

Onderdeel/ Categorie	Eis nr.	Eis
-------------------------	---------	-----

Programma van Eisen Europese Openbare Aanbesteding "Vernieuwing back-up/ disaster & recovery"; datum: 22-04-2025; Versie: 1.0; kenmerk: 2025/0426831

De back-up / disaster & recovery oplossing

1. Algemeen	1.1	Alle geëiste functionaliteit dient bij voorlopige gunning beschikbaar en dus direct bruikbaar te zijn.
	1.2	De back-up/disaster & recovery oplossing is rechtstreek bij de leverancier in Nederland afgenomen. Opdrachtgever behoudt zich het recht om dit tijdens de voorlopige gunning te controleren.
2. Storage	2.1	De geboden oplossing bevat 2 storage pools on-premise, 1 per datacenter.
	2.2	De geboden oplossing bevat een storagepool in de cloud t.b.v. encrypted back-up data. Deze wordt bij de Leverancier afgenomen.
	2.3	De geboden oplossing kan back-up data opslaan bij alle gangbare cloud storage providers.
	2.4	Alle storage pools kunnen gebruikt worden voor zowel primaire- als secundaire kopieën.
	2.5	Back-ups van componenten in de Cloud worden primair weggeschreven naar de Cloud storage om vervolgens te worden gerepliceerd naar de on-premise storage als secundaire kopie. Back-up van componenten on-prem (Categorie B) worden primair weggeschreven naar de on-prem storage om vervolgens te worden gerepliceerd naar de Cloud storage als extra kopie. Back-up van componenten on-prem (Categorie A) worden primair weggeschreven naar de on-prem storage om vervolgens te worden gerepliceerd naar de andere on-prem storagepool als extra kopie.
	2.6	Alle kopieën worden immutable opgeslagen.
	2.7	Alle kopieën worden met een eigen encryptie sleutel versleuteld opgeslagen. De sleutel is alleen beschikbaar voor Opdrachtgever. De gebruikte encryptie key moet afdoende zijn beschermd.
3. Hardware	3.1	Benodigde on-premise hardware wordt ingericht op basis van Referentie architectuur. Inschrijver beschrijft op basis van referentiearchitectuur de benodigde hardware voor het optuigen van de back-up/disaster & recovery oplossing en storage.
	3.2	De oplossing kan gebruik maken van generieke storage servers om vendor-lock te voorkomen en voldoet daarbij nog steeds aan alle eisen (denk aan immutable back-ups). Denk hierbij in ieder geval, maar niet uitsluitend, aan: ExaGrid, HPE Apollo of Dell PowerStore
4. Cloud	4.1	De volgende Hypervisors worden minimaal ondersteund, zowel voor back-up van informatie (IaaS/PaaS) als voor opslag van informatie. ~ Microsoft Azure. ~ AWS. ~ Google cloud. ~ Oracle cloud.
5. Rententie	5.1	De rententie moet per archetype instelbaar zijn
	5.2	De rententie moet per kopie (primair/ secundair) instelbaar zijn.
	5.3	Binnen een archetype moet de rententie kunnen verschillen op basis van classificatie
	5.4	Als de rententie is verlopen moet de betreffende data automatisch en onherroepelijk worden verwijderd / ontoegankelijk gemaakt
	5.5	Het moet mogelijk zijn de rententie van een specifieke set aan data te verlengen. Denk hierbij bijvoorbeeld, maar niet uitsluitend, aan een scenario waarbij een lopend WOO verzoek waar de benodigde data grenst aan de rententie periode
	5.6	Er dient een selectieve set aan data kunnen worden weggeschreven naar een storage oplossing voor lange termijn rententie (>= 7 jaar). De bron voor deze set aan data moet zowel de primaire- als secundaire kopie kunnen zijn
6. Back-up strategie	6.1	Er moet aan de 3-2-1-1-0 norm voldaan worden: - Ten minste 3 kopieën van gegevens: Het hebben van ten minste 3 kopieën van gegevens, waarvan één de primaire kopie is en twee extra kopieën zijn, zorgt voor redundantie en minimaliseert de kans op gegevensverlies. - Opslaan van kopieën op ten minste 2 verschillende media: Door de gegevens op ten minste twee verschillende media op te slaan, zoals harde schijven, tapes of cloudopslag, wordt het risico van gegevensverlies als gevolg van een storing in één medium geminimaliseerd. - Ten minste 1 kopie van de gegevens moet extern worden opgeslagen: Het extern opslaan van ten minste één kopie van de gegevens, bijvoorbeeld op een offsite server of in een cloudopslag, zorgt voor extra bescherming tegen gegevensverlies door diefstal, brand of overstroming. - Ten minste 1 kopie van de gegevens moet immutable worden opgeslagen: Het opslaan van ten minste één kopie van de gegevens, die de gegevens beschermt tegen ransomware en andere kwaadaardige software die het netwerk kan infecteren. - 0 fouten in de back-up- en herstelprocessen: Het uitvoeren van regelmatige testen om ervoor te zorgen dat de back-up- en herstelprocessen correct werken, is essentieel om de gegevensveiligheid te garanderen en eventuele problemen snel op te lossen.
