

1. Ingest		
De Oplossing biedt een duurzame opslag van informatieobjecten van de gemeente Den Haag, maar daarnaast ook overgebrachte of uitgeplaatste informatieobjecten van andere (overheids)organisaties, waarvoor de gemeente Den Haag de zorg draagt. De informatie van deze andere organisaties moet volstrekt gescheiden opgeslagen en beheerd kunnen worden. De informatie van deze andere organisaties moet volstrekt gescheiden opgeslagen en beheerd kunnen worden. In dit document wordt dit aangeduid als een tenantstructuur. Bij een tenantstructuur zijn er meerdere oplossingen naast elkaar beschikbaar met gescheiden databases en software. Dit is geen vereiste, een softwarematige oplossing voldoet ook.		
Nr.	Omschrijving	
1.1	Het moet mogelijk zijn om een tenantstructuur in de duurzame bewaaromgeving in te richten, waarbij de informatieobjecten van de tenants volstrekt gescheiden opgeslagen kunnen worden.	EIS
1.2	De Oplossing kan voor tenants verschillende inname-mogelijkheden toepassen. Hiermee wordt bedoeld de manier waarop de informatieobjecten ontvangen worden, de ingest-controles die uitgevoerd worden, de toegang tot de digitale informatieobjecten, welke preserveringsacties uitgevoerd worden.	EIS
1.3	Informatieobjecten, in een SIP, worden opgenomen (ingest) in de duurzame bewaaromgeving middels een package conform het OAIS-model. De SIP doorloopt verschillende verwerkingsstappen in de ingest-functie om een package tot stand te brengen die, kwalitatief gezien, gereed is voor lange termijn toegankelijkheid. De Oplossing kan het packagen van objecten in AIP conform het OAIS-model faciliteren.	EIS
1.4	Er kunnen per tenant meerdere ingestprocessen tegelijkertijd worden uitgevoerd.	EIS
1.5	De Oplossing controleert op bitintegriteit: controleren of het object na transport onbeschadigd is door het geleverde checksum te vergelijken met het checksum dat De Oplossing heeft aangemaakt.	EIS
1.6	Indien er sprake is van een fout in de bitintegriteit van een informatieobject moet de Oplossing dit signaleren en rapporteren, zodat de beheerder een herstelprocedure kan starten. Een automatische herstelprocedure met rapportagefunctionaliteit is ook geschikt.	EIS
1.7	De Oplossing genereert de PRONOM PUID en slaat die in de metadata bij het bestand op.	EIS
1.8	De Oplossing controleert op toegestane bestandsformaten. De minimale eis is dat de oplossing kan controleren of het informatieobject voldoet aan de lijst met voorkeursformaten, opgesteld door het Nationaal Archief, of het PRONOM-register, opgesteld door The National Archives in het Verenigd Koninkrijk. Mochten de bestandsformaten niet voldoen aan de lijst, dan bepaalt de beheerder of de objecten ingenomen mogen worden.	EIS
1.9	Bij ingest vindt er screening plaats op: virussen, corrupte files, volledigheid, integriteit (checksum), validiteit en juistheid toegekende bestandsformaten.	EIS
1.10	De checksum wordt opgeslagen als een (intern) metadataveld.	EIS
1.11	De Oplossing bevestigt een geslaagde ingest of geeft een foutrapportage. De Oplossing presenteert de uitkomst van alle door de Oplossing uitgevoerde ingests en controles op een geordende en gebruiksvriendelijke manier.	EIS
1.12	De Oplossing biedt daarnaast ook de mogelijkheid om informatieobjecten handmatig op inhoud te controleren. De medewerker kan bijvoorbeeld de informatieobjecten openen en inzien.	EIS
1.13	De Oplossing stelt de technische eigenschappen van de informatieobjecten vast en registreert deze.	EIS
1.14	Het is mogelijk om overzichten te krijgen op zowel lopende als afgeronde ingest workflows.	EIS
1.15	Het is mogelijk om metadata in xml en csv formaten te exporteren. Hierbij moet een selectie van de informatieobjecten mogelijk zijn.	EIS
1.16	Er is een aparte opslag voor aangeleverde informatieobjecten voor ingest (quarantaine-omgeving).	EIS

