, dat Opdrachtgever zorgdrager voor / eigenaar van de informatie van Opdrachtgever blijft ongeacht de opslaglocatie van de informatie en de relatie met de Opdrachtnemer.
1.35	Indien de overeenkomst eindigt, ongeacht de reden voor beëindiging, dienen alle eigendommen van de VRU, inclusief systeem en data, te worden overgedragen aan de opdrachtgever binnen een redelijke termijn, in een formaat dat voor andere systemen bruikbaar is.
1.36	Indien producten en/of diensten worden toegevoegd aan de dienstverlening, of worden doorontwikkeld, dienen de hiervoor aangeboden prijzen marktconform te zijn. Opdrachtgever heeft het recht om de prijzen hierop te toetsen. Indien blijkt dat de aangeboden prijzen niet marktconform zijn, gaan Opdrachtnemer en Opdrachtgever in overleg. Indien dit niet leidt tot een bevredigende oplossing voor beide partijen, behoudt Opdrachtgever zich het recht voor de betreffende producten en/of diensten bij een derde partij af te nemen.
1.37	Opdrachtnemer stuurt voor de 10e van de maand de factuur in betreffende de volgende kalendermaand.



2. Dienstverlening en beheer

Nr.	Omschrijving eis
2.1	De Opdrachtnemer handelt service meldingen adequaat en binnen de afgesproken termijn vastgelegd in de SLA af.
2.2	Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken servicelevels en het doorvoeren van veranderingen en verbeteringen (vastgelegd in evt. verbeterplannen) is regelmatig overleg op diverse organisatieniveaus noodzakelijk. Periodiek vindt overleg plaats tussen de VRU en Opdrachtnemer over deze dienstverlening. Daarnaast zullen in het kader van verlengingen van het contract evaluaties tussen beide Partijen plaatsvinden. Deze structuren worden vastgelegd in de SLA.
2.3	Opdrachtnemer rapporteert periodiek (ten minste éénmaal per kwartaal) over de voortgang van de realisatie van eventuele verbeterplannen .
2.4	Opdrachtnemer zorgt in het geval van een security incident dat data niet verloren gaat en heeft hiervoor aantoonbaar afdoende maatregelen genomen. Opdrachtnemer stelt de verzamelde data beschikbaar voor eventueel onderzoek bij een derde partij.
2.5	Opdrachtnemer hanteert een prioriteitenmethode of een andere methode waarbij er direct hulp wordt geboden bij incidenten met hoge impact en hoge urgentie, d.w.z. issues waarbij de oplossing niet werkt voor meer dan 1 persoon.
2.6	Gepland Onderhoud vindt uitsluitend op werkdagen plaats tussen 21:00u en 7:00u CET. Dag en tijdstip worden tenminste vijf (5) kalenderdagen vooraf gecommuniceerd aan de organisatie, waarbij duidelijk wordt gemaakt waarvoor Onderhoud nodig is, en hoe lang het maximaal gaat duren.
2.7	Opdrachtnemer verplicht zich om de VRU op de hoogte te houden van factoren die van invloed kunnen zijn op de bestaande dienstverlening, als input voor het verder ontwikkelen van de dienstverlening (bijv. nieuwe componenten).
2.8	Opdrachtgever sluit na definitieve gunning een SLA af met Opdrachtnemer waarin nadere afspraken worden gemaakt over de te leveren dienstverlening, binnen de kaders van en in overeenstemming met het Programma van Eisen, beschrijvend document en de Overeenkomst.
2.9	Opdrachtnemer verplicht zich ondersteuning te bieden aan de VRU (m.n. functionele beheerders) rondom het beheer en onderhoud van de functionaliteit van de oplossing en de daarin gebruikte bedrijfsinformatie, d.w.z. het instellen van de (functionele) parameters en de inhoud van databases.



Nr.	Omschrijving eis
2.10	Van de opdrachtnemer wordt verwacht dat zij: 1. Kan beoordelen wat de impact is van geplande veranderingen 2. Afwijkingen en oorzaken van fouten kan vaststellen 3. Onderdelen kan identificeren die gewijzigd moeten worden
2.11	Leverancier dient een technisch aanspreekpunt of supportkanaal te bieden voor integratievraagstukken.
2.12	Opdrachtnemer verplicht zich ervoor te zorgen dat ondersteunende documentatie voor gebruikers en beheerders compleet, correct en up-to-date is.
2.13	De helpdesk is ook beschikbaar via een webportaal. Vragen, meldingen van incidenten en wijzigingsvoorstellen kunnen op alle dagen 24 uur per dag online worden ingediend (formulier). Dergelijke online vragen, meldingen van incidenten en wijzigingsvoorstellen worden automatisch per mail bevestigd en daarmee geregistreerd. Tevens kan de voortgang van deze incidenten en wijzigingsmeldingen digitaal worden geraadpleegd en gevolgd.
2.14	Voor onderhoud en updates kan de inschrijver terugvallen op meerdere programmeurs / consultants met dezelfde kennis en expertise
2.15	Alle gesprekken die gevoerd zullen worden tussen Opdrachtgever en Opdrachtnemer dienen kosteloos te zijn voor de Opdrachtgever en worden geacht bij de aangeboden tarieven te zijn inbegrepen.
2.16	Opdrachtnemer treft voldoende maatregelen teneinde continuïteit van de oplossing te kunnen garanderen, zelfs in het geval waar normaliter een overmachtssituatie zou heersen (bijvoorbeeld bij rampen, calamiteiten, of faillissement van opdrachtnemer). In zulke situaties moet Opdrachtgever de mogelijkheid hebben om zelf, of door derden, beheer, onderhoud en ontwikkeling aan de oplossing te laten plegen.
2.17	Opdrachtnemer heeft een actieve incidentprocedure m.b.t. de communicatie rondom informatiebeveiligingsincidenten met haar klanten. De VRU wordt door de opdrachtnemer benaderd als zij een incident constateren.
2.18	Opdrachtnemer hanteert een prioriteitenmethode of een gelijkwaardige methode waarbij er direct hulp wordt geboden bij incidenten met hoge impact en hoge urgentie, d.w.z. issues waarbij de oplossing niet werkt voor meer dan 1 persoon.