	6.2	Waar mogelijk het incremental forever principe hanteren. Denk hierbij, maar niet uitsluitend, aan: ~ Virtual Machines (VMware, KVM, Hyper-V) ~ Microsoft 365 (Exchange Online, Teams, OneDrive en SharePoint) ~ Kubernetes
	6.3	Databases, Active Directory en EntraID zullen op regelmatige basis een Full back-up nodig hebben en zijn derhalve uitgesloten van bovenstaande
	6.4	Bij een incremental forever back-up moet er op reguliere basis een synthetic full gemaakt kunnen worden
	6.5	Er dienen op nader te definiëren reguliere momenten automatisch health checks uitgevoerd te worden op de Incremental back-ups en back-up chains
7. Restore	7.1	Item level restore moet vanaf zowel primaire- als secundaire storage mogelijk zijn
	7.2	Item level restore moet voor de volgende archetypes in ieder geval mogelijk zijn: ~ Exchange (on-prem en Online); ~ Fileservers; ~ SharePoint Online; ~ Teams; ~ OneDrive; ~ Database servers (MS SQL, PostgreSQL, Oracle, MariaDB enz.
	7.3	Restores moeten zowel in-place als out-of-place mogelijk zijn. Dit geldt voor zowel full restore als item level restore
	7.4	Item level Out-of-place restore moet zowel on-prem als in de cloud mogelijk zijn. Ongeacht de bron van de data.
	7.5	De oplossing kan cross platform restores zonder dat de beheerder een conversie hoeft uit te voeren
	7.6	Een Full restore moet bij elke archetype mogelijk zijn
	7.7	Bij restore van een fysieke of virtuele server kan, na een basis installatie van het OS, de system state vanuit de backup hersteld worden (bare metal restore)
	7.8	De oplossing kan cross hypervisor restoren zonder dat de beheerder een conversie hoeft uit te voeren
	7.9	Met behulp van de nieuwe back-/disaster & recovery oplossing en door de Inschrijver voorgestelde hardware en verbindingen (specs/requirements) dienen de systemen van de gemeente bij een disaster binnen 10 dagen hersteld te zijn.
	7.10	Er is altijd herstel mogelijk vanuit de back-up data. Ook in de toekomst als de licentie / support is verlopen. Daarbij is ook geen afhankelijkheid van connectiviteit
8. Hypervisor (Virtualization)	8.1	De volgende Hypervisors dienen minimaal te worden ondersteund: ~ VMware vSphere; ~ Microsoft Hyper-V; ~ Oracle KVM; ~ IaaS bij diverse Cloud providers (zoals Microsoft Azure, AWS, Google cloud, Oracle cloud)
9. Archetypes	9.1	De volgende archetypes dienen minimaal te worden ondersteund: ~ VMware Virtual Machine; ~ Software Defined configuraties, inclusief koppelingen met objecten. ~ Oracle KVM virtual machine; ~ Microsoft Hyper-V virtual machine; ~ Oracle Database; ~ SQL database; ~ PostgreSQL database; ~ MySQL database; ~ MariaDB database; ~ Microsoft Exchange database (On-prem); ~ Microsoft Exchange mailbox (on-prem en Exchange Online); ~ Microsoft Active Directory; ~ Microsoft Entra; ~ Microsoft 365: -Sharepoint Online -OneDrive for Business -Teams -Exchange Online ~ PaaS / IaaS bij diverse cloud providers; ~ Kubernetes.
10. Validatie data uit back-up bij restore	10.1	Herstel van data uit de back-up moet pro-actief geleverd kunnen worden door middel van recovery in een afgeschermd omgeving. Deze pro-actieve herstel mag nooit de data in productie hinderen
	10.2	Tijdens dit pro-actieve herstel wordt er gecontroleerd of de herstelde data nog vrij is van indicatoren van besmetting. (Ransomware en andere bekende virussen).
11. Ransomware protection	11.1	De back-up oplossing dient een mechanisme te bezitten die (near real-time) verdachte activiteiten en bestanden kan detecteren (thread detection).
	11.2	Bij detectie van verdachte activiteiten en / of bestanden worden er notificaties verstuurd. Denk hierbij aan notificatie via E-mail naar beheerders maar ook aan registratie in een syslog server (SOC/ SIEM).

