



Aanbesteding IAM

Bijlage VII – Programma van eisen en wensen



Inhoudsopgave

1.	EISEN.....	3
1.1	IDENTITEITSBEHEER	3
1.2	TOEGANGSBEHEER	5
1.3	COMPLIANCE	6
1.4	INTEGRATIE.....	7
1.5	ALGEMEEN IAM.....	8
1.6	ARCHITECTUUR.....	8
1.7	DIENTVERLENING	9
2.	INFORMATIEBEVEILINGEISEN	10
2.1	GENERIEK.....	10
2.2	BESCHIKBAARHEID	11
2.3	INTEGRITEIT	11
2.4	VERTROUWELIJKHEID.....	12
2.5	PRIVACY.....	13
2.6	AANVULLENDE EISEN	14
3.	WENSEN.....	16

1. Eisen

1.1 Algemeen IAM

Nr	Omschrijving
30	Het IAM-systeem is voor de gebruikers van het IAM-systeem beschikbaar via SSO.
31	De leverancier levert één centrale omgeving, deze moet geschikt zijn om door Opdrachtgever voor verschillende juridische entiteiten (organisaties/partners) op een efficiënte, uniforme en gestandaardiseerde manier de IAM-functionaliteiten te kunnen ondersteunen. Iedere juridische entiteit is eigenaar van haar eigen data, de data blijft dan ook strikt gescheiden. Het moet mogelijk zijn om de entiteiten eenvoudig te ontvlechten indien de samenwerking beëindigd wordt.
32	De beheerder van opdrachtgever dient extra attributen (kwalificaties, integriteitsverklaringen, certificeringen, roltype, eigenaar enz.) per hoofdobject (voorbeeld: Identiteit, arbeidsrelatie) te kunnen configureren.
36	Het IAM-systeem is voor de eindgebruiker in de Nederlandse taal beschikbaar. Ook instructiemateriaal en gebruikersdocumentatie is in de Nederlandse taal opgesteld. Deze Nederlandse teksten worden bij elke release geactualiseerd De technische beheerdocumentatie is Nederlands- en/of Engelstalig.
37	Het IAM-systeem biedt de mogelijkheid om workflows samen te stellen. Deze workflow kan meerdere (parallele) taken bevatten en elke taak kan afgehandeld worden door een behandelaar of behandelaarsgroep.
38	Het IAM-systeem ondersteunt een handmatig provisioningsproces d.m.v. workflows. Voorbeelden van taken binnen de workflows: - Het versturen van een e-mailbericht naar een beheerder - Het versturen van een taak naar een oplosgroep in een servicemanagementsysteem (TOPdesk, Planon) - Het versturen van een wijziging naar TOPdesk om fysieke middelen zoals laptop, smartphone aan te vragen igv instroom - Het versturen van een taak naar Planon om een toegangspas aan te vragen Bij deze laatste 2 taken moet voorkomen worden dat fysieke middelen meerdere keren aangevraagd worden - Het versturen van een taak naar TOPdesk om IT-middelen in te nemen.
39	het IAM-systeem dient notificaties te kunnen versturen naar één of meerdere gebruikers bijv. in geval van: - een foutsituatie, - het toewijzen van een taak, - afwijzen van autorisatie-aanvraag - herinnering niet uitgevoerde taak - start of einde van de lifecycle van een identiteit of arbeidsrelatie.
41	Het IAM-systeem biedt de mogelijkheid om (verwerkings)processen in te plannen, eenmalig of periodiek.
42	Het IAM systeem dient in een workflow een verzoek of bericht naar een externe service te kunnen sturen en de respons daarvan gebruiken om te bepalen hoe de workflow verder verloopt.
43	Het IAM-systeem dient een overzicht en bewaking van de openstaande taken aan te bieden. Niet tijdig afgehandelde taken moeten op basis van bedrijfsregels gemeld worden bij taakeigenaar en/of doorgestuurd worden naar een vervanger.

