Bijlage D Programma van Eisen

SaaS 'Beheersysteem openbare ruimte en objectenregistratie en voor de gemeenten Heemstede en Bloemendaal

*Alle wijzigingen n. a. v. de Nota van Inlichtingen d.d. 08.09.2023 zijn in het rood verwerkt *
*Alle wijzigingen n. a. v. de Nota van Inlichtingen d.d. 20.09.2023 zijn in het blauw verwerkt *

Algemeen

Nr.	Eis
A1	Leverancier levert een Systeem die door de Organisatie als Objectenregistratie en Basis beheersysteem gebruikt kan worden.
A2	Het Systeem is geschikt voor het registeren van objectgegevens conform IMBOR en voor het **beheren** van assets van de volgende vakdisciplines: - Afval - Begraafplaatsen - **Bomen** - **Borden** - **Civiele constructies** - Ecologie - Evenementen - Gemalen - **Groen** - Grondwater - Havens - Kabels en leidingen - Kunst - Meubilair - Parkeren - **Riolering** - **Spelen** - Sport - Technische installaties - **Verlichting** - **Water** - **Wegen** - Wegmarkeringen Vetgedrukt betekent dat in het Systeem ook dynamische gegevens conform landelijke methodieken van toepassing zijn.
A3	Leverancier beschikt over een informatiebeveiligingssysteem dat door een officiële certificeringsinstantie is gecertificeerd op basis van NEN-ISO /IEC 27001 dan wel onvoorwaardelijk bereid te zijn bij gunning een dergelijke certificering binnen 6 maanden na ondertekening van de overeenkomst succesvol af te ronden. Het certificaat dienen gedurende de gehele uitvoeringsperiode geldig te zijn. De ontwikkeling, beheer en onderhoud van de oplossing moeten binnen de scope van de certificering vallen. De certificering is voorzien van een VVT (verklaring van toepasselijkheid). Indien de Leverancier niet over de geldige ISO 27001 certificaat beschikt of binnen 6 maanden na ondertekening van de overeenkomst de ISO 27001 certificering succesvol kan afronden, toont de Leverancier het voldoen aan de BIO-vereisten

	(uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld) door middel van een door extern erkende EDP-auditor afgegeven (assurance-)verklaring. Leverancier is bereid onvoorwaardelijk bij gunning een dergelijke verklaring binnen 6 maanden na ondertekening van de overeenkomst over te leggen.
A4	Het Systeem functioneert voor wat betreft aspecten van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving (ten minste AVG en BIO),en andere van toepassing zijnde wetgeving. De BIO voldoet uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld. Wij verwijzen in dit kader expliciet naar die BIO-eisen waarbij in de kolom "Verantwoordelijke" (onder meer) de "Dienstenleverancier" wordt benoemd.
A5	Leverancier conformeert zich gedurende de looptijd van de overeenkomst, volledig aan alle voor de opdracht relevante standaarden die door het Forum Standaardisatie op de lijst ‘veelgebruikte open standaarden’ of ‘open standaarden voor pas toe of leg uit’ zijn geplaatst. Specifiek gaat het hierbij om de volgende standaarden: Digikoppeling; Digitoegankelijkheid; Geo-standaarden; GWSW; HTTPS; PDF; ODF; IPv6 en IPv4; OpenAPI Specification; REST-API Design Rules; SAML; StUF; TLS; DNSSEC; SPF; DMARC; DKIM; STARTTLS; DANE; security.txt.

