Bijlage 6 – Programma van Eisen

Eisen ALGEMEEN	
Eis AL1	De ICT-oplossing is direct leverbaar en beschikbaar als een door Opdrachtnemer aangeboden standaard ICT-oplossing zonder maatwerk. De levering van alle onderdelen zoals beschreven in dit Programma van Eisen, de opgeleverde use cases en de beantwoorde Open Vragen zijn gedekt in het prijzenblad.
Eis AL2	De ICT-oplossing voldoet aan alle huidige en toekomstige relevante wetgeving die van toepassing is voor Opdrachtgever bij het uitvoeren van haar taken (zoals onder andere AVG, Wet Modernisering Elektronisch Bestuurlijk Verkeer en de Wet Digitale Overheid en eventuele wetsopvolgers etc)
Eis AL3	Opdrachtnemer garandeert dat de ICT-oplossing gedurende de hele looptijd van de overeenkomst inclusief verlengingen voor gebruik beschikbaar is en onderhouden en ondersteund wordt.
Eis AL4	Opdrachtnemer houdt de aangeboden ICT-oplossing en de koppelingen/*webservices* actueel ten aanzien van wijzigingen in wet- en regelgeving, en standaarden zoals gespecificeerd door het forum standaardisatie op de "pas toe of leg uit lijst". Deze wijzigingen worden beschouwd als onderhoud en leiden niet tot separate kosten.
Eis AL5	De ICT-oplossing en de opdrachtnemer voldoen aan de • Gemeentelijke inkoopvoorwaarden bij IT (onderdeel GIBIT, bijlage 2) • Gemeentelijke ICT Kwaliteitsnormen (onderdeel GIBIT, bijlage 2) • de Concern Informatie Architectuur (CIA, bijlage 10) • de Technische Architectuur (TA, bijlage 9) • Beleid Informatieveiligheid (bijlage 11) • Gebruik van TLS en HTTP Respons Headers (Bijlage 12).
Eis AL6	De kosten van nieuwe releases, updates, patches, fixes (et cetera) en installatie daarvan zijn opgenomen in de aanbieding. Hierbij inbegrepen zijn ook wijzigingen naar aanleiding van wetswijzigingen. De installatie op en het gebruik van een Acceptatieomgeving zijn hierbij ook inbegrepen.
Eis AL7	In het geval van het plotseling wegvallen van of een onvoorziene beëindiging van de dienstverlening door Opdrachtnemer of onderopdrachtnemer (faillissement, overname of calamiteit), wordt de continuïteit van de Oplossing en dienstverlening gegarandeerd door een derde partij (zoals escrow, data-escrow, of een andere vorm van garantstellig zoals een beheerstichting of een tripartite overeenkomst).
Eis AL8	Opdrachtnemer garandeert te allen tijde expliciet compliance van eventuele onderaannemers, hostingpartijen en gelieerde partners aan de overeengekomen afspraken met Opdrachtgever en is daarbij zelf volledig verantwoordelijk.
Eis AL9	De geoffreerde prijzen van de aangeboden Oplossing zijn inclusief alle benodigde licenties, certificeringen en verklaringen van derden, zoals TPM en assurance-verklaringen. Het is niet toegestaan uit te gaan van reeds bij Opdrachtgever aanwezige licenties, tenzij expliciet aangegeven bij de eis.
Eis AL10	Opdrachtgever blijft altijd eigenaar van de transactiedata.
Eis AL11	De aanbieder stelt alle gegevens beschikbaar met betrekking tot alle gebruikte algoritmes van de categorie "A: Hoog risico volgens AI-Act" en "B: Impact op betrokkenen" (Zie Handreiking Algoritmeregister), zodat Opdrachtgever deze kan publiceren op Het Algoritmeregister van de Nederlandse overheid.

Eis AL12	Het is Opdrachtnemer niet toegestaan ontwikkel- en ontwikkeltestwerkzaamheden uit te voeren op de omgevingen die beschikbaar zijn gesteld aan Opdrachtgever.
Eis AL13	Alle handelingen en acties (inclusief raadplegingen) uitgevoerd door gebruikers van de Oplossing, beheerders en door de Oplossing zelf worden gelogd. Deze logs mogen niet aanpasbaar zijn. Er wordt per handeling/actie minstens het volgende vastgelegd: wie, wat, waar, wanneer en, indien het om persoonsgegevens gaat, waarom. Opdrachtgever kan deze logging altijd raadplegen en exporteren.
Eis AL14	Opdrachtnemer levert vóór definitieve gunning de SBOM (Software Bill of Materials) van de oplossing en houdt Opdrachtgever gedurende de looptijd van het contract op de hoogte van wijzigingen hierop.