Nr.	Omschrijving eis
2.19	In de rapportage over de dienstverlening is informatiebeveiliging een specifiek onderdeel. Bij het opstellen van de SLA wordt bepaald over welke KPI's er gerapporteerd wordt.
2.20	Opdrachtnemer zorgt voor patchmanagement, waarbij (beveiligings)patches zo spoedig mogelijk worden geïnstalleerd. Dit zal in de SLA worden gespecificeerd.
2.21	De opdrachtnemer verplicht zich om in het geval van een calamiteit of ramp die de kritische processen van opdrachtnemer raakt, de afgesproken dienstverlening aan VRU binnen 48 uur te continueren. NB Deze eis heeft betrekking op de dienstverlening van opdrachtnemer, niet op de oplossing. Een calamiteit wordt in dit kader gedefinieerd als een ongewenste gebeurtenis die zodanige negatieve gevolgen heeft dat de voortgang van de kritische bedrijfsprocessen van de opdrachtnemer wordt verstoord en de maximale uitvalsduur van deze kritische bedrijfsprocessen dreigt te worden overschreden.
2.22	Regulier gepland onderhoud wordt minimaal twee weken van tevoren aangekondigd.
2.23	Gebruikersbegeleiding: de oplossing moet voorzien in gebruikersbegeleiding en ondersteuning, zoals tooltips, helpdocumentatie en trainingsmateriaal, om gebruikers te helpen bij het effectief gebruik van het systeem.
2.24	De opdrachtnemer houdt de aangeboden oplossing proactief in lijn met de landelijke afgesproken standaarden die betrekking hebben op ICT-standaarden.
2.25	Opdrachtnemer beoordeelt door de VRU gemelde monitoringbevindingen binnen een redelijke termijn, communiceert hierover transparant en treft waar nodig passende corrigerende of mitigerende maatregelen. Herstel- en mitigatietermijnen worden risico gebaseerd vastgesteld op basis van aard, ernst en impact van de bevinding.
2.26	Beschikbaar stellen van een lijst met bestaande connectoren/koppelingen naar mogelijke doelsystemen.
2.27	De Opdrachtnemer biedt Nederlandstalige opleidingen en opleidingsdocumentatie voor de beheerders aan. Deze zijn actueel en gebaseerd op de door de Opdrachtnemer aangeboden versie van de oplossing. Dit geldt ook bij updates van de oplossing.



Nr.	Omschrijving eis
2.28	Per kwartaal wordt door Opdrachtnemer een managementrapportage opgeleverd met daarin tenminste: Overzicht van de geleverde producten / licenties (actief en inactief) gespecificeerd naar aantallen. - De kosten van het afgelopen kwartaal. - De totale kosten die zijn gefactureerd. De gegevens zullen door Opdrachtgever worden gebruikt ter bewaking van de contractuele afspraken In overleg tussen Opdrachtgever en Opdrachtnemer kan de managementrapportage naar behoefte inhoudelijk worden gewijzigd.
2.29	Normen t.a.v. respons- en oplostijden worden opgenomen in de specifieke SLA of DAP tussen Opdrachtnemer en Opdrachtgever.
2.30	De Opdrachtnemer wijst een accountmanager aan, die een vast aanspreekpunt wordt voor de Opdrachtgever. Deze persoon beschikt over een dusdanige positie binnen de organisatie dat hij of zij de belangen van de Opdrachtgever op een adequate wijze kan borgen en bevoegd is tot het nemen van beslissingen. Tevens wordt er een back-up functionaris aangewezen. Bij afwezigheid van de vaste accountmanager, kan deze vervanger alle zaken snel en effectief overnemen.
2.31	Onder een adequate afhandeling van meldingen wordt verstaan een persoon of loket die fungeert als helpdesk. Hier kan de Opdrachtgever meldingen van storingen, vragen, verzoeken, klachten, etc. neerleggen, zowel per mail als telefonisch en via een webportaal. Deze helpdesk dient telefonisch op werkdagen tijdens reguliere kantoortijden bereikbaar te zijn.
2.32	Van iedere service melding is de prioriteit en voortgang zichtbaar. Een melding wordt alleen in overleg met Opdrachtgever gesloten of gereed gemeld.
2.33	De Opdrachtnemer levert na de gunning handleidingen en het opleidingsmateriaal op aan de functioneel beheerder van Opdrachtgever. Levering dient plaats te vinden vóór de testfase en vóór de start van de implementatie.