ICT

Nr.	**Eis**
Algemeen	
I1	Het Systeem werkt als een volledige SaaS-applicatie. De volledig SaaS-applicatie volgens gemeentelijke definitie/vereist geen verdere infrastructuur aan de kant van de gemeente. • De SaaS-applicatie wordt volledig ontsloten via internet. D.w.z. niet via een besloten of privé netwerk, zoals Gemnet, Diginetwerk, VPN, etc. • De SaaS-applicatie is gebaseerd op en volledig te gebruiken via een webbrowser: Google Chrome, Mozilla Firefox, Safari, Microsoft Edge. Op mobiele apparaten zijn apps uit de reguliere App-stores toegestaan. Maatwerksoftware is niet toegestaan, dit geldt ook voor add-ons, plug-ins, etc. • Een oplossing die (gedeeltelijk) afhankelijk is van onze on-premise architectuur, is niet toegestaan. De SaaS-applicatie moet volledig onafhankelijk van de gemeentelijke ICT-infrastructuur functioneren. • Koppelingen tussen de SaaS-applicatie en andere applicaties van de gemeente worden rechtstreeks gelegd tussen de aanbieder van de SaaS-applicatie en de leverancier van de andere applicatie. Het netwerk van de gemeente mag niet als ‘tussenstation’ worden gebruikt. • Identificatie en Authenticatie verloopt bij voorkeur via Microsoft Azure AD. Als dit technisch echt niet mogelijk is, wordt Multifactor Authenticatie toegepast. Andere varianten zijn niet toegestaan. • Bloemendaal en Heemstede werken plaats- en tijdonafhankelijk. De SaaS-applicatie ondersteunt dit volledig. D.w.z. dat de applicatie ten alle tijden volledig werkend te benaderen is van buiten het gemeentehuis en/of het gemeente-netwerk. • Het SaaS-applicatie verkeer dient altijd gebaseerd te zijn op HTTPS via de standaard poort 443. • De SaaS-applicatie is een cloudoplossing waarbij technisch beheer door de leverancier (Leverancier) uitgevoerd wordt. De Leverancier garandeert gedurende de contractperiode de beschikbaarheid en het onderhoud van de

	te leveren Software (Correctief Onderhoud, Preventief Onderhoud, Innovatief Onderhoud en Gebruikersondersteuning). • Presentatie van omgeving aan beheerders en eindgebruikers (inclusief functioneel beheerders) door gebruik te maken van zogenaamde remote desktop, virtual desktop infrastructuur (VDI) en/of server based computing (SBC) technologieën (voorbeelden hiervan zijn o.a. VMware Horizon, Citrix Xenapp en Microsoft remote desktop services) is toegestaan.
I2	Het Systeem biedt een procedure voor het verwijderen van data/informatie (Niet zijnde Exit strategie).
API en gegevensuitwisseling	
I3	De API is getest en beveiligd tegen de dreigingen van de OWASP-API-security top 10 https://apisecurity.io/encyclopedia/content/owasp/owasp-api-security-top-10-cheat-sheet.htm
I4	Het Systeem kan koppelen (gegevens uitwisselen) met andere applicaties door middels moderne API's en via de API-Gateway (2Secure/Layer7).
I5	Dataportabiliteit moet mogelijk zijn voor de inhoud (waarden) van de data in de ICT Prestatie alsmede de bijbehorende metadata bestaande uit ten minste de beschrijving van de betekenis van entiteiten, relaties, attributen en waardenbereik.
I6	Het technische formaat voor dataportabiliteit is een open formaat, en sluit bij voorkeur aan bij de XML- of JSON-standaarden. Indien aan het bovenstaande niet voldaan kan worden en ander gangbaar technisch dataformaat wordt gebruikt, dient de meta-informatie afzonderlijk gedocumenteerd te worden.
I7	Leverancier geeft bij implementatie de specificaties voor dataportabiliteit. Deze specificaties voor dataportabiliteit bevatten voor de export én import van data tenminste: a. de beschrijving van betekenis van de data van entiteit, attributen en waardenbereik; b. de beschrijving van betekenis en relaties (kardinaliteit) tussen gegevens; c. het formaat waarin data kan worden geëxporteerd/geïmporteerd; d. welke gegevens en metadata wel en niet worden meegenomen en het formaat waarin dat plaatsvindt; e. de beschrijving van de import en exportfunctionaliteit die het softwareproduct ondersteunt; f. opgave van de technische formaten die voor dataportabiliteit gebruikt worden.
Autorisatie	
I8	Het Systeem ondersteunt toegang tot gegevens door middel van een autorisatiesysteem op basis van rollen en rechten.
I9	Het Systeem ondersteunt veilig inloggen door SSO door middel van OAuth en SAML en federatie met Azure AD.
I10	Het Systeem heeft een mogelijkheid om vastgelegde autorisaties op alle niveaus inzichtelijk te maken per persoon, per gebruikersgroep en rol. Hiervoor is het toegepaste autorisatieschema te exporteren naar een bestand, dat leesbaar en interpreteerbaar is voor derden (denk aan toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).
Logging	
I13	Het Systeem biedt zodanige functionaliteit m.b.t. auditing/logging dat alle inlog- en muteeracties- door middel van logging een historie wordt vastgelegd (van welke handelingen en pogingen daartoe, wanneer en door wie zijn uitgevoerd). Deze auditing/logging dient zonder tussenkomst van de leverancier door functioneel en daartoe geautoriseerde gebruikers bekeken te kunnen worden.
I14	Het Systeem dient een audittrail van alle inlog- en muteeracties vast te leggen.
I15	Het Systeem dient alle inlog- en muteeracties vast te leggen in een logging. Deze logging blijft een half jaar bewaard.
I16	Het Systeem dient de integriteit van de logging te waarborgen.