12. Management server Met management server wordt de server bedoelt die de aansturing van de back-up oplossing regelt (core component)	12.1	De managementserver draait primair alleen on-prem. Het moet echter wel mogelijk zijn om de managementserver in de cloud eenvoudig op te spinnen om het disaster & recovery proces op te starten.
	12.2	Vanaf het moment dat een virtuele server beschikbaar is moet de managementserver binnen 2 uur op te spinnen zijn.
	12.3	De management server dient on-prem in 2 uur hersteld te kunnen worden.
	12.4	De management server moet zowel hardware matig, software matig (VM) als Cloud based kunnen zijn
	12.5	Bij verlies van de back-up oplossing door een aanval (maar geen verlies van de immutable back-up data) kan er eenvoudig herstel plaatsvinden vanuit deze back-up data
	12.6	Er hoeft niet eerst een complexe infrastructuur opgetuigd te worden voordat er hersteld kan worden vanuit de back-up. Denk bijvoorbeeld aan het beschikbaar zijn van de back-up metadata of deduplicatie databases
	12.7	De configuratie van de management server moet minimaal 1 keer per uur veilig worden gesteld
	12.8	Dit veilig stellen dient op een dusdanige manier gedaan te worden dat er, bij uitval van de management server (om welke reden dan ook), gemakkelijk een nieuwe management server in de lucht kan worden gebracht.

Non-functionals

1. Algemeen	1.1	Alle geëiste non-functionals dienen bij in productie name verwezenlijkt zijn.
	1.2	Het systeem moet primair worden geleverd als on-premise oplossing. Voor authenticatie op het primaire systeem zal de IDP van Opdrachtgever gebruikt worden, waarnaast voor noodsituaties een BTG-account beschikbaar moet zijn. Voor Disaster Recovery en test-doelenden zal een cloud-omgeving worden ingericht, waarbij synchronisatie tussen omgevingen via een geïsoleerde veilige verbinding zal gebeuren.
	1.3	De oplossing is zo eenvoudig mogelijk met zo min mogelijk complexiteit. De beheerlast is zo laag mogelijk. Inzet van vendor professional services bij aanpassingen is niet nodig.
	1.4	Hosting van de dienst en de data vindt fysiek plaats binnen de Europese Economische Ruimte.
	1.5	De oplossing is gebaseerd op proven technology. Het is minimaal 1 jaar beschikbaar en bij minimaal 4 vergelijkbare (semi-)overheidsorganisaties in Nederland zonder noemenswaardige issues in gebruik
	1.6	De oplossing moet voldoen aan relevante wet- en regelgeving
	2.1	De oplossing moet niet afhankelijk zijn van het te beschermen domein van de gemeente, bv vlot herstel is mogelijk als het domein van de gemeente geheel onbeschikbaar is, bijvoorbeeld na een succesvolle ransomware aanval.
	2.2	De oplossing kan gebruik maken van generieke storage servers om vendor lock-in te voorkomen en voldoet daarbij nog steeds aan alle eisen (denk aan immutable backups).
	2.3	De oplossing bevat een audit-trail, welke niet muteerbaar is.
	2.4	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; ~ Bij beëindiging van een bepaalde autorisatie is herleidbaar dat deze autorisatie ooit bestaan heeft, inclusief bijbehorende audit-trail.
2. Technische eisen	2.5	Indien een rol, groep of functie beëindigd wordt, is herleidbaar dat deze ooit bestaan heeft, inclusief bijbehorende audit-trail.
	2.6	Deze logging wordt behalve lokaal opgeslagen, ook naar een centraal loggingsysteem van Opdrachtgever gestuurd.
	2.7	Alle componenten (inclusief koppelingen met externe applicaties) die door Opdrachtnemer beschikbaar worden gesteld en alle ondersteunende applicaties worden bijgehouden op het laatste security- en servicepack-level. De oplossing kan hiermee omgaan.
	2.8	Er moet gebruik worden gemaakt van vaste, specificeerbare (niet random) poorten (TCP/UDP) voor data-verkeer tussen componenten binnen de oplossing.
	2.9	<u>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 voor encryptie van dataverkeer.</u>
	2.10	Opdrachtnemer garandeert de werking van beheerfunctionaliteit op gangbare platforms/browsers zonder de installatie van extra plugins of extensies
	2.11	De oplossing 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.
	2.12	De oplossing ondersteunt zowel het gebruik van een ipv4, als ipv6
	2.13	De oplossing voldoet aan de Baseline Informatiebeveiliging Overheid (BIO), en is voorbereid op BIO2 en de Cyberbeveiligingswet.
	2.14	Opdrachtnemer/Leverancier beschikt over gangbare certificeringen als ISO 27001 en ISO 9001 en passende assurance verklaringen, waarmee de goede werking van de beheersmaatregelen onafhankelijk wordt vastgesteld.
3. Beveiligingseisen	2.15	De oplossing moet flexibel zijn om verschillende opslaglocaties (on-premise, cloud, hybride) te ondersteunen en schaalbaar zijn naarmate de hoeveelheid data groeit
	3.1	De oplossing moet volgens het 4 ogen principe werken bij het verwijderen of aanpassen van configuratie gegevens.
	3.2	Toegang tot de informatie vanuit de backup-data is alleen mogelijk via de nieuwe back-up/disaster & recovery oplossing.
	3.3	Toegang tot dede nieuwe back-up/disaster & recovery oplossing is tenminste met Two-Factor-Authenticatie afgeschermd. De oplossing heeft mogelijkheden extra MFA af te dwingen.
	3.4	De autorisaties dienen rol gebaseerde autorisaties te zijn. 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.
	3.5	Alle data op het systeem is versleuteld volgens vigerende standaarden (BIO, Forum Standaardisatie en NCSC richtlijnen).
	3.6	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 / DAP.
	3.7	De oplossing past strikte scheiding van tenants toe op alle niveaus, behalve fysiek.