Nr.	Omschrijving eis
2.34	De opdrachtnemer borgt dat nieuwe versies en releases van de SaaS-dienst geen negatieve impact hebben op de bestaande werking van koppelingen, dataspecificaties, hulpprogramma's, software en databestanden die VRU gebruikt in combinatie met de SaaS-dienst. Nieuwe releases zijn backwards compatible, zodat aanpassing, ombouw of herconfiguratie aan de zijde van VRU niet noodzakelijk is. Indien een wijziging toch impact heeft op de inrichting of koppelingen van VRU, wordt dit vooraf gemeld, onderbouwd en afgestemd met VRU.
2.35	De opdrachtnemer van de oplossing verzorgt een Nederlandstalige helpdesk, welke als 'single point of contact' dienst doet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, alsook voor informatie over de afhandeling daarvan. De helpdesk is tenminste telefonisch bereikbaar van 8.30 uur tot 17.00 uur op werkdagen. In de SLA geeft inschrijver de omgang, respons- en oplostijden aan met aangemelde incidenten.
2.36	Alle door de Opdrachtnemer direct ten behoeve van de VRU ingezette personeelsleden dienen de Nederlandse taal in woord en geschrift te beheersen, zodanig dat er gesprekken gevoerd kunnen worden en instructies gegeven kunnen worden in de Nederlandse taal.
2.37	De accountmanager o f diens vervanger, zijn telefonisch bereikbaar op maandag t/m vrijdag van 08.30 tot 17.00 uur. Beide personen dienen te beschikken over een goede mondelinge en schriftelijke uitdrukkingsvaardigheid in de Nederlandse taal. Indien er wijzigingen zijn in de contactgegevens van de contactpersoon of de vervanger, wordt dit direct doorgegeven aan de contractbeheerder van de Opdrachtgever.



3. Functioneel

Nr.	Omschrijving eis
3.1	Als de oplossing gebruik maakt van standaard autorisatie rollen levert de Opdrachtnemer een autorisatiematrix op, met daarin de standaardrollen en welke functies die rol mag uitvoeren b.v. invoeren, muteren, publiceren, verwijderen etc.
3.2	Rollen met verhoogd risico moeten op basis van attributen worden voorzien van aanvullende toewijzingsvoorwaarden, waarbij functiescheiding (SoD) en beleidsregels technisch worden afgedwongen. Het systeem moet rollen kunnen classificeren op basis van risicokenmerken en attributen, zodat conflicterende rolcombinaties worden herkend en geblokkeerd of gemitigeerd.
3.3	Standaard mutaties kunnen elektronisch worden goedgekeurd door goedkeurders.
3.4	Account disablen (bijv. Op basis van incidentmelding) moet ook daadwerkelijk resulteren in een geblokkeerd account (niet doordat er nog een actief contract in AFAS staat, dat het account dan weer online komt)
3.5	De aangeboden oplossing ondersteunt AFAS als leidend bronsysteem voor het automatisch aanmaken en beheren van identiteiten binnen het IAM-systeem. Daarnaast moet het mogelijk zijn om identiteiten vanuit andere Identity Providers of bronsystemen toe te voegen. Voor identiteiten die niet vanuit een gekoppeld bronsysteem worden aangeleverd, zoals externe medewerkers, moet het mogelijk zijn deze handmatig via een selfserviceportaal binnen het IAM-systeem aan te maken en te beheren.
3.6	De tooling moet externe gebruikers (guests) kunnen uitnodigen binnen Microsoft Entra ID en deze, op basis van functie en/of rol, automatisch kunnen toewijzen aan de juiste groepen voor toegang tot Microsoft Teams en andere gekoppelde applicaties.
3.7	Duidelijke documentatie van het datamodel, de API's en de integratiemogelijkheden is vereist.
3.8	De oplossing moet Real-time of geplande extractie van data faciliteren
3.9	De opdrachtnemer stelt de applicatie beschikbaar als SaaS-dienst via een webportal. Voor het gebruik van de applicatie zijn geen lokale installaties binnen de VRU-omgeving vereist.
3.10	Indien opdrachtnemer software ontwikkelt (zelf of via onderaannemers), hanteert opdrachtnemer aantoonbaar het principe "security by design" en "privacy by design".