Informatiebeveiliging	
I15a	Het Systeem ondersteunt TLS 1.2 met betrekking tot het beveiligen van de webapplicatie in de browser (het "slotje")
I16a	Het Systeem ondersteunt TLS 1.3 met betrekking tot de API-koppelingen voor gegevensuitwisselingen.
I17	Leverancier past de hardening richtlijnen van het NIST toe.
I18	Alle verplichte relevante beveiligingsstandaarden van het forum standaardisatie zijn toegepast. Leverancier garandeert dat dit zo blijft bij wijzigingen van deze standaarden gedurende de looptijd van het contract, zie voor de huidige lijst: https://www.forumstandaardisatie.nl/open-standaarden/verplicht?trefwoord=172. IPv6 en IPv4 worden ondersteund.
I19	De databasebeheerder mag geen inzage hebben in de opgeslagen gegevens van de Opdrachtgever. Dit is alleen van toepassing voor gegevens met een verhoogd beveiligingsniveau.
~~I20~~	~~Medewerkers van de Leverancier mogen zonder verwerkersovereenkomst geen toegang hebben tot de data van de Opdrachtgever.~~
I21	Het is mogelijk de test omgeving op te zetten door de productieomgeving te kopiëren met de dan bestaande data. Dit is een eenmalige handeling en hoeft niet periodiek herhaald te worden. ~~zonder daarbij de persoonsgegevens uit de productieomgeving mee te kopiëren, of waarbij persoonsgegevens uit de productieomgeving worden gepseudonimiseerd.~~
I22	Beheerportalen mogen niet zonder beperkingen worden blootgesteld, dat wil zeggen alleen benaderbaar zijn vanaf vast te leggen IP adressen en toegang wordt verleend na twee factor authenticatie.
I23	De basisbeveiliging van het Systeem is op orde volgens test van internet.nl.
I24	De basisbeveiliging van de mailcomponent van het Systeem is op orde volgens test van internet.nl
I25	Transport versleuteling voldoet aan de "Guidelines for quantum-safe transport-layer encryption" https://www.ncsc.nl/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption
SLA	
I26	De Leverancier is zonder enig voorbehoud verantwoordelijk voor backup, restore, recovery en uitwijk met betrekking tot de gehele oplossing. Hierbij geldt een Recovery Point Objective van maximaal 24 uur en een Recovery Time Objective van maximaal 4 uur.
I27	Voor het uitvoeren en afhandelen van niet-standaard wijzigingen, levert Leverancier voor de start van de uitvoering een plan van aanpak en een raming voor de eventuele kosten en doorlooptijd. Pas na akkoord van de Opdrachtgever op dit plan van aanpak zal Leverancier zijn werkzaamheden starten.
I28	Nieuwe releases moeten er in ieder geval voor zorgen dat de functionaliteit, zoals beschreven in de aanbestedingsstukken, gebruikt kan blijven worden. Nieuwe releases mogen dus niet leiden tot een verminderde functionaliteit of het niet meer kunnen voldoen aan de eerder hieraan gestelde eisen en wensen.
I29	Nieuwe releases worden standaard voorzien van releasenotes vooraf, welke minstens 5 werkdagen voorafgaand aan de release worden verstrekt aan de gemeente. De releasenotes omvatten ten minste: instructiemateriaal, informatie over eventuele impact op koppelingen, informatie over eventuele impact op certificaten en informatie over gewijzigde functionaliteit.
I30	Nieuwe major releases worden standaard uitgerold op de testomgeving. Deze kunnen in geval van releasefunctionaliteit die beduidende impact heeft op het gebruik, verplichte configuratie activiteiten van de gemeente vergt of niet standaard gedeactiveerd is, met een termijn van minimaal 10 werkdagen worden getest en