Het project

1. Algemeen	1.1	Opdrachtnemer is in staat uitvoering te geven aan de Opdracht gedurende de gehele looptijd van de overeenkomst, zoals omschreven in de aanbestedingsleidraad en bijbehorende documenten.
2. PoC	2.1	Inschrijver benoemt voor de PoC tijdens de verificatiefase een projectmanager die de regie over het gehele proces uitvoert en het enige aanspreekpunt is voor de Opdrachtgever. De projectmanager en verdere uitvoering van de PoC worden kosteloos door Inschrijver beschikbaar gesteld.
3. Levering	3.1	Opdrachtnemer voert alle verpakkingsmateriaal af en laat deze, voor zover mogelijk, recycleren.
	3.2	Alle geleverde hard- en software dient te vallen onder het aangeboden support-contract.
4. Projectplan (implementatieplan)	4.1	Opdrachtnemer stelt samen met Opdrachtgever, binnen 2 weken na voorlopige gunning, een projectplan (implementatieplan) op. Het projectplan bevat een voorstel met betrekking tot de planning van de implementatie van de nieuwe back-up/disaster & recovery oplossing.
5. Detail ontwerp oplossing	5.1	Bij ontwerpen maakt u keuzes. Een goede ontwerper maakt keuzes en anticipeert daarbij op toekomstige veranderingen, ofwel een goed ontwerp is duurzamer, flexibeler, kwalitatief beter en gaat langer mee. Ontwerpen is daarom meer dan een werkende back-up/disaster & recovery oplossing ontwerpen. Ontwerpen brengt structuur aan, waardoor het systeem eenvoudig aan te passen is aan veranderende eisen. Een goed doordacht en uitgewerkt ontwerp is dus een investering in toekomstige waarde. Het vakmanschap van een ontwerper uit zich in een duidelijke abstractie, het scheiden van functies en het volgen van toepasselijke patronen. Dit leidt tot een begrijpelijk en duidelijk in kaart gebracht ontwerp. Opdrachtgever verlangt dat de ontwerper(s) van Opdrachtnemer: ~ de kennis en kunde hebben om de juiste (ontwerp)keuzes te maken, ~ kennis en ervaring hebben om gestructureerde ontwerpen op te leveren, ~ bekend zijn met begrippen als Design Patterns, Separation of Concern en Data Integrity, ~ de benodigde kwaliteit hebben om goede, bewezen stabiele en 'eenvoudig aan te passen' omgeving te ontwerpen. ~ alles vastleggen in documentatie (infrastructuur, architectuur, verbindingen, ontwerpkeuzes, beslissingen, etc.)
	5.2	Het ontwerp en de implementatie moeten voldoen aan de kenmerken toekomstgericht, toekomst vast, flexibiliteit, continuïteit, simpel (vermijden van onnodige complexiteit), geautomatiseerd en sterke beveiliging.
	5.3	Het is natuurlijk onmogelijk om vandaag te voorspellen wat precies de behoeften van morgen zullen zijn, maar het is een verantwoordelijkheid van de ontwerper om het mogelijk te maken dat de oplossing eenvoudig in de toekomst kan aansluiten op nieuwe technologieën. Dit kan door steeds te beseffen dat datgene wat u ontwerpt eenvoudig vervangen moet kunnen worden door iets anders, of verder uitgebreid moet kunnen worden. Een architectuur die opgedeeld is in onafhankelijke componenten met gedefinieerde koppellakken is daarbij een eis, die we willen terug zien komen in de documentatie.
6. Implementatie oplossing	6.1	De Opdrachtnemer levert een "turn-key" back-up/disaster & recovery oplossing. Implementatie wordt door Opdrachtnemer uitgevoerd, in samenspraak met Opdrachtgever. Waarbij de Opdrachtnemer in ieder geval verantwoordelijk is voor: ~ installeren van de complete back-up/disaster & recovery oplossings on-premise op referentie hardware. ~ Inrichten en configureren van de nieuwe back-up/ disaster & recovery oplossing conform het ontwerp, waarbij een minimum van 2 instances per archetype die op het moment van inrichten bij Opdrachtgever in gebruik zijn geldt. (waar van toepassing) ~ Instellen policies (back-ups, retention enz.). ~ Inventariseren en implementeren van benodigde autorisaties. ~ Doorvoeren vereiste beveiligingsmaatregelen in de nieuwe back-up/ disaster & recovery oplossing. ~ Realiseren van de koppeling met de storage (on-premise en in de Cloud). ~ Realiseren van de overige koppelingen en verbindingen. ~ Testen van de inrichting en de werking van de nieuwe back-up/ disaster & recovery oplossing, en oplossen van issues.
	6.2	De Opdrachtnemer brengt in samenwerking met Opdrachtgever de huidige processen in kaart. Beschrijft per proces/procedure hoe dit met nieuwe back-up/ disaster & recovery oplossing werkt. Beschrijft in ieder geval de volgende procedures: ~ Maken back-up, ~ Uitvoeren restore, ~ Aanpassen config (schedules, storage policies, retention enz.), ~ User beheer, ~ Uitvoeren updates.
	6.3	De partij die de implementatie bij Opdrachtgever verzorgt, heeft kennis en ervaring van alle componenten van de oplossing, en kan zelfstandig de volledige implementatie kan verzorgen.
	6.4	De Opdrachtnemer houdt tijdens de implementatie een overzicht bij van alle ontwerp keuzes, en deelt dit document wekelijks/ na wijzigingen met de Opdrachtgever.
	6.5	De Opdrachtnemer borgt tijdens implementatie dat issues met hoge prioriteit direct opgepakt worden.