Eisen TECHNIEK	
Eis TE1	Webapplicaties maken gebruik van een koppeling met Single Sign On (SSO) voor medewerkers van Opdrachtgever met Azure AD/Entra ID als de Identity Provider. Opdrachtnemer mag hierbij gebruik maken van SAML 2.0 of Open-id connect (OAuth 2.0). De set aan gegevens en attributen bestaat uit: • User principal name • Email • First name • Last name De SSO-koppeling wordt alleen gebruikt voor authenticatie. Autorisatie dient plaats te vinden binnen de gekoppelde applicatie. Voor de toegang tot applicaties wordt gebruik gemaakt van Conditional Access. Voor andere gebruikers dan medewerkers van Opdrachtgever is minimaal 2-factor verplicht als authenticatie middels een TOTP-code via een authenticator app.

Eisen SAAS	
Eis SA1	De oplossing ontwikkelt mee met de levenscyclus van de besturingssystemen, zoals de Windows-omgeving en van de internet-browsers.
Eis SA2	De oplossing werkt volledig zonder aanvullende client installaties.
Eis SA3	De opdrachtnemer verzorgt het technisch beheer zoals het maken van back-ups, het onderhoud en de installatie van nieuwe versies en updates, beveiliging tegen ongeautoriseerde toegang etc.
Eis SA4	Onderhoud wordt altijd vooraf schriftelijk gemeld aan Opdrachtgever met omschrijving van de werkzaamheden die verricht gaan worden. Dit geldt voor iedere omgeving die beschikbaar is gesteld aan Opdrachtgever, ook in de implementatiefase. Na onderhoud wordt altijd schriftelijk het verloop van de werkzaamheden gemeld aan Opdrachtgever. Onderhoud op de productieomgeving wordt uitgevoerd op momenten dat gebruikers hier minimaal last van ondervinden; tussen 20.00 en 07.00 uur. Andere momenten alleen na toestemming van Opdrachtgever.
Eis SA5	Bij verwerking van bijzondere en/of gevoelige persoonsgegevens levert de SaaS-Leverancier jaarlijks een SOC II Type II verklaring en/of een TPM op basis van een andere erkende norm op het gebied van informatieveiligheid.

Eis SA6	Bij verwerking van een financieel proces dat, bijvoorbeeld voor de jaarrekening, van materieel belang kan zijn, levert de SaaS-leverancier jaarlijks een ISAE 3402 Type II verklaring.
Eisen KOPPELINGEN	
Eis KO1	Een koppeling waarbij minimaal een van de applicaties on-premise staat loopt altijd via de integratie laag van Gemeente ’s-Hertogenbosch.
Eis KO2	Koppelingen tussen twee systemen, die niet binnen het gemeentelijk netwerk staan, lopen bij voorkeur via de gemeentelijke integratielaag. Indien dat niet mogelijk is en er sprake is van enige vorm van aansprakelijkheid en/of verantwoordelijkheid bij Opdrachtgever moeten deze koppelingen aan de volgende eisen voldoen: A. De opdrachtgever heeft te allen tijde, zonder tussenkomst van de opdrachtnemer, zicht op: • de beschikbaarheid van de koppeling; • de performance van de koppeling; • functionele uitval; • technische uitval; • de variabele kosten (indien van toepassing) die gepaard gaan met het gebruik van de koppeling (hoogte en door wie gemaakt). B. De opdrachtnemer is bij een storing verantwoordelijk voor de foutanalyse met betrekking tot de koppeling en beschikt over de middelen om het onderzoek uit te voeren. C. Indien er sprake is van uitwisseling van vertrouwelijke gegevens wordt in de audittrail- en/of logging minimaal vastgelegd: • wanneer de koppeling is gebruikt; • wie de transactie heeft geïnitieerd (medewerker); • waarom de transactie is geïnitieerd (doelbinding); • welke gegevens (soort en inhoud) zijn uitgewisseld. De audittrail/logging is alleen door geautoriseerde personen opvraagbaar en is direct beschikbaar of wordt op verzoek per omgaande geleverd. D. De opdrachtnemer is verplicht een datalek per omgaande te melden aan de opdrachtgever. E. De opdrachtnemer moet de koppeling op bovenstaande eisen (A t/m D) laten toetsen door een door de opdrachtgever aan te wijzen partij. De opdrachtgever accepteert ook een TPM-verklaring, waarin de koppeling aantoonbaar aan bovenstaande eisen (A t/m D) voldoet.
Eis KO3	Gegevensuitwisseling tussen ICT-oplossingen waarvoor geen standaarden beschikbaar zijn, koppelen op basis van REST API's.
Eis KO4	De werking van het koppelvlak is volledig gedocumenteerd en ter beschikking gesteld, in het geval REST door middel van Open API of RAML.