Nr.	Omschrijving eis
3.11	De Oplossing moet aansluiten op de standaard dienst (autorisatie): 'organisatie eenmalig aanloggen' Nu gerealiseerd door Microsoft Entra ID SSO/MFA.
3.12	Opdrachtnemer maakt inzichtelijk welke normen van het Forum Standaardisatie op https://www.forumstandaardisatie.nl/open-standaarden-zijn-toegepast .
3.13	De opdrachtnemer staat toe dat de digitale gebruikershandleiding van de oplossing (wanneer niet beschikbaar via de oplossing) op het interne netwerk van de VRU beschikbaar wordt gesteld.
3.14	De aangeboden oplossing ondersteunt het automatisch toekennen van één of meerdere rollen aan een identiteit op basis van kenmerken en attributen uit bronsystemen. Hierbij moeten kenmerken zoals afdeling, team, functie of andere organisatorische attributen kunnen worden gebruikt als voorwaarden voor roltoewijzing. Wanneer een identiteit aan de gestelde criteria voldoet, moeten de bijbehorende rollen automatisch aan deze identiteit kunnen worden gekoppeld.
3.15	Opdrachtnemer past het principe van "least-privilege" en "need to know" toe en beperkt zo de toegang tot het noodzakelijke. Permissie/rechten-niveaus zijn door de Opdrachtgever te configureren na oplevering.
3.16	Het systeem ondersteunt functiescheiding en biedt de mogelijkheid om toegangsbeperkingen in te stellen en af te dwingen op basis van rollen en individuele identiteiten.
3.17	De aangeboden oplossing ondersteunt een koppeling met AFAS waarmee functiegegevens, organisatorische positionering en andere relevante gebruikersattributen kunnen worden opgehaald. Hierbij moet de positie van de medewerker binnen de organisatiestructuur inzichtelijk zijn op basis van kenmerken zoals functie, afdeling, team, domein en vestiging. Deze gegevens moeten binnen het IAM-systeem als attributen kunnen worden gebruikt voor het bepalen en toekennen van rollen en autorisaties.
3.18	De aangeboden oplossing ondersteunt een koppeling met een servicemanagementsysteem waarmee via een ticketsysteem autorisaties kunnen worden aangevraagd. De aangevraagde autorisaties moeten vervolgens automatisch door het IAM-systeem of na goedkeuring door een rolbeheerder kunnen worden toegekend.



Nr.	Omschrijving eis
3.19	Het systeem ondersteunt koppelingen met cloudapplicaties, zoals SharePoint en Microsoft Teams, en biedt functionaliteit voor het beheren van identiteiten, rollen en bijbehorende autorisaties binnen deze cloudomgevingen.
3.20	De aangeboden oplossing ondersteunt het ophalen van aanvullende attributen uit aangesloten bronsystemen, naast de standaard beschikbare attributen. Het moet mogelijk zijn om deze attributen aan te wijzen en te gebruiken als criteria voor het bepalen, aanmaken en toekennen van rollen aan identiteiten.
3.21	De Oplossing moet het mogelijk maken om beheerhandelingen op gebruikersaccounts vanuit het IAM-systeem te initiëren en door te voeren in gekoppelde Doelsystemen, ten minste voor Active Directory. Hieronder vallen minimaal het resetten van wachtwoorden en het disablen van gebruikersaccounts.
3.22	De oplossing moet compatibel zijn met Azure Data Factory, Power BI en gangbare ETL-tools zoals Python, PowerShell en SQL.
3.23	Standaard mutaties kunnen elektronisch worden goedgekeurd door leidinggevendenden
3.24	De oplossing ondersteunt periodieke controles waarbij autorisatie-eigenaren bestaande rechten kunnen beoordelen en bevestigen of intrekken. (Access Review)
3.25	Goedkeurder kan ook een andere rol zijn dan leidinggevende (bijv. in het geval van uitgifte licenties/devices)
3.26	De oplossing kan de herkomst tonen van de bron of toegangsstroom per identiteit.
3.27	Mobiele toegang: de oplossing is compatibel met mobiele apparaten, zodat gebruikers toegang hebben tot het systeem vanaf verschillende apparaten, zoals PC's, smartphones en tablets, voor flexibiliteit en gebruiksgemak. Het systeem is responsive.
3.28	Autorisaties op rollen en andere groepen kunnen genest worden. Dit betekent bijvoorbeeld dat een rol een andere rol kan bevatten. Voorbeeld: een redacteur kan algemene redactierechten hebben, maar ook rechten voor specifieke onderdelen van de website, terwijl een andere redacteur die rechten niet heeft, maar b.v. weer andere acties op de site kan doen.
3.29	Binnen de aangeboden oplossing kan de beheerder een overzicht genereren van alle gebruikers met toegekende autorisaties.



Nr.	Omschrijving eis
3.30	De aangeboden oplossing ondersteunt een rollenmodel waarin binnen het IAM-systeem één business role kan bestaan uit meerdere applicatierollen. Per applicatierol moet inzichtelijk zijn aan welk doelsysteem en welke applicatiegroep deze is gekoppeld en welke autorisaties daarmee binnen het betreffende doelsysteem worden toegekend. Hierdoor moet vanuit de business role zichtbaar zijn tot welke systemen, applicatiegroepen en informatie de gekoppelde identiteiten toegang verkrijgen.
3.31	De oplossing moet mogelijkheden bieden om data en rollen te classificeren.
3.32	Een gebruiker kan meerdere rollen hebben binnen de oplossing. Hij of zij kan toegang hebben tot meerdere autorisatieniveaus.
3.33	De Oplossing moet integraties ondersteunen met systemen binnen de VRU, waaronder de in gebruik zijnde HRM-software (AFAS), Active Directory, Microsoft 365, CMS-systemen en databases, zodat gegevens en autorisatie-informatie naadloos tussen de verschillende systemen en platforms kunnen worden uitgewisseld.
3.34	De oplossing moet mogelijkheden bieden voor logging en monitoring van data-opvragingen en extracties .
3.35	opdrachtgever heeft de mogelijkheid om opdrachtgever-specifieke workflows op te stellen en in te richten al dan niet met hulp van opdrachtnemer
3.36	Het systeem moet een veilige activatieprocedure voor nieuwe gebruikers ondersteunen, conform de actuele beveiligingsrichtlijnen (zoals MFA en gescheiden mails)
3.37	De Oplossing moet naast medewerkers die via de koppeling met het HR-systeem automatisch in het IAM-systeem worden aangemaakt, ook gastaccounts en andere externe identiteiten kunnen registreren en beheren. Gastaccounts, waaronder accounts voor leveranciers en andere externe personen, moeten vanuit het IAM-systeem kunnen worden opgevoerd, zichtbaar zijn en gedurende hun levenscyclus vanuit het IAM-systeem kunnen worden beheerd, waaronder gastaccounts in Entra ID.
3.38	De aangeboden oplossing is koppelbaar met AFAS om identiteitsgegevens bij gebruikers en/of medewerkers in AFAS te wijzigen.
3.39	De aangeboden oplossing is koppelbaar met AFAS zodat functiegegevens en aanverwante informatie over gebruikers als attributen te gebruiken is om rechten en rollen te bepalen.