7. Training	7.1	"Training on the job" vindt i.o.m. Opdrachtgever plaats in huis dan wel digitaal. Dit betreft maatwerk ondersteuning van de beheerders van de gemeente bij het inrichten van de omgeving, het doorvoeren van beveiligingsmaatregelen, het realiseren van koppelingen en verbindingen, het uitvoeren van de genoemde werkzaamheden ten behoeve van de in productie name.
8. Acceptatie	8.1	Opdrachtnemer stelt (samen met Opdrachtgever) acceptatie-testplan op met als doelstelling de verificatie van de gestelde eisen in het document.
	8.2	Het project kent twee acceptatiemomenten: 1. Acceptatie van de inrichting en de werking van de oplossing. Deze acceptatietest moet aantonen dat: o de complete opstelling (software & hardware) is opgeleverd, ingericht en voldoet aan de functionele een non-functionele eisen uit dit Programma van Eisen . o de werking van de nieuwe back-up/disaster & recovery voldoet aan de functionele een non-functionele eisen uit dit Programma van Eisen. 2. Volledige acceptatie van het project. o Deze acceptatie moet aantonen dat alles is opgeleverd conform Aanbestedingsdocumentatie, Nota van Inlichtingen, Inschrijving, Projectplan en Acceptatie-testplan .
	8.3	Opdrachtnemer begeleidt de acceptatietesten door Opdrachtgever en verhelpt eventuele issues mbt de geleverde back-up/disaster & recovery oplossing, die voortkomen uit de acceptatietesten.
	8.4	Indien de acceptatietesten niet het gewenste resultaat geven, vinden hertesten plaats nadat de issues verholpen zijn.
	8.5	Indien het testen van een instelling niet mogelijk is, dient Opdrachtnemer aan te tonen dat de benodigde configuratie van een instelling is aangebracht.
	8.6	Zowel het detailontwerp, de gevraagde documentatie en de hardening zijn onderdeel van de acceptatie.
	8.7	Aan het eind van het project wordt gecontroleerd of alles conform specificaties is opgeleverd, wat leidt tot decharge van Opdrachtnemer. Mocht uit de acceptatie naar voren komen dat de opgeleverde back-up/disaster & recovery oplossing niet voldoet of niet compleet zijn, dan dient Opdrachtnemer dit binnen 5 werkdagen te verhelpen
9. Documentatie	9.1	Documentatie wordt opgesteld in de Nederlandse of de Engelse taal. Engelse woorden voor IT en merk specifieke termen zijn in Nederlandstalige documentatie toegestaan.
	9.2	Opdrachtgever wordt eigenaar van alle gemaakte documenten en ontwerpen.
	9.3	Documenten worden in Word-formaat aan opdrachtgever opgeleverd.
	9.4	Tekeningen worden in een nader af te stemmen, bewerkbaar voor opdrachtgever, formaat (bij voorkeur Microsoft Visio) opgeleverd.
	9.5	Onder de documentatie valt in ieder geval een uitgewerkt detailontwerp, een beschrijving van de configuratie van alle geleverde componenten en beschrijving van veel voorkomende werkprocedures.
	9.6	In de documentatie worden in ieder geval de gebruikte standaarden, motivatie van gemaakte keuzes waaronder de toegepaste hardening toegelicht.
	9.7	Opdrachtnemer draagt zorg voor het maken van een gedetailleerd ontwerp bij de start van de implementatie. Dit dient samen met de Opdrachtgever gemaakt te worden en beschikbaar gesteld te worden t.b.v. de implementatie. Na decharge van het project dient het ontwerp overgedragen te worden aan de beheerorganisatie.