Eisen FUNCTIONEEL	
Eis FU1	De gebruikersinterface moet alle voorkomende diakrieten uit tekenset UTF-8 correct kunnen tonen en afdrukken. Ook op alle koppelvlakken wordt het gebruik van diakrieten ondersteund. Bij (iedere) zoekfunctie in de ICT-oplossing moeten de diakrieten en hoofdletters worden genegeerd. Daarmee wordt bedoeld dat bij het zoeken met of zonder diakrieten en/of hoofdletters, de gegevens worden gevonden en getoond met de juiste diakrieten en hoofdletters (dus de fictieve naam “LàCreté” wordt gevonden bij zoeken met op zowel “LàCreté” als “LaCrete” als “lacrete”.
Eis FU2	De helpfunctie dient gevuld te zijn bij levering en wordt door Opdrachtnemer onderhouden bij updates.

Eis FU3	De schermafhandeling moet ondersteund worden met zelfverklarende meldingen. Dit betekent dat de gebruiker moet kunnen lezen en zonder het raadplegen van documentatie moet kunnen begrijpen welke actie wordt vereist of wat fout is gegaan.

Eisen AUTORISATIE, PRIVACY & SECURITY	
Eis AP1	Autorisatie vindt plaats binnen de ICT-oplossing. Bij het definiëren van autorisaties wordt onderscheid gemaakt in creatie-, raadpleeg-, mutatie- en verwijderrechten.
Eis AP2	De ICT-oplossing biedt de mogelijkheid om rollen te definiëren die aan gebruikers worden toegekend. Via deze rollen worden de autorisaties op zaken/processen bepaald. Autorisaties zijn mogelijk op het niveau van organisatorische eenheid, rol en medewerker.
Eis AP3	De ICT-oplossing biedt de mogelijkheid om vertrouwelijkheidscategorieën in te richten. Toegang tot functies en schermen is gekoppeld aan een rol. Gebruikers worden aan één of meerdere rollen gekoppeld. Op rol-niveau kan per vertrouwelijkheidscategorie de standaard autorisaties ingericht worden voor zaken/processen.
Eis AP4	Autorisaties kunnen door een beheerinterface eenvoudig worden geconfigureerd. Het hele rollen- en rechtenmodel binnen de Oplossing kan op één plek geconfigureerd worden door Opdrachtgever. In de Oplossing is het mogelijk om configuraties rollen en rechten te stapelen, overerven, kopiëren en delegeren.
Eis AP5	Opdrachtnemer geeft inzicht in opgetreden beveiligingsincidenten. Beveiligingsincidenten zijn incidenten die inbreuk maken op beveiligingseisen betreffende de beschikbaarheid, integriteit en exclusiviteit. De beveiligingsincidenten worden direct gemeld bij de daarvoor aangewezen contactpersoon van Opdrachtgever
Eis AP6	De BIO is het normenkader dat als uitgangspunt dient voor het Beleid Informatieveiligheid en het Plan Informatieveiligheid van Gemeente ’s-Hertogenbosch. De Oplossing voldoet aan de Cyberbeveiligingswet (Cbw) en de BIO2.

Eisen BEHEER	
Eis BH1	Opdrachtnemer sluit een Service Level Agreement af met Opdrachtgever met daarin de eisen zoals omschreven in de GIBIT (bijgesloten) en minimaal: • rollen en verantwoordelijkheden; • overlegstructuur en rapportages; • het aantal releases per jaar; • werkwijze bij een release (communicatie, testen, documentatie); • invloed van Opdrachtgever aan de inhoud van de releases; • de recoveryprocedure; • de escalatieprocedure • de wijze van rapporteren over bovengenoemde onderwerpen; • service windows; • responsetijden; • Uptime; • RPO (recovery point objective): hoeveel uren werk mag verloren gaan; • RTO (recovery time objective): hoelang mag het systeem uit de lucht zijn;