1.2 Identiteitsbeheer

Nr	Omschrijving
1	Beaufort is de bron voor persoonsgegevens, arbeidsrelatiegegevens, organisatiestructuurgegevens en leidinggevend in het IAM-systeem. Mutaties op deze gegevens moeten automatisch gesynchroniseerd worden met het IAM-systeem. het IAM-systeem moet identiteiten near realtime aanmaken.
2	Het IAM-systeem is leidend voor het genereren van het e-mailadres. Het moet mogelijk zijn om voor de verschillende partnerorganisaties een eigen e-mail-convententie te definiëren voor accounts en e-mailadressen. Wanneer in het HR-systeem wijzigingen plaatsvinden op attributen die ten grondslag liggen aan de opmaak van het e-mailadres, dan wordt het aangepaste e-mailadres bijgewerkt in het HR-systeem en wordt de identiteit in het IAM-systeem bijgewerkt. In de doelsystemen (o.a. AD, TOPdesk), wordt het primaire e-mailadres van de bestaande accounts gewijzigd en wordt geen nieuw account aangemaakt.
3	Het IAM-systeem past validatieregels toe bij het synchroniseren. Deze validatieregels gelden zowel voor handmatige invoer van identiteiten als voor automatische mutaties. Mutaties die niet valide zijn moeten tegengehouden worden. Hierbij dient een taak aangemaakt te worden voor de functioneel beheerder HR en een notificatie gemaakt te worden. De beheerder dient de tegengehouden mutaties, na onderzoek te kunnen doorvoeren of verwijderen.
4	Het IAM-systeem zorgt ervoor dat een identiteit maar 1 keer voorkomt per partnerorganisatie . Ongeacht de wijze van registratie (Youforce, Beaufort, andere bron, bulk import of handmatig) wordt bij een nieuwe identiteit gecontroleerd of de identiteit reeds voorkomt bij de betreffende partnerorganisatie. Bij een mogelijke dubbeling biedt het IAM-systeem de mogelijkheid om deze eenvoudig te corrigeren: mogelijke dubbele identiteiten worden getoond met een keuze voor nieuwe identiteit aanmaken, samenvoegen of negeren.
5	Naast medewerkergegevens moeten ook andere bronnen ontsloten worden en identiteiten aangemaakt worden, zowel automatisch als handmatig, het gaat hierbij om: - medewerkers van andere organisaties die met het account van hun eigen organisatie autorisatie krijgen - medewerkers van contractpartijen (schoonmaak, beveiliging, ICT, accountants etc) die respectievelijk een toegangspas, toegangspas+AD-account, toegangspas+AD-account+e-mailadres krijgen - RPA of machines - etc.
6	Het IAM-systeem biedt de mogelijkheid om via selfservice-portaal niet-medewerkergegevens veilig te registreren, wijzigen en te archiveren/verwijderen. Hierbij minimaal de volgende attributen kunnen registreren: achternaam, tussenvoegsels, voornaam, samengestelde naam (afgeleid), organisatie, afdeling, functie, locatie, rol, leidinggevende, ingangsdatum, einddatum. Hierbij de mogelijkheid hebben om aan te geven of deze attributen optioneel of verplicht zijn. Indien een identiteit geregistreerd wordt door een niet-leidinggevende, dan een notificatie naar de leidinggevende sturen.
7	Het IAM-systeem kan bij handmatige registratie per organisatieonderdeel automatisch op basis van de afdeling bepalen wie de leidinggevende is en wie de vervangers zijn. Indien leidinggevende niet bekend is bij een afdeling, wordt deze overgenomen van de bovenliggende afdeling.
8	De leidinggevende dient de mogelijkheid te hebben om specifieke taken, zoals goedkeuren van autorisaties, te kunnen delegeren aan een andere medewerker. Delegatie dient ook weer ingetrokken te kunnen worden.

1.3 Toegangsbeheer

Nr	Omschrijving
10	Het IAM-systeem ondersteunt de mogelijkheid om op basis van configureerbare bedrijfsregels met attributen (zoals type medewerker, team, afdeling, functie) automatisch rollen of rechten toe te kennen voor alle typen gebruikers-accounts: normaal-, gast-, en beheerder-account. Voorbeelden van bedrijfsregels zijn: - het IAM-systeem autoriseert op basis van de risicoclassificatie van de voorziening; - het IAM-systeem stelt uitsluitend voorzieningen beschikbaar indien de medewerker over de bij de voorziening behorende screening beschikt. - een medewerker zonder geldige arbeidsrelatie heeft geen toegang tot voorzieningen - autorisaties moeten uitgesteld op ingangsdatum in kunnen gaan - accounts en autorisaties moeten per datum uit dienst automatisch ingetrokken worden.
12	Een identiteit inclusief alle bijbehorende accounts dienen door één handeling/mutatie in het IAM-systeem direct gedeactiveerd te worden (rode knop), inclusief toegang tot alle voorzieningen. Dit geldt ook voor accounts van applicaties die niet onder SSO vallen ook deze moeten direct gedeactiveerd worden.
13	Na een deactivering van een identiteit moet een identiteit met alle eerder toegekende voorzieningen door één handeling/mutatie in het IAM-systeem weer geheractiveerd kunnen worden.
15	Het IAM-systeem dient autorisatiemodellen RBAC en ABAC te ondersteunen. Hierbij worden de volgende situaties onderkend: - basisautorisaties (birthright), de standaard voor de gehele partnerorganisatie - autorisaties die afgeleid worden op basis van bedrijfsregels - specifiek/onvoorspelbaar. Deze autorisaties worden handmatig aangevraagd.
16	Het IAM-systeem ondersteunt de mogelijkheid om applicatirollen uit gekoppelde doelsystemen zowel toe te wijzen aan rollen alsook aan te vragen via selfservice.
18	Functiescheiding, het IAM-systeem moet conflicterende rollen en autorisaties signaleren. Controle op functiescheidingregels gebeurt in ieder geval op de volgende momenten: - Bij reconciliatie van de gegevens - Bij de toewijzing op basis van RBAC; - Bij de aanvragen van een aanvullende rol/autorisatie vanuit het selfservice-portaal - Bij het aanmaken van een nieuwe rol; - Bij het aanmaken van een nieuwe functiescheidingregel. Conflicterende autorisaties moeten mogelijk zijn.
19	Bij een rol wordt via bedrijfsregels vastgelegd wie aanvraagbevoegd is voor de rol. Voorbeeld van bedrijfsregel is medewerker werkt op een bepaalde afdeling. Een aanvrager kan alleen rollen zien en aanvragen waarvoor hij aanvraagbevoegd is. Een leidinggevende kan alleen rollen en/of autorisaties zien en toekennen, waartoe hij bevoegd is.
22	De leidinggevende dient zowel rollen als losse autorisaties eenvoudig voor de medewerkers te kunnen aanvragen en intrekken. Dit gaat om zowel permanente als tijdelijke rechten, dit laatste door het opgeven van een einddatum. Indien het om een hoog-risico-voorziening gaat, moet de eigenaar van de voorziening ook goedkeuring geven voor de aanvraag Een medewerker moet ook zelf (tijdelijke) autorisaties kunnen aanvragen, waarbij de leidinggevende goedkeuring geeft, IAM-beheerders kunnen voor alle medewerkers autorisaties aanvragen, wijzigen of intrekken.
24	Het IAM-systeem dient autorisaties op de volgende voorzieningen te kunnen vastleggen: datagebieden, applicaties (incl licentie), distributielijsten, shared mailbox.
25	Het IAM-systeem moet zowel SAAS-applicaties als onprem-applicaties kunnen aansluiten.
26	Het IAM-systeem synchroniseert de voorzieningen (groepen) uit AD en entra ID met de autorisaties in het IAM-systeem en geeft de mogelijkheid hier attributen aan toe te voegen .