Licenties, support & beheer

1. Licenties	1.1	Alle in de aanbesteding gevraagde functionaliteit zal binnen de aangeboden licentie moeten vallen. Eventueel benodigde Add-On licenties zullen in de aanbidding meegenomen moeten worden
	1.2	De (primaire) Cloud storage dient meegenomen te worden in de aanbidding. Dit betreft encrypted backup data / backup storage pools.
	1.3	Indien door verhoging van het aantal systemen of de hoeveelheid data extra licenties moeten worden afgenomen, mag de prijs van licenties niet geïndexeerd worden.
	1.4	Volgende feature is onderdeel licentiestructuur "backup operations create a point-in-time snapshot of data to be used for various data protection operations." Deze 'snapshot back-up' ondersteund alle database systemen
	1.5	Het systeem is berekend op groei van de hoeveelheid data en de verschuiving van data naar de cloud zodanig dat de eerste 3 jaar géén grote extra investeringen nodig zijn. In de prijsopgave moet Opdrachtnemer onderbouwen hoe dit met het aangeboden systeem gerealiseerd kan worden.
2. Support	2.1	De support dient te worden meegenomen in de aanbidding
	2.2	De aangeboden oplossing heeft tijdens het moment van aanbieden geen end-of-sale binnen 5 jaar, om in deze periode eventuele benodigde add-ons te kunnen aanschaffen.
	2.3	Het Supportcontract treedt in werking bij de in productie name van de back-up/disaster & recovery oplossing.
	2.4	Het Supportcontract is bij het begin van het daadwerkelijke implementatietraject afgesloten.
	2.5	Het Supportcontract bevat in ieder geval de onderstaande afspraken: ~ Voor alle P1 incidenten reageert Opdrachtnemer/Leverancier tijdens kantooruren uren binnen 60 minuten. Kantooruren Opdrachtgever zijn van 8.00 tot 17.00 uur. ~ Voor alle P2 incidenten reageert Opdrachtnemer/Leverancier tijdens kantooruren uren binnen 120 minuten. Kantooruren Opdrachtgever zijn van 8.00 tot 17.00 uur. ~ Voor alle P3/P4 incidenten reageert Opdrachtnemer/Leverancier tijdens kantooruren uren binnen 1 dag. Kantooruren zijn van 8.00 tot 17.00 uur. ~ Opdrachtgever kan tijdens kantooruren telefonisch contact opnemen met Support van Opdrachtnemer om incidenten te melden. ~ Zodra een incident is geregistreerd en bevestigd door Opdrachtnemer/Leverancier, werkt Opdrachtnemer/Leverancier aan het op afstand verhelpen en oplossen van het incident van de Opdrachtgever tijdens kantooruren. ~ Opdrachtgever heeft toegang tot het downloaden, installeren en gebruiken van firmware-updates voor haar producten. ~ Opdrachtgever kan een online chat starten met een gespecialiseerde technische resource om vragen te stellen, hulp of algemene technische begeleiding te krijgen. ~ Opdrachtgever heeft 24x7 toegang tot online zelfbediening van Opdrachtnemer en mogelijkheden om het zelf op te lossen (Service Portaal) ~ Opdrachtgever kan in de Service Portaal cases aanmaken en beheren, waarschuwingen en meldingen bekijken (inclusief aankondigingen van beschikbare kritieke downloads en
3. Beheer	3.1	Patch management van niet door Opdrachtgever beheerde componenten is aantoonbaar ingericht. Updates en upgrades worden tijdig uitgevoerd volgens overeengekomen afspraken opgenomen in de SLA / DAP.
	3.2	De door Opdrachtnemer uit te voeren updates en upgrades worden tijdig aangeleverd door Opdrachtnemer, conform de nader te definiëren afspraken in de SLA / DAP.
	3.3	T.b.v. upgrades en updates van de oplossing documenteert de Opdrachtnemer de belangrijkste wijzigingen en consequenties voor het functioneren van de oplossingen en de koppelingen en stelt deze beschikbaar aan de Opdrachtgever in de vorm van release notes.