Nr.	Omschrijving eis
3.40	Systeem dient accounts en groepen te kunnen aanmaken in AD. Een nieuwe oplossing gaat tijdens de implementatiefase ook groepen in de bestaande Active Directory moeten kunnen maken, zodat bij de overgangsperiode AD en het systeem wederzijds mutaties kunnen verwerken;
3.41	Het IAM-systeem ondersteunt het creëren van een unieke identifier op basis van attributen uit bron-, doel- en cloudsysteem, waaraan authenticatievoorzieningen zoals SSO en MFA kunnen worden gekoppeld.
3.42	Er worden workflows opgesteld / ingericht voor het aanvragen van additionele rollen en rechten door een medewerker.
3.43	De Oplossing moet de mogelijkheid bieden om inactieve rollen, gebruikers zonder rollen en rollen zonder members/gebruikers te detecteren en rapporteren.
3.44	Het moet mogelijk zijn op basis van de identiteitsgegevens die binnen de oplossing bekend zijn exports te maken en identiteiten toe te voegen aan gekoppelde doelsystemen.
3.45	De risicoscore van een Autorisatie moet gebruikt kunnen worden om meldingen en corrigerende maatregelen te triggeren wanneer een overtreding is gedetecteerd.
3.46	De Oplossing toont in het autorisatiemodel welke rollen uitdeelbaar zijn en door wie en kan hier een rapportage van uitdraaien.
3.47	Het moet mogelijk zijn om binnen de oplossing identiteiten op basis van kenmerken uit bronsystemen te koppelen aan rollen.
3.48	Op basis van de rol wordt in de doelapplicaties toegang gegeven en/of autorisaties gezet voor de identiteiten die gekoppeld zijn aan de rol.
3.49	Het moet mogelijk zijn om naast eventuele standaardvelden ook extra velden op te halen vanuit de bronsystemen die gebruikt kunnen worden om identiteiten te koppelen aan rollen.
3.50	Het systeem ondersteunt het beleggen van eigenaarschap voor rollen, autorisaties en informatiebronnen, zodat per object duidelijk is wie verantwoordelijk is voor het beheer en de beschikbaarstelling ervan.
3.51	Naast de standaard profielen kunnen er ook extra rechten worden aangevraagd, eventueel via ons ticketsysteem. Goedgekeurde aanvragen dan kunnen via een koppeling naar de IAM oplossing worden overgezet ter uitvoering.



Nr.	Omschrijving eis
3.52	Systeem dient accounts en groepen te kunnen muteren in AD. Tijdens de overgangsperiode tussen inrichting van de oplossing en de huidige situatie moeten zowel indienst- en uitdiensttredingen als mutaties in de AD en de oplossing kunnen worden uitgevoerd.
3.53	Vervanging kan per begin- en einddatum worden ingevoerd en toegangsrechten verlopen automatisch wanneer einddatum verstreken is
3.54	Aan iedere gebruiker kunnen automatisch basis-autorisaties worden toegewezen.
3.55	Het is mogelijk autorisaties in te richten per individuele gebruiker, per gebruikersgroep en/of per organisatieonderdeel.
3.56	De oplossing moet rechten automatisch kunnen intrekken wanneer een gebruiker uit dienst treedt of van functie wijzigt. (Joiner-Mover-Leaver)
3.57	Het systeem heeft een helder rechten- en rollensysteem (toegang en autorisatie) voor de autorisaties binnen de oplossing zelf.
3.58	Het moet mogelijk zijn om externen met een identiteit van buiten het VRU netwerk te koppelen aan een rol.
3.59	Medewerker heeft de mogelijkheid om zelf additionele rechten aan te vragen
3.60	Functies en rollen moeten kunnen worden aangemaakt als Active Directory- en/of Entra ID-groepen, zodat deze gebruikt kunnen worden voor applicatietoegang en rechtenbeheer.
3.61	Naast identiteiten aangeleverd door het HR-systeem (of andere bronsystemen) moeten ook identiteiten handmatig opgevoerd kunnen worden