	Ook moet de mogelijkheid bestaan om meerdere voorzieningen te groeperen in een IAM-autorisatieprofiel.
28	Het IAM-systeem ondersteunt voor de eigen applicatie de inrichting van rollen en autorisaties voor verschillende groepen gebruikers (beheerders, leidinggevend, medewerker etc). Bijvoorbeeld: - De medewerker heeft alleen maar toegang tot informatie behorende bij de eigen identiteit - De leidinggevende heeft toegang tot de taken die behoren bij zijn medewerkers; - De rolbeheerder van een partnerorganisatie heeft alleen toegang tot de gegevens van de partnerorganisatie waarvoor hij werkzaam is - functioneel beheerder van SSC Ons kan alle activiteiten uitvoeren en heeft toegang tot alle identiteiten, rollen en autorisaties van alle partnerorganisaties.

1.4 Compliance

Nr	Omschrijving
44	Het IAM-systeem biedt voor de gebruiker op alle schermen en rapportages zoek-, filter- en sorteerfunctionaliteit op identiteit-attributen, rollen en autorisaties. De mogelijkheid om flexibel velden toe te voegen of achterwege te laten. Ook de mogelijkheid om deze instellingen te bewaren voor hergebruik.
45	Standaard IAM-rapportages worden door het IAM-systeem geleverd, eventueel als PowerBI-template.
47	het IAM-systeem dient rapportages te kunnen exporteren naar standaarden zoals pdf, xls, xml, CSV.
49	het IAM-systeem dient tbv periodieke controles: vooraf gedefinieerde rapportages, periodiek automatisch te kunnen genereren, om per eigenaar (leidinggevende, roleigenaar of systeemeigenaar), de afzonderlijke autorisaties te laten valideren of het geheel in één keer te valideren, met de mogelijkheid om reden van afkeuren te geven.
50	Het IAM-systeem biedt een overzicht met de status van alle periodieke controles met filtering op status (uitstaand, verlopen, gereed), organisatie, afdeling, eigenaren (leidinggevend, systeemeigenaren, roleigenaren), type voorziening.
51	Bij een identiteit moet altijd inzichtelijk zijn welke autorisaties de identiteit heeft en op welke wijze en wanneer deze autorisatie verkregen is (via welke bedrijfsregel of via selfservice aangevraagd).
52	Het IAM-systeem kan per rol en/of voorziening een historisch overzicht maken van wie, wanneer en met welke bevoegdheden toegang tot de voorziening heeft of heeft gehad.
53	Het IAM-systeem levert een overzicht van de voorzieningen met autorisatieregels.
54	Het IAM-systeem levert een overzicht van de gedefinieerde rollen met autorisatieregels en autorisaties.
55	Het IAM-systeem levert een overzicht van Accounts die niet vanuit het IAM-systeem beheerd worden en rechtstreeks in AD of Entra ID zijn aangemaakt.
56	Het IAM-systeem biedt rapportages om inconsistentie in data tussen bron en IAM evenals IAM en doelsystemen te rapporteren.
57	Het IAM-systeem biedt de mogelijkheid om de toegekende autorisaties volgens het autorisatiemodel (SOLL) te vergelijken met de effectieve geregistreerde autorisaties volgens de voorzieningen (IST), waarbij duidelijk is wat de IST is, wat de SOLL is, wat de afwijkingen zijn, welke autorisaties ingetrokken moet worden en wat nader uitgezocht moet worden. Inzicht per organisatie, afdeling, functie/rol en medewerker.
58	Indien vanuit de reconciliatie-analyse verschillen zijn geconstateerd, voorziet het IAM-systeem in directe provisioning en deprovisioning van accounts en autorisaties (of taken voor de niet geautomatiseerde voorzieningen) op basis van afwijkingen van de SOLL-definitie in de IST situatie.

	Een door de reconciliatie gedeactiveerde voorziening dient in IAM door een beheerder weer geheractiveerd kunnen worden.
59	Een overzicht welke conflicterende autorisaties/rollen (functiescheiding) aan een medewerker zijn toegekend, voor hoe lang en door wie.

1.5 Integratie

Nr	Omschrijving
9	Het IAM-systeem zorgt voor provisionen van identiteiten naar de volgende doelsystemen: - AD-systeem partner - Entra ID partner - TOPdesk Ons, - TOPdesk ZWO - TOPdesk OVR - Planon Provisioning is binnen 60 minuten uitgevoerd en volledig afgehandeld.
29	Het moet als opdrachtgever mogelijk zijn om zelf eenvoudig koppelingen met doelsystemen te configureren (bijv. aan/uitzetten van de koppeling, filteren van gegevens, mapping van gegevens).
33	De hoofdobjecten (identiteiten, rollen, autorisaties etc) van het IAM-systeem zijn aan te maken of te wijzigen via een API-koppeling met ander systeem en indien nodig bv i.g.v. legacy ook via een import-functie (.csv, .xml, .xlsx).
71	Het moet mogelijk zijn om bi-directionele koppelingen te ondersteunen. Het moet mogelijk zijn om vanuit het IAM-systeem via API's toegang te krijgen tot externe systemen en andersom, externe systemen via een API toegang krijgen tot het IAM-systeem. Er is duidelijke documentatie voor ontwikkelaars hoe API's van het IAM-systeem te gebruiken.
72	De software ondersteunt tenminste de volgende standaarden. 'Pas toe leg uit' standaarden (verplicht) - OpenID.NLGov en SAML - NL GOV Assurance profile for OAuth 2.0 - Digikoppeling - Digitoegankelijk (EN 301 549 met WCAG 2.1) - DKIM, DMARC, DNSSEC - OpenAPI Specification - REST-API Design Rules - STARTTLS en DANE - TLS Aanbevolen standaarden voor uitwisselingsfundament Forum Standaardisatie - OAuth - SCIM - OData - SOAP - XML - JSON Aanvullende standaarden - XACML - LDAPS - LDIF - AD LDS (Active Directory Lightweight Services) - JMS (Java Messaging Services) Deze standaarden worden bijgehouden op het laatste security- en servicepack-level.