1.17	Gedrag van documenten (indien aanwezig) wordt meegenomen bij ingest; character reading/hyperlinks/macro's/formules/audiovisueel.	EIS
1.18	Het is na ingest mogelijk metadata toe te voegen en te bewerken, zowel van afzonderlijke informatieobjecten als in bulk.	EIS
1.19	De applicatie hanteert Unicode voor de codering van grafische tekens en symbolen en is daardoor in staat onder meer om te gaan met diakrieten.	EIS

2. Duurzame bewaaromgeving		
Nr.	Omschrijving	
2.1	Geautoriseerde medewerkers kunnen informatieobjecten inzien.	EIS
2.2	Geautoriseerde medewerkers kunnen in de duurzame bewaaromgeving eenvoudig en gebruiksvriendelijk zoeken naar aanwezige digitale informatieobjecten. Zoeken moet kunnen op deze metadata indien die zijn aanwezig zijn in de applicatie (meegegeven bij de ingest of aangevuld). Ook kan er booleaans en met jokertekens worden gezocht.	EIS
2.3	Originele manifestaties die ingenomen zijn in de duurzame bewaaromgeving behouden hun authenticiteit en wijzigen nooit. In de duurzame bewaaromgeving worden er <i>by default</i> geen originele manifestaties verwijderd. Bij wijzigingen wordt er een nieuwe manifestatie gemaakt, zodat het originele manifestatie behouden blijft.	EIS
2.4	De Oplossing registreert welke manifestatie het originele informatieobject is.	EIS
2.5	Een informatieobject kan verschillende manifestaties kennen. In de Oplossing wordt per informatieobject aangegeven welke manifestatie beschikbaar wordt gesteld.	EIS
2.6	In de duurzame bewaaromgeving kunnen bepaalde manifestaties vernietigd worden. Hierbij wordt het vier-ogen principe toegepast.	EIS
2.7	Informatieobjecten moeten in openbaarheid kunnen worden beperkt.	EIS
2.8	Het moet mogelijk zijn om de resultaten van een zoekactie (op metadata) te filteren en te sorteren.	EIS

3. Tijdelijke bewaaromgeving

De tijdelijke bewaaromgeving is specifiek voor het uitplaatsen van archieven. Deze omgeving kent dezelfde eisen en wensen als de duurzame bewaaromgeving die voor overbrengen wordt gebruikt. De eisen en wensen worden hier niet herhaald. Voor uitplaatsen geldt een aantal aanvullende eisen en wensen die hieronder staan uitgewerkt.

Nr.	Omschrijving	
3.1	De Oplossing biedt de mogelijkheid om een vernietigingstermijn aan informatieobjecten toe te kennen en te wijzigen. Dit kan per stuk of batchgewijs aan de hand van een selectie.	EIS
3.2	De Oplossing biedt de mogelijkheid om een overbrengingstermijn aan informatieobjecten toe te kennen en te wijzigen. Dit kan per stuk of batchgewijs. Tevens moet er overerving plaats kunnen vinden van de overbrengingstermijn.	EIS
3.3	Bij het naderen van de vernietigingstermijn krijgt de functioneel beheerder een attendering.	EIS
3.4	Bij het naderen van de overbrengingstermijn krijgt de functioneel beheerder een attendering.	EIS
3.5	De Oplossing moet op basis van de aanwezige metadata een selectie kunnen maken van te vernietigen en over te brengen informatieobjecten. Dit overzicht bevat minimaal deze informatie: metadata waarmee inzichtelijk wordt om welk archief het gaat, of het in aanmerking komt voor blijvende bewaring of vernietigd moet worden, wie de wettelijke eigenaar is, wat de vernietigings- of overbrengingstermijn is, in welke tenant de informatieobjecten opgeslagen staan en of er bijzonderheden zijn (bijvoorbeeld een hotspot).	EIS
3.6	De functioneel beheerder kan een heel uitgeplaatst archief of een onderdeel daarvan verplaatsen naar de digitale bewaaromgeving. Voordat dit daadwerkelijk kan plaatsvinden moet een extra waarschuwing worden gegeven.	EIS
3.7	Het moet mogelijk zijn om informatieobjecten die uitgeplaatst zijn in de tijdelijke bewaaromgeving met een export terug te leveren aan de eigenaar van het archief (bijvoorbeeld een particuliere instelling of overheidsorganisatie). Dit kan op verschillende niveaus zijn, denk aan dossier, document, manifestatie.	EIS
3.8	Het is mogelijk om informatieobjecten in onderlinge samenhang op een rechtmatige en onherroepelijke manier te vernietigen. Na de vernietiging mogen de brondocumenten en de bijbehorende metadata niet meer in de Oplossing voorkomen.	EIS
3.9	Het is mogelijk om geautomatiseerd (per zorgdrager) een vernietigingslijst te genereren, inclusief vernietigingsgrondslag waarbij de vernietigingslijst is aan te passen.	EIS
3.10	Het is mogelijk bestanden te vernietigen met toepassing van het vier-ogen principe.	EIS