4. Project implementatie

Nr.	Omschrijving eis
4.1	Bij (onvoorziene) uitloop van de implementatie wordt de inzet van accountmanager, projectmanager en technisch consultant verlengd
4.2	De opdrachtnemer borgt dat gedurende de inrichting en aansluiting van de eerste connectoren, workflows en vergelijkbare onderdelen zoveel mogelijk dezelfde Nederlandstalige technisch consultants worden ingezet.
4.3	De projectmanager van de opdrachtnemer is verantwoordelijk voor naleving van, aan- en bijsturing op het plan van aanpak in nauwe samenwerking met de projectmanager van opdrachtgever
4.4	Bij onvoorziene uitval van projectmanager, accountmanager of technisch consultant wordt, i.o.m. opdrachtgever een gelijkwaardige projectmanager of technisch consultant beschikbaar gesteld tegen dezelfde voorwaarden
4.5	Voor de gehele periode van implementatie worden, in samenwerking met opdrachtgever, duidelijke afspraken gemaakt over samenwerking, planning, rapportages, communicatie, verantwoordelijkheden en escalatie. Deze afspraken worden binnen een maand na start contract afgestemd en vastgelegd.
4.6	Opdrachtnemer stelt zoveel als mogelijk een vaste (groep) technisch consultant(s) beschikbaar voor de periode van inrichting en aansluiting van de eerste connectoren, workflows e.d.
4.7	Opdrachtnemer stelt projectmanager beschikbaar voor de periode van inrichting en migratie en geoffreerde uren tot minimaal 6 weken na live-gang (= start in gebruikname alle door opdrachtgever afgenomen functionaliteiten in productieomgeving systeem)
4.8	De opdrachtnemer dient voor de uitvoering van het project een implementatieplan op te stellen.



5. Security, privacy en compliance

Nr.	Omschrijving eis
5.1	Logbestanden worden minimaal 90 dagen bewaard, op verzoek in leesbaar formaat aan de VRU beschikbaar gesteld voor analyse- en auditdoeleinden en beschermd tegen ongeautoriseerde toegang, wijziging of verwijdering.
5.2	Opdrachtnemer is in staat voor de afgenomen dienst voldoende logging beschikbaar te stellen voor het aanleveren van een audit trail in geval een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens (AP). Dit in overeenstemming met de Selectielijst gemeenten en intergemeentelijke organen 2020 en de BIO.
5.3	Indien er selfservice is ingericht biedt de oplossing inzicht in de actuele status en voortgang van aanvragen en taken.
5.4	De aangeboden oplossing biedt binnen workflow processen inzicht in de actuele status en voortgang van aanvragen en taken. Voor iedere roltoewijzing moet binnen het IAM-systeem zichtbaar zijn of deze in behandeling, toegewezen of afgewezen is. Deze status moet direct raadpleegbaar zijn bij de betreffende identiteit op de pagina waar de roltoewijzing wordt weergegeven.
5.5	Het moet mogelijk zijn om per rol inzage te hebben en te kunnen instellen welke autorisaties en toegangen bij deze rol horen.
5.6	Het systeem biedt inzicht in het eigenaarschap en de bijbehorende autorisatieniveaus voor mailboxen, fileshares, distributielijsten en licenties.
5.7	Data zoals deze opgeslagen en gebruikt wordt in de aangeboden oplossing moet beschikbaar, integer en controleerbaar zijn.
5.8	De opdrachtnemer hanteert voor de SaaS-dienst een Recovery Point Objective van maximaal 24 uur en toont aan dat dit wordt geborgd met ingerichte, gedocumenteerde en periodiek geteste back-up- en restoreprocedures.
5.9	De opdrachtnemer garandeert d.m.v. backup & restore-procedures dat gegevensverlies maximaal 24 uur kan bedragen.
5.10	Opdrachtnemer treft maatregelen om de kans op cyberaanvallen en/of kwaadaardige software te minimaliseren, waarbij minimaal technologieën als firewalls, antimalware, IDS, IPS, hardening en encryptie zijn toegepast en up to date worden gehouden.
5.11	Persoonsgegevens mogen alleen worden getoond voor zover deze noodzakelijk zijn voor de uitvoering van de servicedesктаak.



Nr.	Omschrijving eis
5.12	De opdrachtnemer voert periodiek (minimaal 1x per jaar) een onafhankelijke pentest en kwetsbaarheidsscans uit op de aangeboden omgevingen. Opdrachtnemer verschaft over de uitvoering en de resultaten een jaarlijkse rapportage aan de VRU.
5.13	Eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. dergelijke beveiligingstest/-audits dienen te worden meegenomen bij de doorontwikkeling van de oplossing (als onderdeel van het onderhoud) en zo nodig op de kortst mogelijke termijn te worden gepatcht.
5.14	De webapplicaties die opdrachtnemer aanbiedt, zijn ingericht conform de richtlijnen van het NCSC (Nationaal Cyber Security Centrum) "ICT-Beveiligingsrichtlijnen voor Webapplicaties - Verdieping".
5.15	Opdrachtnemer beschikt over passende continuïteits-, back-up- en herstelvoorzieningen voor de dienstverlening en kan op verzoek aantonen hoe verstoringen worden beheerst en hoe de herstelbaarheid van gegevens en systemen die betrekking hebben op de dienstverlening periodiek wordt getoetst.
5.16	Fouten of afwijkingen in datalevering moeten detecteerbaar en herleidbaar zijn. De bron en actualiteit van de data moet gecontroleerd kunnen worden.
5.17	Autorisaties kunnen door de functioneel-/applicatiebeheerders worden ingesteld, beheerd en gecontroleerd.
5.18	De oplossing is voorzien van DDOS-bescherming.
5.19	De VRU heeft toestemming de componenten/diensten die onderdeel zijn van dienstverlening van opdrachtnemer aan de VRU permanent op te nemen in kwetsbaarheden-scanners van VRU.
5.20	Digitale toegankelijkheid: Van de opdrachtnemer wordt verwacht dat zij bij ontwerp, realisatie, oplevering en doorontwikkeling van de oplossing voldoet en blijft voldoen aan de European Accessibility Act
5.21	Opdrachtnemer treft maatregelen om de kans op cyberaanvallen en/of kwaadaardige software te minimaliseren, waarbij minimaal technologieën als firewalls, antimalware, IDS, IPS, hardening en encryptie zijn toegepast en up to date worden gehouden.
5.22	De Oplossing moet ondersteunen dat toegangsgegevens die voortkomen uit bijvoorbeeld een wachtwoordreset of de initiële uitgifte van een account op een veilige wijze aan een bevoegde ontvanger worden verstrekt. Hierbij moet kunnen worden voorkomen dat volledige inloggegevens gezamenlijk via één onbeveiligd communicatiekanaal worden gedeeld.