73	Alle data uit het IAM-systeem is te ontsluiten via ESB van Opdrachtgever voor andere toepassingen zoals PowerBI reporting, monitoringsoplossing, logmanagement en andere toepassingen. De frequentie is minimaal dagelijks
75	Het IAM-systeem dient Event, Security en Audit logging geautomatiseerd te versturen naar het SSC-Ons logmanagement systeem Rapid7

1.6 Architectuur

Nr	Omschrijving
60	Het IAM-systeem is modulair opgebouwd zodat componenten uitgeschakeld kunnen worden en standaard functionaliteiten toegevoegd kunnen worden. Daarnaast moeten aanpassingen in de functionaliteit van de ene component minimale impact hebben op de andere componenten zodat bijvoorbeeld testwerkzaamheden beperkt blijven.
61	De IAM-oplossing heeft een adequate foutenafhandeling, hierna volgen enkele voorbeelden: - foutmeldingen worden voor gebruikers in begrijpelijke taal weergegeven. - het niet beschikbaar zijn van een gekoppelde doelsysteem leidt tot een foutmelding en niet tot het crashen van de applicatie. - bij het niet beschikbaar zijn van een doelsysteem bewaakt het IAM-systeem automatisch alle nog niet afgehandelde handelingen, dit is zichtbaar in een portal - het niet synchroon zijn van medewerkergegevens en identiteitgegevens mag niet leiden tot onvoorspelbare of onjuiste resultaten - inconsistentie als gevolg van foutsituaties worden gerapporteerd en gemonitord
62	Gebruiksparementen zijn via een interface aan te passen. De userinterface (en bijbehorende logica) dient ervoor te zorgen dat er geen (zo min mogelijk) fouten gemaakt kunnen worden bij het configureren.
63	Inschrijver voorziet in voorzieningen zodat SSC Ons en zijn partners inspraak heeft bij gewenste nieuwe functionaliteiten beschikbaar voor alle klanten.
64	Opdrachtnemer zorgt ervoor dat bij onderhoud of nieuwe releases de bestaande koppelingen blijven werken. Dit geldt voor zowel standaard als maatwerkkoppelingen. In geval van legacy-koppelingen en de API wordt niet meer ondersteund, wordt een overgangsfase van 6 maanden gehanteerd om Opdrachtgever de gelegenheid te geven om wijzigingen door te voeren. Ook zorgt de Opdrachtnemer dat bestaande inrichtingen blijven werken.
65	Naast de productieomgeving wordt een acceptatietestomgeving opgeleverd bedoeld voor het testen van nieuwe releases, testen van configuraties, het testen van koppelingen en voor opleidingsdoeleinden. Deze omgeving is duidelijk herkenbaar en visueel afwijkend van de productieomgeving. Productiedata is in deze omgeving niet toegestaan.
67	Op basis van het afgesloten contract garandeert de Inschrijver dat het systeem, gedurende de contractperiode, doorontwikkeld zal worden zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief, ook verstaan dat op het systeem adaptief onderhoud wordt uitgevoerd om als opdrachtgever te blijven voldoen aan in de contractperiode geldende wet- en regelgeving en inspeelt op ontwikkelingen in de markt. Nieuwe ontwikkelingen op grond van specifieke wensen van de Opdrachtgever vallen hierbuiten.
68	Leverancier is op de hoogte van de ontwikkelingen rondom common ground, de betrokkenheid van gemeentes bij Dimpact en de wens van de gemeentes om hun informatievoorziening te vernieuwen door gebruik te maken van de architectuur die onder common ground ligt.
69	De ideale leverancier laat zien welke visie hij heeft op het koppelen van laag 3 van de common ground waar IAM oplossingen aanwezig zijn. Ook laat de leverancier zien hoe zijn visie is op het autoriseren van loosely coupled componenten (openzaak, openformulier etc)

74	Het functionele en technische datamodel wordt door de inschrijver opgeleverd, waarbij definities van tabellen, kolommen, velden en relaties inzichtelijk wordt gemaakt
79	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.
80	Het systeem wordt geleverd als SAAS-oplossing. Dat betekent dat (toegang tot) de standaardsoftware als Dienst wordt aangeboden, vanuit een door de Opdrachtnemer ingerichte en technisch beheerde omgeving, inclusief alle daarvoor benodigde licenties, software, hardware, netwerkverbindingen, etc. De opdrachtnemer is verantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid (zie eisen informatiebeveiliging)
81	Er moet gebruik worden gemaakt van vaste, specificeerbare poorten (TCP/UDP) voor data-verkeer tussen opdrachtnemer en opdrachtgever.
82	Het systeem is als webapplicatie te gebruiken op een desktop, laptop, smartphone of tablet (responsive) De werking hierop wordt gegarandeerd op recente versies van gangbare platforms/webbrowsers zonder extra plugins: - Windows, MacOS - Edge, Safari, Chrome, Firefox - Android, iOS
83	Het systeem ondersteunt een multi-tenant-inrichting. Vanuit het IAM-systeem wordt bij het aanmaken van het account of het toekennen van rechten de tenants van de partners centraal aangestuurd. Hierbij moet rekening gehouden worden met o.a. verschillende OU,- naamconventie E-mailadres, homedrive-letters etc.