4. Preservering		
Nr.	Omschrijving	
4.1	De Oplossing geeft op basis van de lijst met voorkeursformaten, opgesteld door het Nationaal Archief, of het PRONOM-register, opgesteld door The National Archives in het Verenigd Koninkrijk, automatisch een update aan de beheerder als een bestandstype verouderd dreigt te raken.	EIS
4.2	De functioneel beheerder kan actieve preserveringsacties uitvoeren in delen van de collectie in de bewaaromgeving. De Oplossing biedt de mogelijkheid om delen van de hele collectie te selecteren (bijvoorbeeld door een versie van een bestandsformaat te selecteren) en preserveringsacties uit te voeren.	EIS
4.3	De Oplossing kan een bulk aan informatieobjecten tegelijkertijd converteren naar een ander opslagformaat.	EIS
4.4	De Oplossing bewaart de nieuwe manifestatie (conversie) naast het originele object in de bewaaromgeving.	EIS
4.5	Alle preserveringsacties worden gedocumenteerd en bewaard. De beheerder kan te allen tijde nagaan wanneer een nieuwe manifestatie is gemaakt en hoe en door wie het uitgevoerd is.	EIS
4.6	De Oplossing biedt preserveringsfunctionaliteiten en borgt de authenticiteit, betrouwbaarheid, integriteit en raadpleegbaarheid van de informatieobjecten.	EIS
4.7	De Oplossing controleert automatisch de bestanden waarvan de checksum niet meer gelijk is aan de ge-ingeste versie en repareert deze automatisch.	EIS
4.8	De Opdrachtgever kan zelf in de Oplossing een overzicht maken van de bestanden waarvan de checksum is gerepareerd, indien niet meer gelijk met de ge-ingeste versie (Fixity check).	EIS