	• bereikbaarheid van de helpdesk; • de maximale tijdsduur van reageren en oplossen van de verschillende diensten op het gebied van onderhoud, problemen en incidenten, per niveau; • de consequenties bij het niet of niet tijdig leveren van de verschillende diensten op het gebied van onderhoud, problemen en incidenten, per niveau; • de minimale periode om wijzigingen aan te kondigen die impact hebben op het gebruik van data of koppelvlakken.
Eis BH2	Opdrachtnemer heeft een helpdesk die op werkdagen te bereiken is tussen 8.30 en 17.00 uur. De helpdesk is het centrale punt voor het melden van problemen en incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan. De helpdesk is onderdeel van de overeenkomst, waarvoor geen extra kosten in rekening gebracht mogen worden.
Eis BH3	Voor de ICT-oplossing wordt een acceptabele, goed werkbare performance voor circa 10 gelijktijdige gebruikers gegarandeerd. 'Acceptabel' vertaalt zich onder meer naar, maar niet uitputtend, de volgende responstijden: • Opstarten van de applicatie binnen 10 seconde (in 99% van de gevallen). • Inloggen in de applicatie binnen 2 seconde (in 99% van de gevallen). • Toetsaanslagen worden binnen 0,1 seconde op het scherm getoond (in 99% van de gevallen). • Binnen 0,5 seconde kan worden gewisseld van Gegevensveldwisseling, zowel met muis als met toetsenbord (in 99% van de gevallen). • Bij een schermwisseling kan de eindgebruiker binnen 2 seconden zijn werk doen in het nieuwe scherm (in 99% van de gevallen). • Preview van bestanden worden binnen 2 seconde getoond (in 99% van de gevallen). • Openen van een bestand is binnen 3 seconden gereed (in 90% van de gevallen). • Eenvoudige query's leveren binnen 5 seconden resultaat (in 90% van de gevallen). Daar waar responstijden niet worden gehaald geeft de interface van de Oplossing aan dat deze bezig is met het uitvoeren van de opdracht.
Eis BH4	Voor functionele aanpassingen met en wettelijke grondslag waarbij nieuwe releases of patches worden geleverd, geldt dat deze minimaal 6 weken voor de wettelijke ingangsdatum worden opgeleverd op de acceptatie-omgeving met een schriftelijke uitleg.
Eis BH5	De Oplossing beschikt over functionaliteit om beheeractiviteiten uit te voeren door Opdrachtgever zonder tussenkomst van Opdrachtnemer zoals het (extra) kunnen opstarten en monitoren van het berichtenverkeer en batches.
Eis BH6	Een beheerder van Opdrachtgever ontvangt een notificatie wanneer er technische problemen optreden in de oplossing of een koppeling.

Eisen IMPLEMENTATIE	
Eis IP1	Opdrachtnemer zorgt voor een volledige implementatie op de acceptatie- en productieomgeving van de aangeboden ICT-oplossing. De aangeboden ICT-oplossing is beschikbaar en bruikbaar in productie per 1-4-2027
Eis IP2	Het implementatietraject is gericht op een implementatie die start binnen 4 weken na definitieve gunning;

Eisen EXIT FASE	
Eis XF1	Na het einde van de overeenkomst krijgt Opdrachtgever aansluitend minimaal 3 maanden tijd om met behulp van de hier aangeboden ICT-oplossing de boekhouding administratie en fiscaal af te sluiten. Licentiekosten en onderhoud voor deze periode zijn inbegrepen in de aangeboden prijs.
Eis XF2	Opdrachtnemer stelt na verzoek van Opdrachtgever binnen twee weken alle data inclusief documenten beschikbaar voor verder eigen gebruik, al dan niet in een nieuwe ICT-oplossing. Opdrachtnemer stelt hier geen verdere eisen aan en brengt geen extra kosten (behoudens de genoemde kosten in deze aanbesteding) in rekening voor het beschikbaar stellen van bovengenoemde data aan Opdrachtgever.
Eis XF3	Opdrachtnemer maakt een exitplan dat voldoet aan de Europese Dataverordening (Data Act) en die beschrijft hoe de exit-fase uitgevoerd gaat worden. Goedkeuring van exitplan door Opdrachtgever is voorwaardelijk voor de acceptatie.