1.7 Dienstverlening

Nr Omschrijving	
88	Opdrachtnemer stemt in met het minimale niveau van dienstverlening zoals beschreven in de SLA en geeft duidelijk aan daar waar KPI's of normen niet haalbaar zijn. Het staat Opdrachtgever vrij servicelevels, normen en KPI's toe te voegen. Wijzigingen middels track changes.
89	Opdrachtnemer stemt in met afspraken en procedures in het DAP en vult aan waar gevraagd en past aan waar nodig. Wijzigingen middels track changes.. Finale afstemming en afronding (V1.0) met de Servicemanager van Opdrachtgever is gereed voor afronding implementatie van de 1e aangesloten partner.

2. Informatiebeveiligseisen

2.1 Generiek

Nr	Omschrijving
100	Leverancier stelt opdrachtgever in de gelegenheid om o.a. de volgende rapportages op te stellen: • Rapportages rondom het authenticatieproces: inlogtijd, uitlogtijd, mislukte inlogpogingen (gebruikersnaam en IP-adres); • Rapportages rondom het gebruikersbeheer: aangemaakte accounts, verwijderde accounts, geblokkeerde accounts, wijzigingen op accounts (door wie), groepen; • Rapportages rondom rollen, en autorisaties; • Raadplegingen van persoonsgegevens: aantal raadplegingen per gebruiker, raadplegingen per zoek sleutel.
101	Indien van toepassing voor de ICT-prestatie zijn de volgende open standaarden van het Forum Standaardisatie onder meer en expliciet verplicht: • DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, SAML, SPF, STARTTLS, DANE, STIX en TAXII, TLS en WPA2. • NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 (Informatiebeveiliging).
102	De leverancier zal voor de prestaties voldoende personen inzetten met voldoende opleiding, vaardigheden en kennis van de bedrijfsvoering en organisatie van de Opdrachtgever, om de prestaties te verrichten. Wanneer de hierboven genoemde personen zich bij de Opdrachtgever bevinden, of in direct contact met de Opdrachtgever staan, zal het personeel van de leverancier de gedragsvoorschriften van de Opdrachtgever naleven. Hiermee zal gevolg gegeven worden aan redelijke verzoeken van de Opdrachtgever.
103	De ICT-Prestatie stelt de opdrachtgever in staat te voldoen aan: • De (U)AVG; • De Baseline Informatiebeveiliging Overheid; • De beveiligingsrichtlijnen voor webapplicaties van het NCSC; • Archiefwet 1995, Archiefbesluit 1995; • Het Algemeen en Technisch Informatiebeveiligingsbeleid van Opdrachtgever • Leverancier licht toe hoe de ICT-Prestatie de Opdrachtgever ondersteunt om hieraan te voldoen.
104	De ICT-prestatie dient aan te sluiten bij de principes van 'privacy bij design' en 'privacy by default' zoals beschreven in de AVG.
105	Indien de leverancier gebruik maakt van een onderaannemer gelden alle eisen onverminderd voor de onderaannemer. De leverancier is verantwoordelijk voor een juiste invulling en werking van de eisen bij de onderaannemer.
106	De leverancier maakt gebruik van een methode of best practice voor secure software development, zoals bijvoorbeeld van het CIP: https://www.cip-overheid.nl/
107	Leverancier (in haar rol als verwerker) zal aan de Opdrachtgever (in haar rol als verwerkingsverantwoordelijke) zo snel mogelijk, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) inbreuk in verband met persoonsgegevens (datalek). Opdrachtnemer vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen. Daarbij wordt ook vermeld welke verbetermaatregel zijn/worden getroffen door de opdrachtnemer.
108	Risico's voor informatiebeveiliging en privacy zijn expliciet benoemd en passende beheersmaatregelen zijn expliciet belegd.
109	Informatiebeveiligseisen worden opgenomen in leveranciersovereenkomsten.

110	De applicatie wordt periodiek en minimaal eens per jaar op kwetsbaarheden onderzocht (kwetsbaarheidsscans en penetratietesten). Kwetsbaarheden worden geclassificeerd en krijgen opvolging.
111	De leverancier geeft transparant en kostenloos inzicht in certificeringsdocumenten en rapportages opgesteld door EDP-auditors.
112	Leverancier heeft beheersmaatregelen tegen malware getroffen.
113	Leverancier treft beheersmaatregelen om onbevoegde toegang tot, schade aan en interferentie (storing/uitval) met informatie en informatievewerkende faciliteiten van Opdrachtgever te voorkomen, zodat de bedrijfsvoering niet wordt onderbroken of aangetast.

2.2 Beschikbaarheid

Nr	Omschrijving
114	De leverancier draagt zorg voor een Escrow. Zo heeft de Opdrachtgever in voorkomend geval de mogelijkheid om bij het in vervulling gaan van één of meer in de Escrow genoemde voorwaarden, software die onderdeel is van het contract, eigenmachtig te (laten) gebruiken voor het herstellen van fouten en anderszins het onderhouden en beheren van de standaardprogrammatuur.
115	Voor de software is sprake van een gescheiden test en productie omgeving (OTAP).
116	De leverancier heeft een wijzigings- en acceptatieproces. De acceptatie wordt hierbij uitgevoerd door de opdrachtgever.
117	Systeemmeldingen kunnen met SNMP verstuurd worden naar een centraal monitoring systeem.
118	Remote access vindt alleen plaats via de door SSC ONS beschikbaar gestelde middelen.
119	Er is een exitplan en -strategie (en export van data). Zie ook GIBIT artikel 22: • De Opdrachtnemer maakt een Exitplan en strategie en stemt deze af met de Opdrachtgever. • Gegevens worden op basis van standaarden opgeslagen met als doel portering naar andere dienstverleners mogelijk te maken in geval van een exit. • Alle gegevens (grafische bronbestanden, grafische producten en bijbehorende metadata) worden door de Opdrachtnemer bij exit kostenloos geëxporteerd.