	geaccepteerd, alvorens de release wordt uitgerold naar de productieomgeving. Bij productiebelemmerende bevindingen wordt, totdat adequaat herstel en het testen hiervan heeft plaatsgehad, gezamenlijk een uitrolmoment bepaald.
I31	Het wijzigingen- en releasebeheer omvat eveneens het uitbrengen van impact analyses op basis van business requirements. Het betreft hier algemeen advies over een adequaat gebruik en beheer van de aangeboden oplossing in relatie tot management- en gebruikers- en beheerbehoeften van de Opdrachtgever.
I32	De Leverancier verzorgt een helpdesk, welke als 'single point of contact' dienstdoet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, alsook voor informatie over de afhandeling daarvan. De helpdesk is telefonisch bereikbaar van 8.30 uur tot 17.00 uur op werkdagen (maandag tot en met vrijdag met uitzondering van officiële feestdagen). Buiten deze tijden wordt een calamiteitenregeling door Leverancier beschikbaar gesteld (van toepassing zijnde op de incidenten met prioriteit TOP zoals onderstaand beschreven). In de SLA geeft Leverancier de omgang, respons- en oplostijden aan voor aangemelde incidenten. Daarbij wordt tevens de calamiteitenregeling beschreven.
I33	De helpdesk is ook beschikbaar via internet (webportaal of e-mail). Vragen, meldingen van incidenten en wijzigingsvoorstellen kunnen op alle dagen 24 uur per dag online worden ingediend (formulier). Dergelijke online vragen, meldingen van incidenten en wijzigingsvoorstellen worden automatisch per mail bevestigd en daarmee geregistreerd. Tevens kan de voortgang van deze incidenten en wijzigingsmeldingen in een webportaal worden geraadpleegd en gevolgd.
I34	Op basis van de urgentie en impact onderscheidt Leverancier in ieder geval drie prioriteiten voor incidenten en andersoortige meldingen (vragen, verzoek om informatie, service requests), te weten hoog, midden en laag. Naast bovenstaande prioriteiten is er een categorie 'TOP' welke van toepassing is voor incidenten waarbij de dienstverlening van Opdrachtgever (of de processen) ernstige hinder ondervindt (webportalen niet-beschikbaar, voor beheerders niet-beschikbaar), waarbij de informatieveiligheid in het gedrang komt of waarbij doorwerken in het Systeem leidt tot schade aan het Systeem of de data. Bij het indienen van een melding of incident is de gemeente altijd leidend in de bepaling van de prioriteit van de melding en daarmee zelfstandig sturend voor de onderstaand beschreven reactie-, oplos- en statusupdate-tijden.
I35	In het proces tussen het optreden van een incident en de definitieve oplossing onderscheidt Leverancier in ieder geval de volgende begrippen met bijbehorende definitie: Responstijd: de maximale tijd tussen het indienen van een melding en het versturen van de ontvangstbevestiging door Leverancier. Reactietijd: de maximale tijd tussen het indienen van een melding tot het aannemen van de melding door één van de oplosgroepen van Leverancier. Oplostijd: de maximale tijd tussen het indienen van een melding en het aanbieden van een oplossing (bij incidenten en wijzigingen) of het beantwoorden van een vraag. Statusupdate tijd: de maximale tijd tussen het indienen van een melding en de eerste statusupdate, of tussen de voorgaande statusupdate en de meest recente statusupdate. In de SLA die onderdeel vormt van de overeenkomst worden vermelde tijden nader ingevuld.