Eisen Ingest	
Eis ING1	Bij opname vindt er een controle plaats op bitintegriteit door middel van checksums. Deze controle op de integriteit van gegevens (data) vindt plaats om de juistheid, betrouwbaarheid en authenticiteit van de informatieobjecten binnen de nieuwe omgeving te garanderen. Een fout in de bitintegriteit van een informatieobject wordt gesignaleerd en gerapporteerd. Het resultaat van een checksum wordt als metagegevens toegevoegd aan de ontvangen informatieobjecten.
Eis ING2	Bij opname vindt er een controle plaats op bestandsformaten. Deze functie dient de opslagformaten van de ontvangen objecten vast te stellen.
Eis ING3	Bij opname vindt er een controle plaats op belemmeringen voor duurzame toegankelijkheid. De ontvangen informatieobjecten en -packages dienen gecontroleerd te worden op eigenschappen die duurzaam toegankelijk bewaren in de weg kunnen staan of die speciale preserveringsmaatregelen vergen. In deze controle worden tenminste virussen, corrupte bestanden, versleutelde bestanden (encrypties) meegenomen.
Eis ING4	Het is mogelijk informatieobjecten aan bestaande dossiers toe te voegen of om nieuwe dossiers te vormen.
Eis ING5	Bij opname vindt er een controle plaats om na te gaan of de ontvangen informatieobjecten versies zijn van reeds aanwezige informatieobjecten. Hierbij zou vastgesteld moeten worden of: • het object hoort bij een of meer andere bestaande en in de opslag al aanwezige versies van hetzelfde object; • het object is een extra manifestatie van bestaande in de opslag al aanwezige manifestaties van eenzelfde informatieobject.
Eis ING6	De oplossing bevestigt een geslaagde ingest of geeft een foutrapportage.
Eis ING7	Originele manifestaties van informatieobjecten behouden hun authenticiteit en wijzigen nooit.
Eis ING8	Er wordt geregistreerd welke manifestatie het originele informatieobject is.

Eisen Gegevensbeheer

Eis GB1	Het is na opname mogelijk metagegevens toe te voegen en te bewerken, zowel van afzonderlijke informatieobjecten als in bulk (categorie opname). • Metagegevens moeten op alle niveaus toegevoegd of gewijzigd kunnen worden, zowel voor losse informatieobjecten, een selectie van informatieobjecten als in bulk. • Automatische overerving van metagegevens naar lagere aggregatieniveaus is mogelijk
Eis GB2	De informatieobjecten moeten in openbaarheid kunnen worden beperkt.
Eis GB3	Delen van het archief moeten met een export in bulk terug geleverd kunnen worden.
Eis GB4	Informatieobjecten kunnen in onderlinge samenhang op een rechtmatige en onherroepelijke manier vernietigd worden met toepassing van het vier-ogen principe.
Eis GB5	Metadatering moet conform het MDTO plaats kunnen vinden. Daarnaast kunnen geautoriseerde medewerkers zelf meerdere metagegevensschema's toevoegen en aanpassen.

Eisen Preservering	
Eis PR1	Opslag in voorkeurs- en acceptabele bestandsformaten van het nationaal Archief is mogelijk.
Eis PR2	Informatieobjecten kunnen in bulk geconverteerd worden naar een ander bestandsformaat.
Eis PR3	Na conversie worden de nieuwe manifestaties naast de originele informatieobjecten bewaard.
Eis PR4	De oplossing controleert automatisch de bestanden waarvan de checksum niet meer gelijk is aan de ge-ingeste versie en repareert deze automatisch. Bij een geconstateerde fout dient een notificatie gestuurd te worden, of start eventueel direct een herstelprocedure met gebruikmaking van onder andere mirror-, back-up-, en restorefuncties van de voorziening.
Eis PR5	Alle preserveringsacties worden gedocumenteerd en bewaard

Eisen Ontsluiten en beschikbaar stellen	
Eis OBS1	De gebruikersinterface ondersteunt viewers voor het bekijken van bestanden met voorkeurs- en acceptabele bestandsformaten van het Nationaal Archief.
Eis OBS2	Er kan eenvoudig en gebruiksvriendelijk full tekst gezocht worden.
Eis OBS3	Resultaten van een zoekactie kunnen op metagegevens gezocht, gefilterd en gesorteerd worden.
Eis OBS4	Het is mogelijk booleaans en met jokertekens te zoeken.
Eis OBS5	De informatieobjecten zijn in hun opgeslagen bestandsformaat te raadplegen en downloaden. Reproducties van informatieobjecten kunnen zowel los als in bulk via een exportfunctionaliteit ter beschikking gesteld kunnen worden