SLA/ DAP

1. Onderhoud, support en SLA	1.1	Alle geleverde hard- en software wordt voor de gehele duur van de overeenkomst onderhouden, gesupport en voorzien van reguliere en noodzakelijke (security)updates.
	1.2	Mocht in de contractperiode wet- en regelgeving veranderen, dan voert Opdrachtnemer/Leverancier deze wijziging overeenkomstig de door overheid gestelde termijnen binnen de back-up/disaster & recovery oplossing door, zonder het contract open te breken en nieuwe onderhandelingen te starten. De hieruit voortvloeiende werkzaamheden worden met betrokken partijen afgestemd, evenals de eventueel door te belasten kosten.
	1.3	Afspraken op operationeel niveau dienen in een DAP (Dossier Afspraken en Procedures) opgenomen te worden. Het DAP wordt beschouwd als een levend dossier wat tijdens de duur van de overeenkomst aangepast kan worden op verzoek van zowel opdrachtgever als opdrachtnemer.
	1.4	De beheerders kunnen voor support rechtstreeks contact opnemen met Opdrachtnemer/ Leverancier.
	1.5	Bij telefonisch en schriftelijk contact met de supportdesk van Opdrachtnemer is Nederlands of Engels de voertaal.
	1.6	De support van Opdrachtnemer/ Leverancier is 5 dagen x 9 uren bereikbaar, waarbij minimum eisen voor de SLA van toepassing zijn.
	1.7	Opdrachtnemer gaat er mee akkoord dat eisen zoals in dit PvE verwoord minimaal worden opgenomen in de SLA.
	1.8	Na de ontwerpfase wordt in overleg tussen Opdrachtnemer en Opdrachtgever een dienstverleningsovereenkomst (SLA) definitief opgesteld en vastgesteld
	1.9	De support- en onderhoudscontracten gaan in bij in productie van de back-up/disaster & recovery oplossing.
2. Minimaal op te nemen c.q. te	2.1	Opdrachtnemer monitort en borgt de performance van het systeem na implementatie. Onderdeel hiervan is een nulmeting en op gezette tijden controleren wat de status van performance is ten opzichte van de nulmeting/norm (inclusief trendoverzicht).
	2.2	SLA/DAP omvat een beschrijving van: - het incident-, change- en releasemanagement proces van de back-up/disaster & recovery oplossing (inclusief koppelingen/verbindingen). - het service level management proces en bijbehorende rapportages.
	2.3	Bepalen prioritering met betrekking tot oplossingen en/of een gebrek aan het systeem (escalatiemodel); ~ Prio1 (calamiteit): 60 minuten reactietijd. 4 uur hersteltijd. ~ Prio2 (hoog): 2 uur reactietijd. Hersteltijd volgende werkdag ~ Andere meldingen (Prio3/Prio4; middel/laag): 1 dag reactietijd. Hersteltijd 5 werkdagen (best effort).
	2.4	Communicatie over status van aangemelde problemen; ~ Prio1: elke 2 uur een statusupdate. ~ Andere meldingen (Prio2/Prio3/Prio4): een voorspelling over de oplostermijn en bij lopende onderzoeken of geen zicht op een oplossing binnen de termijn elke werkdag een statusupdate.
	2.5	Een beschrijving van de wijze waarop er contact is tussen Opdrachtnemer en Opdrachtgever/ Leverancier na het implementatietraject voor wat betreft support.
	2.6	Een beschrijving van de wijze waarop er contact is tussen de accountmanager van Opdrachtnemer en de Opdrachtgever. Er dient jaarlijks overleg te zijn met de accountmanager van Opdrachtnemer/Leverancier.
	2.7	Gepland onderhoud valt buiten het beschikbaarheidspercentage. Dit gepland onderhoud wordt bij voorkeur één (1) maand van tevoren bekend gemaakt en in afstemming met Opdrachtgever ingepland. Afspraken omtrent downtime worden opgenomen in de SLA.
	2.8	Afspraken over inrichting van patch- en vulnerability management. SMART afspraken t.a.v. het verrichten van (noodzakelijke) systeemupdates, het oplossen van kwetsbaarheden, het melden van kwetsbaarheden aan Opdrachtgever, en een beschrijving wie wat doet ihkv patch- en vulnerability management .
	2.9	Afspraken over levering van reguliere en noodzakelijke (security)updates.
	2.10	De helpdesk van Opdrachtnemer/Leverancier is bereikbaar op werkdagen tussen 8:00 uur en 17:00 uur.