5. Administratieve ondersteuningsomgeving		
Nr.	Omschrijving	
5.1	De Oplossing kan informatieobjecten in een bulkactie naar een ander formaat converteren.	EIS
5.2	De Oplossing moet MDTO als standaard metadataschema gebruiken. De functioneel beheerder kan zelf meerdere metadataschema's toevoegen en toepassen. De functioneel beheerder kan bijvoorbeeld aangeven welke velden verplicht en optioneel zijn.	EIS
5.3	De functioneel beheerder kan zelf de ingest workflow inrichten. Functioneel beheerder kan bijvoorbeeld aangeven welke controle tools van toepassing zijn op de geleverde SIP.	EIS
5.4	De Oplossing houdt een logging bij wie welke handeling (openen, wijzigen, verwijderen, verplaatsen, etc) wanneer heeft gedaan.	EIS
5.5	De functioneel beheerder kan op ieder moment zelf rapportages/overzichten maken op basis van een bepaalde selectie aan gegevens.	EIS
5.6	De functioneel beheerder kan generieke rapportages op maat maken en aanbieden aan de medewerkers.	EIS
5.7	De Oplossing moet (ook per tenant) een rapportage kunnen maken van het aantal opgenomen informatieobjecten.	EIS
5.8	De Oplossing moet (ook per tenant) een rapportage kunnen maken van de gebruikte opslagcapaciteit.	EIS
5.9	De Oplossing moet (ook per tenant) een rapportage kunnen maken van aangetroffen risico's, zoals bijvoorbeeld virussen, fouten, verouderde bestandsformaten, etc.	EIS
5.10	Het is mogelijk metadata te wijzigen of toe te voegen op alle niveaus. Dit kan uitsluitend worden uitgevoerd door een beheerder. Van wijzigingen of toevoegingen wordt gelogd wanneer en door wie deze zijn uitgevoerd. De oude waarde van gewijzigde metadata blijft bewaard, maar wordt aangemerkt als "vervallen" of als inactief aangemerkt. Dit is mogelijk per document/selectie/bulk. Het is niet mogelijk metadata (velden-element) te verwijderen.	EIS
5.11	De Oplossing kan een <i>persistent identifier</i> (PID) aanmaken. Dit is een unieke, permanente digitale link als virtuele vindplaats van een digitaal object.	EIS
5.12	Indien een in de Oplossing op te nemen digitaal object al een persistent identifier heeft, kan deze worden opgenomen als virtuele vindplaats van het betreffende digitale object.	EIS
5.13	De functioneel beheerder moet zelfstandig in staat zijn wijzigingen aan te brengen in de generieke instellingen van de Oplossing. Denk hierbij aan autorisatiemodel, organisatiestructuur, definiëren en scheduleren van taken, etc.	EIS

6. Beschikbaar stellen		
Nr.	Omschrijving	
6.1	De Oplossing biedt de mogelijkheid om het beschikbaar informatieobject in een afwijkend en open formaat aan te bieden dan het origineel, omdat het zo sneller en geschikter is voor representatie of afdrukmogelijkheden. Ook het oorspronkelijke formaat moet te downloaden zijn. Onder een open formaat wordt bijvoorbeeld verstaan de open standaard volgens het Forum Standaardisatie.	EIS
6.2	Informatie-objecten die in openbaarheid zijn beperkt, kunnen niet worden geraadpleegd door ongeautoriseerde gebruikers.	EIS
6.3	De Oplossing moet in bulk DIP-objecten conform het OAIS-model kunnen maken en deze via een exportfunctionaliteit ter beschikking kunnen stellen.	EIS
6.4	Opdrachtgever kan zelf, zonder tussenkomst van de Opdrachtnemer, de metadata selecteren die geïndexeerd moeten worden, zodat ingericht kan worden op welke metadata een gebruiker van het e-depot kan zoeken, sorteren en filteren.	EIS
6.5	De gebruikersinterface ondersteunt viewers voor het bekijken van bestanden met voorkeursformaten, opgesteld door het Nationaal Archief.	EIS