2.3 Integriteit

Nr	Omschrijving
120	Onderliggende software componenten, zoals operating systemen, database software, browser versie, programmeer framework enz., waarop de software is gebouwd en draait dienen altijd een door de oorspronkelijke leverancier van de betreffende software of framework ondersteund te zijn. Bijvoorbeeld: als Microsoft Windows gebruikt wordt, is dit op basis van een nog door Microsoft ondersteunde versie. Windows10 zou acceptabel zijn, maar Windows7 niet meer omdat het end-of-life is.
121	De leverancier heeft maatregelen genomen om de toegang tot de broncode van informatiesystemen te beperken tot de medewerkers, die deze code onderhouden of installeren.
122	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
123	Versies van de software worden voor de in productie name door de leverancier onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
124	Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10.

125	De applicatie voorziet in validatiecontroles op ten minste de volgende aspecten: • Gegevens en verwerkingen kunnen worden gecorrigeerd vanuit de applicatie na invoer • Consistentiecontroles zijn in de applicatie voorzien om de correcte verwerking van gegevens te waarborgen.
126	Er is sprake van logging in de applicatie. Relevante zaken om te loggen zijn: • Type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte); • (poging tot) Ongeautoriseerde toegang; • Handelingen met speciale bevoegdheden, waarbij alle handelingen van "superusers" worden gelogd; • Systeemwaarschuwingen; • (poging tot) Wijziging van de beveiligingsinstellingen.
127	Bij de verwerking van persoonsgegevens worden in de log aanvullend de volgende zaken opgenomen: • Ontvangen gegevens; • Gestelde vraag; • Datum/tijdstip van aanroep; • Naam van leverende of afnemende bron of systeem; • Een gebruikersnaam of ID; • Eventuele transformaties of verrijkingen; • Eventueel opgetreden fouten.
128	Een logregel bevat minimaal: • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID; • De gebeurtenis; • Waar mogelijk de identiteit van het workstation of de locatie; • Het object waarop de handeling werd uitgevoerd; • Het resultaat van de handeling; • De datum en het tijdstip van de gebeurtenis.
129	De logging is alleen beschikbaar voor daartoe geautoriseerde medewerkers.
130	De logging is read-only. Het muteren en verwijderen van log-records is niet toegestaan.
131	Logging kan op basis van één van deze formats CEF, JSON & Syslog naar een extern logmanagement systeem gestuurd worden.
132	Bij interne of externe applicatiekoppelingen biedt de applicatie voldoende waarborgen tussen componenten zodat er geen verlies van berichten optreedt (bijvoorbeeld buffering van berichten) en dat de validiteit van berichten beschermd is (uitsluiting van oa spoofing, MITM).
133	Bij webservice koppelingen wordt uitgegaan van "dubbel SSL," dat wil zeggen een PKI-certificaat voor TLS en een PKI-certificaat om de serveridentiteit vast te stellen.
134	Onderliggende software (inclusief frameworks en libraries) wordt structureel voorzien van beveiligingspatches. In het contract of SLA worden hiervoor reguliere afspraken gemaakt aangaande frequentie en betaling.
135	De opdrachtgever heeft het recht om in overleg met de leverancier webapplicaties of servicekoppelingen te onderwerpen aan penetratietesten op kosten van de opdrachtgever. De leverancier heeft hierbij de verplichting om geconstateerde kwetsbaarheden in de applicatie op te lossen zonder meerkosten. Termijnen van de oplossing worden in overleg met een gebruikersvereniging of bij gebrek hieraan in overleg met de opdrachtgever bepaald.

2.4 Vertrouwelijkheid

Nr	Omschrijving
136	Autorisaties kunnen worden ingericht op basis van functies (rol-gebaseerd) waarbij functie-scheiding is toegepast.

137	Er zijn geen "algemene" accounts / gebruikers binnen de software. Als deze noodzakelijk zijn, betreft het een beperkt aantal en met specifieke doelen. De leverancier dient hierin inzicht te geven.
138	Wachtwoordeisen en geldigheidsduur kunnen gesteld worden vanuit de software. Het kan daarmee voldoen aan het wachtwoordbeleid van de Opdrachtgever.
139	Wachtwoorden zijn beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag door middel van hashing en encryptie.
140	De omgeving is voorzien van encryptie conform hoofdstuk 6 Technisch Informatiebeveiligingsbeleid van de Opdrachtgever. Deze wordt op verzoek toegestuurd naar de Inschrijver.
141	De aangeboden websites worden altijd versleuteld dan wel voorzien van PKI-overheid Extended Validation SSL certificaat (EV SSL) (of vergelijkbaar).
142	De hosting en opslag van data vindt plaats vanaf een locatie binnen de Europese Unie.
143	De Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Opdrachtnemer van de applicatie. Dit geldt zowel voor gegevens in de Test-, Acceptatie- als Productieomgevingen.
144	Het is de leverancier verboden, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de opdrachtgever, de uitvoering van een overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden.
145	De leverancier heeft een geheimhoudingsplicht aangaande alle vertrouwelijke gegevens dan wel anderszins gevoelige informatie van de opdrachtgever die de leverancier in het kader van de opdracht ter kennis is gekomen.
146	De leverancier heeft een geheimhoudingsplicht aangaande de informatie opgenomen in de systemen.
147	De leverancier is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. Leverancier waarborgt hierbij tevens ook met scheiding van taken onbedoelde of ongeautoriseerde toegang. De opdrachtgever heeft het recht hierop te controleren.
148	De leverancier is verantwoordelijk voor de kwalificaties en screening van het eigen personeel. Op verzoek van opdrachtgever dient een VOG te worden overlegd, van personen die worden ingezet op de opdracht.
149	Alle voorwaarden en eisen die gelden voor personeel van de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor de Opdrachtgever.
150	Bij gebruik van PKI(o) certificaten beschikt de leverancier over vastgestelde procedures voor sleutelbeheer. De leverancier geeft bij de aanbesteding inzicht in de manier waarop sleutelbeheer is geregeld.
151	Autorisaties worden conform autorisatiebeleid en -proces aangemaakt en beheerd.