Nr.	Omschrijving eis
5.23	Het IAM-systeem moet een configureerbaar wachtwoordbeleid ondersteunen en afdwingen, waarbij wachtwoordrestricties kunnen worden ingericht conform het geldende informatiebeveiligings- en privacybeleid van de organisatie. Hierbij moet onder andere rekening kunnen worden gehouden met eisen ten aanzien van wachtwoordlengte, complexiteit, hergebruik, geldigheidsduur en veilige opslag van wachtwoorden.
5.24	Voor gebruikers die bekend zijn in de Active Directory van de VRU die toegang zoeken tot de oplossing geldt “single sign-on” (SSO) via ADFS/Microsoft Entra ID Federation met behulp van SAML2 (SHA-2) of ADFS/Microsoft Entra ID Federation met behulp van OpenID Connect. Vanaf een VRU-werkplek wordt een gebruiker automatisch ingelogd zonder login prompt.
5.25	De Opdrachtnemer draagt zorg voor gebruikersauthenticatie alvorens gebruikers toegang tot de data verkrijgen. Hieronder verstaan wij een gebruikersnaam en sterk wachtwoord, conform het geldende VRU-wachtwoordbeleid.
5.26	De werking van de IT-Oplossing kan worden getest zonder gebruik te maken van echte persoonsgegevens.
5.27	Mutaties in autorisaties moeten gelogd worden
5.28	Opdrachtnemer ondersteunt de export van beveiligingsgebeurtenissen in een gangbaar en machineleesbaar formaat, zodat integratie met de SIEM-voorziening van de VRU mogelijk is.
5.29	Gegevens die door of namens de VRU binnen de dienstverlening worden verwerkt, blijven onder zeggenschap van de VRU. Opdrachtnemer stelt deze gegevens bij beëindiging van de dienstverlening binnen een overeengekomen termijn beschikbaar in een gangbaar en bruikbaar formaat en verwijdert resterende gegevens aantoonbaar en veilig, tenzij wettelijke bewaarplichten anders vereisen.
5.30	Opdrachtnemer gaat vertrouwelijk om met alle door de VRU verstrekte informatie, gebruikt deze uitsluitend voor het uitvoeren van de dienstverlening en waarborgt dat onderaannemers contractueel zijn gebonden aan passende geheimhoudings- en informatiebeveiligingsverplichtingen.



Nr.	Omschrijving eis
5.31	Indien de dienstverlening gebruikmaakt van een multi-tenant cloud- of hostingomgeving, waarborgt opdrachtnemer dat gegevens en omgevingen van de VRU aantoonbaar logisch en/of technisch zijn gescheiden van die van andere klanten. Op verzoek toont opdrachtnemer aan hoe deze tenant-segmentatie is ingericht en periodiek wordt gecontroleerd.
5.32	De opdrachtnemer informeert de VRU tijdig over wijzigingen in de dienstverlening die impact kunnen hebben op het gebruik of de beveiliging van de oplossing of dienst.
5.33	Opdrachtnemer informeert de VRU over geconstateerde of verwachte kwetsbaarheden met betrekking tot de dienstverlening die gevolgen kunnen hebben voor de VRU. Daarbij vermeldt opdrachtnemer ten minste de aard en omvang van de kwetsbaarheid, de (verwachte) impact voor de VRU en de getroffen of nog te treffen maatregelen.
5.34	De aangeboden oplossing ondersteunt attestatie door de feitelijk toegekende rechten in doelsystemen te vergelijken met de gewenste rechten zoals vastgelegd in profielen en rollen binnen het IAM-systeem. De oplossing moet in rapportages inzichtelijk maken waar verschillen bestaan tussen de actuele situatie (IST) en de gewenste situatie (SOLL), zodat afwijkingen kunnen worden beoordeeld en opgevolgd.
5.35	Alle wijzigingen aan identiteiten, rollen, autorisaties en goedkeuringsprocessen moeten volledig herleidbaar worden vastgelegd in een audittrail.