Juridische eisen

1. Juridische eisen	1.1	Alle overlegde gegevens zijn naar waarheid ingevuld. Opdrachtgever behoudt zich het recht op schadevergoeding voor in geval van onjuistheden en/of onvolledige informatie en/of het niet kunnen nakomen van hetgeen door u is aangeboden.
	1.2	Inschrijver gebruikt het voorgeschreven prijsinvalformulier en vult deze volledig in (Bijlage 7). Wijzigingen aan de lay-out van deze invalformulieren is niet toegestaan.
	1.3	Inschrijver en de te leveren dienstverlening voldoen en blijven voldoen aan het doel waarvoor Opdrachtgever ze gebruikt en voldoen aan alle Nederlandse wet- en regelgeving en eventuele van toepassing zijnde branche gerelateerde regelgeving.
	1.4	Deze Aanbesteding inclusief alle bijlagen is vertrouwelijk.
	1.5	Inschrijver neemt vertrouwelijkheid in acht ten aanzien van de informatie die hem bekend is of wordt over de wijze van inrichting en functioneren van de organisatie van Opdrachtgever.

- | | |
|-----|--|
| 1.6 | Op de Aanbesteding en de hieruit voortkomende Overeenkomst zijn uitsluitend de 'Algemene inkoopvoorwaarden GIBIT 2023' van toepassing, voor zover daarvan in de Overeenkomst niet wordt afgeweken. |
| 1.7 | Inschrijver conformeert zich volledig en onvoorwaardelijk aan de 'Algemene inkoopvoorwaarden GIBIT 2023' (Bijlage 1). |
| 1.8 | Inschrijver conformeert zich volledig en onvoorwaardelijk aan de bijgevoegde Verwerkersovereenkomst (Bijlage 8). |
| 1.9 | Inschrijver conformeert zich volledig en onvoorwaardelijk aan de bijgevoegde concept Overeenkomst (Bijlage 5). |

Facturering

1. Facturatieschema	1.1	Na de voorlopige gunning zal in samenspraak met de Opdrachtnemer de planning van de levering van de producten en van de werkzaamheden worden vastgesteld. Op basis hiervan zal een definitief facturatieschema worden vastgesteld.
2. Facturatie	2.1	Voor de facturatie van de leveringen en de geleverde dienstverlening stuurt Opdrachtnemer een (verzamel)factuur. In ieder geval dient op iedere factuur de volgende informatie vermeld te worden: ~ Het inkoopnummer van opdrachtgever dat in de Opdracht is vermeld; ~ De naam van de contactpersoon/besteller van Opdrachtnemer; ~ Volledige NAW van Opdrachtnemer; ~ Het Kamer van Koophandel nummer van Opdrachtnemer; ~ Het bankrekeningnummer (IBAN-code) van Opdrachtnemer. Indien u uw verbintenissen, voortvloeiende uit de Overeenkomst niet geheel of niet naar behoren nakomt, heeft Opdrachtgever het recht de betaling op te schorten
	2.2	Alle facturen worden digitaal gericht aan crediteuren@haarlem.nl
	2.3	Opdrachtnemer levert van tevoren proforma facturen aan met een weergave van de kosten die werkelijk gefactureerd gaan worden, de juiste NAW gegevens inclusief BTW en bankrekening nummer. Deze proforma facturen heeft Opdrachtgever nodig voor het aanmaken van de verplichtingen.