7. Non-functionals bewaar		
Nr.	Omschrijving	
7.1	In lijn met de geldende architectuurprincipes van de Gemeente Den Haag wordt het e-depot als SaaS toepassing uitgevraagd. Dat betekent dat er geen installatie op servers bij de Gemeente Den Haag nodig is, en dat er wel sprake is van 'ontzorging' op het technische vlak: installatie, beschikbaarheid, beveiliging, beheer, performance en dergelijke vallen onder de verantwoordelijkheid van de inschrijver.	EIS
7.2	Opdrachtnemer is verantwoordelijk voor de correcte en rechtmatige naleving van de licentieverplichtingen voor het gebruik van software ook van derden. Het licentiemodel omtrent aantal gebruikers moet op basis van actuele behoefte flexibel en schaalbaar zijn.	EIS
7.3	De oplossing biedt naast een productieomgeving ook een volwaardige testomgeving, die qua hardware-specs wel mag afwijken, maar waarvan de softwareversie gelijk is aan de productie-omgeving, of één niveau voorloopt.	EIS
7.4	De gemeente Den Haag verwijst voor inkoop van een nieuwe ICT-toepassing naar twee lijsten: - De "Pas Toe of Leg Uit" lijst van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/verplicht) - De Aanbevolen Standaarden van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen) Opdrachtnemer wordt geacht zich te houden aan de standaarden uit de "Pas Toe of Leg Uit" lijst. De gemeente Den Haag streeft het naleven van de Aanbevolen Standaarden, die veelal de beoogd opvolger zijn van de Verplichte Standaarden, nadrukkelijk na. Daar waar een inschrijver in staat is om een Aanbevolen Standaard te leveren wordt gevraagd dat te vermelden. In het kader van de aankoop van een e-depot oplossing legt de gemeente de nadruk op het zoveel mogelijk volgen van de standaarden ten aanzien van koppelingen tussen applicaties en de beveiliging van deze koppelingen. De gemeente hecht hierbij sterk aan onderstaande Standaarden uit de "Pas Toe of Leg Uit" lijst: - OpenAPI Specification - REST-API Design Rules - oAUTH 2.0	EIS
7.5	De leverancier staat ervoor in dat met de Oplossing kan worden voldaan aan de AVG, UAVG en de "Baseline Informatiebeveiliging Overheid" (BIO https://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf) welke deel uitmaakt van de gemeentelijke ICT-kwaliteitsnormen.	EIS
7.6	Rechten worden in de applicatie toegekend aan rollen en niet op basis van personen (RBAC). Het moet mogelijk zijn nieuwe rollen met nieuwe combinaties van autorisaties te definiëren. https://nl.wikipedia.org/wiki/Role-based_access_control	EIS
7.7	De Oplossing biedt een federatieve koppeling, waarbij medewerkers van de gemeente gebruik maken van hun gemeentelijk account om in te loggen op de SaaS-omgeving.	EIS
7.8	De Oplossing dient, naast het voldoen aan de eisen behorende bij het gekozen 'normenstelsel', zoals ISO27001 of de BIO, te voorzien in logging en monitoring op individueel accountniveau.	EIS
7.9	Alle vormen van logging worden minimaal 2 jaar bewaard.	EIS
7.10	Transactielogs moeten kunnen worden geëxporteerd.	EIS
7.11	Logs moeten kunnen worden opgeschoond. Hierbij geldt het vier-ogen principe.	EIS
7.12	Gegevens moeten zowel in rust (in applicatie) als tijdens transport versleuteld zijn.	EIS
7.13	Opdrachtnemer meldt informatiebeveiligingsincidenten direct aan de daartoe aangewezen functionaris van de gemeente Den Haag.	EIS