6. Technisch, integraties en gegevensbeheer

Nr.	Omschrijving eis
6.1	Responsetijden op schermen zijn gemiddeld < 1 seconde voor elke gebruiker (ongeacht het aantal gebruikers) van de aangeboden oplossing bij het invoeren van informatie en het schakelen tussen velden en schermen. Dit geldt niet voor het genereren van overzichten en rapportages.
6.2	De productieomgeving van de Oplossing is voldoende schaalbaar en performant zodat deze op piekmomenten tot 100 concurrent users kan opvangen, tegen gelijkblijvende performance en in overeenstemming met SLA.
6.3	Batchverwerkingen (mag ook overdag) binnen de Oplossing beïnvloeden de performance van de Oplossing voor andere Eindgebruikers niet negatief.
6.4	Er kan 24 uur per dag en 7 dagen per week gebruik worden gemaakt van de oplossing. De beschikbaarheid van de oplossing is voor minimaal 99,9 %, gemeten op jaarbasis , buiten geplande onderhoudstijden, gegarandeerd. Downtime vanwege installatie- en herstelverzoeken van de VRU wordt niet meegerekend in het meten van deze beschikbaarheid.
6.5	De oplossing moet in staat zijn om binnen 4 (vier) uur alle gewijzigde rollen en rechten op basis van attribuut-gebaseerde rol-toekenning te verwerken in de koppeling met de Microsoft Active Directory en Microsoft Entra ID voor 3100 identiteiten
6.6	De oplossing moet ondersteuning bieden voor veilige, geautomatiseerde toegang via service accounts of OAuth.
6.7	De aangeboden oplossing biedt de mogelijkheid tot het importeren en exporteren van bulkgegevens in CSV en XML formaat.
6.8	Veilige toegang moet mogelijk zijn via bijvoorbeeld HTTPS en versleutelde API's.
6.9	De Oplossing moet kunnen integreren met de bestaande voorzieningen voor Single Sign-On (SSO) en Multi-Factor Authenticatie (MFA) van de organisatie, waaronder Microsoft Entra ID, zodat toegang tot en beheer van de Oplossing conform de geldende beveiligingsmaatregelen van de organisatie kan plaatsvinden.
6.10	Opdrachtnemer zorgt dat alle data versleuteld wordt opgeslagen en verstuurd. Hierbij wordt minimaal gebruik gemaakt van AES-256 en de meest recente ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC worden gevolgd.



Nr.	Omschrijving eis
6.11	De oplossing moet ondersteuning bieden voor koppelingen met Microsoft Azure-diensten zoals Azure Blob Storage en Azure SQL Database.
6.12	De oplossing moet ondersteuning bieden voor incrementele data-opvragingen (delta loads) om verwerkingstijd en resources te beperken.
6.13	De IT-Oplossing ondersteunt zowel het IPv4 als het IPv6.
6.14	De on-premises Active Directory is de bron voor gebruikersaccounts. Accounts dienen on-premises te worden aangemaakt; synchronisatie naar Entra ID vindt plaats via de bestaande Entra Connect-implementatie.
6.15	Data moet voldoende gestructureerd en consistent zijn om analyse en rapportage mogelijk te maken.
6.16	Alle functionele beheertaken met betrekking tot de oplossing kunnen worden uitgevoerd terwijl gebruikers zijn ingelogd.
6.17	De oplossing moet native integreren met Microsoft Entra ID en Microsoft 365 via ondersteunde Microsoft API's, waaronder Microsoft Graph API.
6.18	De oplossing moet betrouwbare toegang bieden tot de onderliggende data, bijvoorbeeld via API's, webservices of directe databaseconnecties.
6.19	De aangeboden oplossing is koppelbaar met databases MS SQL, MySQL, Postgress, MariaDB om gebruikersinformatie op te halen en om identiteit, autorisatie of andere informatie weg te schrijven
6.20	Het moet mogelijk zijn meerdere bronsystemen te koppelen aan de oplossing
6.21	De IAM-oplossing moet werken zonder het gebruik van browser-plugins. Het gebruik van browser plugins (zoals bv. Flash, ActiveX, Java Runtime) aan de client/gebruikerskant is niet toegestaan.
6.22	De oplossing wordt geleverd als SaaS-dienst, waarbij zowel het draaiende houden (operations) als het doorontwikkelen (development) door de Opdrachtnemer wordt uitgevoerd. Het technisch-beheer en applicatie-beheer ligt volledig bij de Opdrachtnemer.
6.23	De oplossing moet Multi-Factor Authentication (MFA) ondersteunen in combinatie met Microsoft Authenticator en daarbij de op het moment van implementatie door Microsoft ondersteunde moderne authenticatiemethoden van Microsoft Authenticator kunnen toepassen.



Nr.	Omschrijving eis
6.24	De tooling moet alle benodigde Active Directory-attributen kunnen beheren. Bij het aanmaken van een gebruikersaccount moet automatisch een uniek viercijferig nummer worden gegenereerd en vastgelegd in het attribuut carLicense. Hierbij moet worden geborgd dat het nummer niet reeds in gebruik is.
6.25	De aangeboden oplossing volgt de ontwikkelingen binnen moderne browser technologie, zoals nu HTML5 en CSS3 evenals de toekomstige mogelijkheden en ontwikkelingen.



Colofon

Dit is een uitgave van
Veiligheidsregio Utrecht

Tekst: afdeling F&I, team inkoop
Fotografie:
Ontwerp: afdeling Communicatie

14 oktober 2026