2.5 Privacy

Nr	Omschrijving
152	De leverancier stelt de Opdrachtgever in staat om zelf access management uit te voeren. De Opdrachtgever dient direct invloed uit te kunnen oefenen over de accounts (en bijbehorende autorisaties) van de eigen medewerkers.
153	De leverancier houdt een actuele registratie bij van geautoriseerde accounts/gebruikers.
154	De leverancier verschaft relevante informatie over de wijze waarop – en onder welke voorwaarden – cryptografie wordt gebruikt om persoonsgegevens van betrokkenen te beschermen.

155	De leverancier maakt gebruik van een proces waarbij logbestanden periodiek gecontroleerd worden teneinde onrechtmatig gebruik of andere onregelmatigheden vast te stellen. De logbestanden dienen informatie te verschaffen over de vertrouwelijkheid, beschikbaarheid en integriteit van persoonsgegevens, en of daarop een inbreuk is geweest.
156	De leverancier bepaalt onder welke voorwaarden dergelijke logbestanden aan de Opdrachtgever worden verstrekt. Deze voorwaarden worden aan Opdrachtgever medegedeeld.
157	De leverancier zorgt dat er passende maatregelen worden getroffen waarmee persoonsgegevens die in dergelijke logbestanden verschijnen, voldoende worden beschermd en niet voor andere doeleinden worden gebruikt.
158	Indien gebruik wordt gemaakt van mobiele fysieke media (zoals een USB-stick) om persoonsgegevens over te zetten, legt de leverancier vast welk fysiek medium is gebruikt, wie de bedoelde verstuurder/ontvanger zijn, alsmede de datum en tijd.
159	Persoonsgegevens worden alleen opgeslagen op mobiele fysieke media (zoals een USB-stick) met encryptie-functionaliteit.
160	Bij informatiebeveiligingsincidenten aan de kant van de leverancier wordt door de leverancier expliciet onderzocht of bij dat incident persoonsgegevens zijn gemoeid, tenzij dat redelijkerwijs niet aannemelijk is.
161	Indien het uitvoeren van audits door de Opdrachtgever onwenselijk of redelijkerwijs niet mogelijk is, overlegt de leverancier – voorafgaand aan het afsluiten van het servicecontract – onafhankelijk bewijs waaruit blijkt dat de getroffen beveiligingsmaatregelen conformeren aan de door de Opdrachtgever gestelde eisen en beleid.
162	De leverancier zorgt dat tijdelijke bestanden (cache) die persoonsgegevens bevatten periodiek worden verwijderd.
163	De leverancier legt alle verstrekkingen van persoonsgegevens (waar de Opdrachtgever verwerkingsverantwoordelijke voor is) aan andere partijen schriftelijk vast.
164	De leverancier en de Opdrachtgever maken schriftelijke afspraken over de manier waarop persoonsgegevens worden verwijderd, gepseudonimiseerd of geanonimiseerd. De leverancier heeft over dit onderwerp beleid opgesteld. In dat beleid wordt ook ingegaan op de bewaartermijn van persoonsgegevens na eindigen van het contract.
165	De leverancier dient (doorlopend) inzichtelijk te maken in welke landen persoonsgegevens (kunnen) worden opgeslagen. Eventuele contractuele waarborgen in het kader van hoofdstuk V van de AVG dient de leverancier eveneens inzichtelijk te maken.

2.6 Aanvullende eisen

Nr	Omschrijving
166	De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden.
167	Er zijn maatregelen getroffen die zeker stellen dat voldoende, complete en juiste (log)informatie beschikbaar is om gebeurtenissen zorgvuldig te analyseren (onderzoeken).
168	De dienstenleverancier en/of de ICT-afdeling draagt zorg voor het opstellen en onderhouden van beveiligingsdocumentatie die door de CISO verlangd en gecontroleerd wordt ten behoeve van de toestemmingsverlening.
169	De dienstenleverancier en/of de ICT-afdeling past hardening toe ter beveiliging van credential stores en -mechanismen.
170	De dienstenleverancier en/of ICT-afdeling past softwarebescherming toe overeenkomstig vastgestelde en gedocumenteerde procedures van de organisatie.