7.14	De Gemeente Den Haag wordt onmiddellijk geïnformeerd bij dagvaardingen en onderzoeken van uw organisatie en/of andere klanten van uw organisatie door toezichthouders.	EIS
7.15	De Oplossing wordt jaarlijks getoetst op de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Opdrachtnemer dient daar jaarlijks medewerking aan te verlenen door vragen (vanuit de applicatie Recourse of per reguliere mail) te beantwoorden en daar waar nodig bewijs voor aan te leveren.	EIS
7.16	Uw organisatie kan door middel van een ICV of TPM jaarlijks aantonen dat de Oplossing voldoet aan de Baseline Informatiebeveiliging Overheid (BIO), waarbij aantoonbaar voldaan wordt aan de maatregelen zoals voorgeschreven door de IBDVNG, zie Maatregelen set BBN2+ (https://www.informatiebeveiligingsdienst.nl/product/maatregelenset-bbn2/ voor zover van toepassing op: "Dienstenleverancier /ICT-afdeling" (kolom H)).	EIS
7.17	De gemeente Den Haag organiseert jaarlijks een Hack event. Tijdens dit event krijgt een groot aantal ethische hackers de mogelijkheid om de door de gemeente Den Haag gebruikte applicaties en systemen welke bereikbaar zijn vanaf het internet te onderwerpen aan een test. De bevindingen worden gedeeld met de leveranciers die daarna de bevinding(en) kan oppakken. Medewerking van de leverancier (beschikbaar stellen test of productie omgeving en oplossen van de kwetsbaarheden tijdens het event) wordt zeer op prijs gesteld. Echter zal er geen vergoeding tegenover staan, maar kan dit in feite wel worden gezien als een meervoudige en goedkope pentest. Uiteraard zijn de deelnemende ethische hackers gebonden aan de voorwaarden van de gemeente Den Haag en hun leveranciers. Opdrachtnemer is deelnemer aan het jaarlijks evenement Hâck the Hague, stelt oplossing beschikbaar voor penetratie test tijdens evenement en zorgt voor opvolging van gevonden kwetsbaarheden tijdens het evenement.	EIS
7.18	Opdrachtnemer verleent medewerking aan het opnemen van de website(s) in een detectie portaal. Om eventuele kwetsbaarheden van een website in een zo vroeg mogelijk stadium te detecteren maakt de gemeente Den Haag gebruik van Cybersprint. Het door Cybersprint gebruikte Digital Risk Protection platform detecteert automatisch alle online kwetsbaarheden van bekende, 'verborgen', en valse online toegangspunten. Zij brengen het online aanvalsvlak in beeld en geven advies over mogelijke maatregelen. De door gemeente Den Haag gebruikte website zal, indien leverancier hiermee instemt, opgenomen worden in het Cybersprint portaal waarna er bij het ontdekken van kwetsbaarheden bevindingen doorgegeven zullen worden en na een redelijke termijn opgelost moeten worden.	EIS
7.19	De Oplossing beschikt over een context afhankelijke helpfunctionaliteit, geschreven in de Nederlandse of Engelse taal met ten minste: - instructies voor het gebruik van het portaal; - uitleg van de schermen binnen het portaal; - legenda van gebruikte iconen.	EIS
7.20	Exit van de informatie en metadata uit de oplossing in een standaardformaat moet mogelijk zijn conform de GIBIT voorwaarden.	EIS
7.21	Opdrachtnemer draagt bij beëindiging van het contract en/of in geval van veranderende (technische) omstandigheden alle (manifestaties van de) informatieobjecten, metadata en logfiles uit de Oplossing in onderlinge samenhang kosteloos over aan Opdrachtgever. Informatieobjecten, metadata en logfiles worden conform vigerende standaarden gestructureerd en binnen een redelijke termijn aangeleverd.	EIS
7.22	Na de beëindiging van de overeenkomst en de bevestiging van een succesvolle overdracht door Opdrachtgever worden alle data in de Oplossing vernietigd. Opdrachtnemer verstrekt een proces-verbaal van de vernietiging van de gegevens uit de Oplossing. Hierin wordt tenminste vermeld welke informatie is vernietigd, op welke wijze en de omvang van de informatie.	EIS

7.23	De aangeboden Oplossing (dat wil zeggen: alle met 'ja' beantwoorde eisen en wensen en uw antwoorden op de open vragen) is binnen zes maanden na ingang van de overeenkomst leverbaar zonder maatwerk en de levering van alle in de offerte opgenomen onderdelen zijn gedekt in het prijssjabloon. Als bepaalde functionaliteit specifiek voor deze aanbesteding wordt ontwikkeld, dan wordt deze in de eerstvolgende release opgenomen als standaardfunctionaliteit van de Oplossing.	EIS
7.24	U, en uw eventuele partners, dienen te voldoen aan de geldende Europese en Nederlandse wet- en regelgeving.	EIS
7.25	Data is te allen tijde binnen de Europese Economische Ruimte opgeslagen, dit geldt ook voor back-up en continuïteitskopieën.	EIS
7.26	Opdrachtnemer heeft toegang tot (bij voorkeur online) documentatie en trainingsmateriaal.	EIS