Systeem

Nr.	**Eis**

S1	Het Systeem wisselt objectgegevens uit met de Geovoorziening: Neuron BGT via het horizontaal tweerichtings berichtenverkeer conform StUFGeoIMGeo.
S2	Het Systeem wisselt via WFS gegevens uit met de interne raadpleegomgeving: Geoweb.
S3	Het Systeem wisselt gegevens uit met de externe portalen; gwsw.nl (via OroX), pdok.nl (via services) ~~en SENSRnet (via Services)~~.
S4	Het Systeem wisselt via API gegevens uit met de beheersystemen voor Gemalen en pompen: Aquaview en XDM
S5	Het Systeem wisselt via API gegevens uit met de WION-services voor de registratie van boven- en ondergrondse netten (WIBON).
S6	Het Systeem kan gebruikt worden op mobiele apparatuur.

Functioneel

Nr.	**Eis**
F1	Objecten kunnen conform IMBOR 2022 geregistreerd worden in het Systeem.
F2	Het Systeem beschikt over functionaliteit om gegevens over te nemen uit de revisieomgeving of uit revisiebestanden.
F3	Het Systeem beschikt over functionaliteit om gegevens via API's uit te wisselen.
F4	Het Systeem beschikt over functionaliteit voor het uitvoeren van inspecties.
F5	Het Systeem beschikt over functionaliteit voor het maken van planningen en begrotingen.
F6	Het Systeem beschikt over functionaliteit voor het registeren en verwerken van uitgevoerde werkzaamheden.
F7	Het Systeem beschikt over functionaliteit voor het schouwen op basis van beeldkwaliteit op basis van beeldmeetlatten.
F8	Het Systeem beschikt over functionaliteit voor het toepassen van 360 graden foto's.
F9	Het Systeem beschikt over functionaliteit voor het autoriseren van gebruikers.
F10	Het Systeem beschikt over functionaliteit voor het zoeken naar, selecteren van en filteren van gegevens.
F11	Het Systeem beschikt over functionaliteit voor het grafisch registeren van objecten.
F12	Het Systeem beschikt over functionaliteit voor het starten van videobeelden op de locatie van het toestandsaspect van het rioleringsobject.
F13	Het Systeem beschikt over functionaliteit voor raadplegers.
F14	Het Systeem beschikt over functionaliteit voor het maken van themakaarten.
F15	Het Systeem beschikt over functionaliteit voor het maken van management dashboards.
F16	Het Systeem beschikt over functionaliteit voor het importeren van objectgegevens voor tenminste de formaten XLS, CSV en Shape.
F17	Het Systeem beschikt over functionaliteit voor het exporteren van objectgegevens voor tenminste de formaten XLS, CSV en Shape.
F18	Het Systeem beschikt over functionaliteit voor het vastleggen van de historie van objectgegevens.
F19	Het Systeem beschikt over functionaliteit voor het controleren van de consistentie van gegevens.
F20	Het Systeem beschikt over uitgebreide helpfunctionaliteit.
F21	Het Systeem moet door de Organisatie zelf ingericht kunnen worden.

Methodieken

Nr.	**Eis**
M1	Bij het beheer van bomen wordt gebruik gemaakt van het Handboek Bomen 2022.

M2	Bij het beheer van civiele constructies wordt gebruikt gemaakt van de CUR117 en NEN2767.
M3	Bij het beheer van groen wordt gebruik gemaakt van de Groenbeheersystematiek van het CROW.
M4	Bij het beheer van riolering en stedelijk water wordt gebruik gemaakt van het Gegevenswoordenboek Stedelijk Water (GWSW).
M5	Bij het beheer van wegen wordt gebruik gemaakt van de Algemene Beheersystematiek Verhardingen
M6	Bij het beheer van Spelen en Sport wordt geïnspecteerd conform Warenwetbesluit Attractie- en Speeltoestellen (WAS).
M7	Bij het beheer van de objecten in de openbare ruimte wordt gebruik gemaakt van de beeldmeetlatten de Kwaliteitscatalogus Openbare Ruime (KOR) conform CROW 380.