171	De dienstenleverancier en/of ICT-afdeling past (veilig) onderhoud toe overeenkomstig vastgestelde en gedocumenteerde procedures van de organisatie.
172	De authenticiteit en integriteit van software, firmware, patches en security-updates is bij installatie technisch geborgd.
173	Back-ups worden zodanig opgeslagen dat bij een incident niet zowel het ICT-systeem als de back-ups worden getroffen.
174	ICT-systemen leggen ten minste het volgende vast: • authenticatiegebeurtenissen; • bestands- en objectgebeurtenissen; • export- (bijv. downloads) en importgebeurtenissen (bijv. uploads); • gebeurtenissen betreffende gebruikersaccounts; • gebeurtenissen betreffende accounts met speciale bevoegdheden.
175	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is (kritieke beveiligings-updates/patches) worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten binnen vier weken na beschikbaar komen worden doorgevoerd. Als de inschatting is dat overige applicaties niet meer kunnen werken mag hier vanaf geweken worden, er moet dan wel een workaround bedacht worden. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst voor gemeenten (IBD).
176	De dienstenleverancier en/of ICT-afdeling test software en firmware updates voorafgaand aan installatie volgens vastgestelde (test)procedures als onderdeel van patchmanagement, releasemanagement en/of lifecycle management.

3. Wensen

Nr	Omschrijving	Weging
1	Bij wijziging van een arbeidsrelatie is er vaak sprake van overlap van werkzaamheden. Het IAM-systeem moet geautomatiseerd een tijdelijke verlenging van de oude rechten mogelijk maken.	2
2	Het komt voor dat een medewerker meerdere arbeidsrelaties heeft binnen eenzelfde partnerorganisatie. De manager van de eerste arbeidsrelatie is primair de goedkeurder. De manager van de tweede arbeidsrelatie moet ook kunnen goedkeuren. Bij het beëindigen van één van de arbeidsrelaties moeten de business rollen opnieuw worden bepaald en rechten ingetrokken worden. Ook moeten de goedkeuringsrechten van de manager voor die arbeidsrelatie ingetrokken worden.	2
3	Simuleren van wijzigen op een rol. Voordat een wijziging in een rol daadwerkelijk doorgevoerd wordt, moet het mogelijk zijn om: - op verzoek het effect van de wijziging te zien. - om een grenswaarde voor het aantal wijzigingen in te stellen, waarbij een waarschuwing gegeven wordt indien deze waarde wordt overschreden. Voorbeelden: - een autorisatie wordt toegevoegd aan een rol, welke identiteiten krijgen deze autorisatie - een autorisatie wordt uit een rol verwijderd. bij welke identiteiten gaat de autorisatie daadwerkelijk verwijderd worden.	3
4	Het IAM-systeem biedt de mogelijkheid om bij het samenstellen van een rol in te stellen dat goedkeuring vereist is, zowel van roleigenaar alsook van de eigenaar van de voorziening (goedkeuring dat de voorziening in de rol opgenomen wordt).	2
5	Gebruikers willen naast TOPdesk niet nog een portaal om autorisaties aan te vragen en/of goed te keuren. Op welke manier lost het IAM-systeem dit op?	3
6	Bij het aanvragen van rollen en rechten wordt de leidinggevende geholpen door een overzicht, waarin inzicht gegeven wordt welke autorisaties vergelijkbare medewerkers op de afdeling hebben.	3
7	Het IAM-systeem ondersteunt het automatiseren van het beheer van identiteiten (eigenaar, lid, gast) en toegang tot Microsoft Teams (kanalen, bestanden etc) en Sharepoint inclusief rapportagefunctionaliteit over de identiteiten en verleende autorisaties, indien de eigenaar van het Team of SP-site dit wenst.	3
8	De helpfunctie is contextueel: vanuit een specifiek scherm wordt direct ingezoomd op het betreffende onderwerp.	1
9	De functioneel beheerder kan zelf specifieke helpteksten toevoegen. Eis is dat deze helpteksten bij een nieuwe versie niet overschreven worden.	1
10	het IAM-systeem dient notificaties te kunnen versturen via verschillende kanalen (meldingen in IAM, mail, mobiele app). Dit kan een gebruiker zelf instellen.	1
11	Aanvullende IAM-rapportages worden als PowerBI-template geleverd.	2
12	Het IAM-systeem biedt dashboards met daarin opgenomen de rapportages en KPI's voor dagelijkse sturing.	2
13	De inschrijver heeft de mogelijkheid om de acceptatietestomgeving te vullen met gegevens en dit werkend te hebben in de hele keten van bron- en doelsystemen	2
14	Leverancier heeft het groeipact Common Ground ondertekend. Noot: SSC ONS hecht waarde aan het gedachtengoed Common Ground en wil dat haar (toekomstige) leveranciers zich achter de principes van Common Ground scharen. Dit leidt ertoe dat een grote stap gezet wordt naar een open, transparante overheid, waarbinnen met	1

	inachtneming van de privacyregels gegevens sneller en veiliger kunnen worden uitgewisseld, intern zowel als extern.	
15	Voor derdelijns support stelt opdrachtnemer een servicedesk ter beschikking met bij voorkeur Nederlands sprekende medewerkers. De openingstijden dienen minimaal aan te sluiten bij de tijden zoals vastgelegd in de SLA. De servicedesk is te benaderen voor technische en functionele vragen door Opdrachtgever. Er zijn geen extra kosten gemoeid met de afhandeling van deze vragen.	1
16	De medewerkers van de Opdrachtnemer beheersen bij voorkeur de Nederlandse taal in woord en geschrift op een voldoende niveau om de dienstverlening te kunnen borgen.	1
17	Opdrachtgever gebruikt TOPdesk als ITSM-systeem. Het ITSM-systeem van de opdrachtnemer kan met behulp van een API koppelen naar TOPdesk opdrachtgever om zo efficiënt de incidenten en wijzigingen te melden en automatisch de status te ontvangen in TOPdesk.	1
18	De leverancier maakt gebruik van een methode of best practice voor secure software development, zoals bijvoorbeeld van het CIP: https://www.cip-overheid.nl/	1
19	Een doorstroom of een uitstroom van een externe medewerker uit een andere organisatie leidt tot automatische mutaties/handelingen in het IAM-systeem door een federatieve koppeling met de externe organisatie	3