8. Architectuur en techniek		
Nr.	Omschrijving	
8.1	De Oplossing dient als een volledige cloudoplossing via het https protocol te worden aangeboden.	EIS
8.2	Beschikbaarheid is gedefinieerd als 'eigenschappen van het geheel van ICT-diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of de dienst (en daarmee informatie) beschikbaar is voor de geautoriseerde gebruiker, op de momenten dat het beschikbaar moet zijn'. Beschikbaarheid wordt gemeten aan de hand van de Mean Time Between Failures (MTBF). Dit is de gemiddelde tijd tussen het herstel van het ene incident en het optreden van het volgende incident. De Oplossing is 24 uur per dag, 7 dagen per week beschikbaar en heeft een beschikbaarheid van 99,9 %, behoudens gepland onderhoud. De gemiddelde tijd tussen storingen (MTBF) bedraagt minimaal 200 dagen.	EIS
8.3	Grote bulkacties met betrekking tot het beheer van informatieobjecten hebben geen invloed op de performance voor de andere functies	EIS
8.4	Het e-depot is een Oplossing waarin dagelijks grote hoeveelheden informatieobjecten worden geïmporteerd, bewerkt en uitgeleverd. Dit vereist een omgeving welke is ingericht op performance. Met performance bedoelen we in dit kader niet alleen de respons van de interface na zoekacties, maar alle routines en processen die uitgevoerd worden. Ook imports van grote en complexe bestanden, zoals audio, video en databases, moeten vlot verlopen, bulkacties op records moeten snel uitgevoerd kunnen worden, en meerdere medewerkers moeten tegelijkertijd in het systeem kunnen werken. Omdat performance een veelomvattend en niet eenvoudig te kwalificeren begrip is, is het lastig om dit te vertalen naar een overzicht met louter eisen en streefgetallen.	EIS
8.5	De Oplossing moet kunnen omgaan met diakrieten.	EIS
8.6	De Oplossing is webgebaseerd en kan benaderd en volledig gebruikt worden via de actuele alsmede in ieder geval de 2 meest recente versies van alle courante webbrowsers, zoals Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Apple Safari en Mozilla Firefox zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX) en extensies.	EIS
8.7	De Oplossing kan overweg met Federatieve Authenticatie, waarbij de leverancier optreedt als Resource Provider en de gemeente als Identity Provider.	EIS
8.8	De Oplossing maakt gebruik van pagina's die responsive zijn naar gelang de grootte van het beeldscherm (het apparaat) van de gebruiker. Apparaten van het formaat smartphone kunnen hiervan uitgesloten worden.	EIS
8.9	De Oplossing gebruikt geen shared servers.	EIS
8.10	De Oplossing omvat een toereikende automatisch back-up en beschikt tevens over een recovery proces.	EIS
8.11	Het back-up proces is de verantwoordelijkheid van Opdrachtnemer en voorziet in opslag van de back-up op een andere geografische locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	EIS
8.12	In geval van een gebeurtenis, waarbij er sprake is van recovery (bijvoorbeeld een ramp, calamiteit of incident) dient de Oplossing binnen 48 uur weer volledig beschikbaar te zijn en bedraagt het verlies van informatie maximaal 1 werkdag.	EIS
8.13	Indien er informatie moet worden uitgewisseld tussen twee SAAS-applicaties, ondergebracht bij twee verschillende leveranciers, verloopt dit via de API Gateway van de gemeente Den Haag. In het geval dat de twee applicaties bij een leverancier zijn ondergebracht, mag de communicatie direct plaats vinden, mits de leverancier aantoonbaar aan de Haagse security en privacy voorwaarden voldoet (o.a. via leveringsovereenkomst). Koppelingen tussen SaaS oplossingen en een bij de gemeente gehost systeem verlopen eveneens in principe over de gemeentelijke API Gateway. Uitzonderingen op deze regel worden alleen toegestaan vanwege technische beperkingen, en indien de alternatieve beveiliging van het transport toereikend is.	EIS
8.14	De componenten van uw netwerk en applicatie dienen 'gehardened' te zijn. Denk aan besturingssystemen kritieke componenten, web servers, netwerkapparatuur, databases. Inschrijver dient dit op eerste verzoek aan te tonen.	EIS
8.15	De vernietiging van opslag aan einde van het contract vindt op zodanige wijze plaats dat de gegevens met geen enkele forensische procedure kunnen worden hersteld.	EIS