Bijlage Programma van Eisen WDW

Algemeen

Nr.	Eis
A1	Inschrijver 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.
A3	Het Systeem is geschikt voor het beheren van assets (inspecties, maatregelen) van in ieder geval de volgende vakdisciplines: - Afval - Bomen - Civiele constructies - Ecologie - Faunavoorzieningen - Groen - Grondwater - Kabels & Leidingen - Meubilair - Riolering - Sport - Technische installaties - Verkeer - Verkeersregelinstallaties - Wegen
A4	De GIBIT-voorwaarden zijn van toepassing.
~~A5~~	~~Inschrijver dient, eventueel met behulp van onderaannemers, in het bezit te zijn van een geldig ISO 27001 certificaat (bij voorkeur organisatorisch geïmplementeerd conform de controls van ISO 27002) of aantoonbaar gelijkwaardig. Als gelijkwaardig wordt erkend een ander keurmerk en/of een verklaring, uitgebracht door een onafhankelijke instantie die voldoet aan de Europese normenreeks voor certificering, waarmee de inschrijver aantoont volledig te voldoen aan de gestelde eisen die ten grondslag liggen aan het gevraagde certificaat. Voeg een geldig certificaat en een toepassingsverklaring aan uw inschrijving toe of een ander keurmerk/verklaring die gelijkwaardig is aan ISO 27001.~~
A6	Het Systeem voldoet met betrekking tot aspecten van beveiliging en privacy aan de wettelijke eisen die de AVG en BIO stellen. 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.
A7	Inschrijver conformeert zich, uiteraard met de reikwijdte van de opdrachtscope en de eigen inschrijving hierop, 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~~ • Geo-standaarden • GWSW • IMKL • IPv6 en IPv4 • OpenAPI Specification • REST-API Design Rules • SAML

	• StUF • TLS

ICT

Nr.	Eis
I1	Het Systeem werkt als een volledige SaaS-oplossing of als een Citrix-oplossing. Met dit laatste wordt bedoeld dat ook van een virtual desktop-oplossing of een combinatie van een SaaS- en een virtual desktopoplossing gebruikt gemaakt kan worden.
I2	Het Systeem ondersteunt TLS 1.3 met betrekking tot de API-koppelingen voor gegevensuitwisselingen.
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 biedt een procedure voor het verwijderen van data/informatie (Niet zijnde Exit strategie).
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 Systeem ondersteunt toegang tot gegevens en functionaliteit door middel van een autorisatiesysteem op basis van rollen en rechten.
I7	Het Systeem ondersteunt veilig inloggen door SSO door middel van OAuth en SAML en federatie met Azure AD.
I8	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 (zoals toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).
I9	~~Het Systeem biedt zodanige functionaliteit m.b.t. auditing/logging dat van alle relevante handelingen en pogingen daartoe voor wat betreft processen, processtappen en statuswijzigingen - zowel door gebruikers als het Systeem zelf - 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.~~ Het Systeem biedt zodanige functionaliteit m.b.t. auditing/logging dat alle inlog- en muteeracties- alsmede errormeldingen 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.
I10	~~Het Systeem dient een audittrail van de proces- en gebruikersacties vast te leggen.~~ Het Systeem dient een audittrail van alle inlog- en muteeracties vast te leggen.
I11	Het Systeem dient de volgende handelingen vast te legen in een logging: inloggen, acties, logging in IIS inclusief eventuele applicatiefouten en data muteer acties. Deze logging blijft een half jaar bewaard.
I12	Het Systeem dient de integriteit van logging te waarborgen.
I13	Het Systeem kan koppelen (gegevens uitwisselen) met andere applicaties middels moderne API's
I14	De Leverancier past de hardening richtlijnen van het NIST toe
I15	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.
I16	De databasebeheerder mag geen inzage hebben in de opgeslagen gegevens van de Opdrachtgever. Dit is alleen van toepassing voor gegevens met een verhoogd beveiligingsniveau.
~~I17~~	~~Medewerkers van de leverancier mogen zonder verwerkersovereenkomst geen toegang hebben tot de data van de Opdrachtgever.~~
I18	Het is mogelijk de test omgeving op te zetten door de productie omgeving te kopiëren zonder daarbij de persoonsgegevens uit de productie omgeving mee te kopiëren, of waarbij persoonsgegevens uit de productieomgeving worden gepseudonimiseerd.
I19	Er zijn maatregelen genomen om het Systeem te beschermen tegen DDOS aanvallen.
I20	Beheerportalen mogen niet zonder beperkingen worden blootgesteld en toegang wordt verleend na twee factor authenticatie.
I21	Het is mogelijk de applicatie logging te koppelen aan het SIEM van de Opdrachtgever
I22	De Leverancier heeft maatregelen genomen voor het beheer van technische kwetsbaarheden (BIO 12.6.1). Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
I23	Leverancier is verplicht om de basisbeveiliging van het Systeem periodiek door externen te laten toetsen. Opdrachtgever heeft het recht om bevindingen van deze toets op te vragen.
I24	De webinterface van het Systeem is beveiligd tegen de OWASP-top 10 en leverancier garandeert dat dit gedurende de looptijd van het contract zo blijft.
I25	Data at rest (ook de back-up) en data in transit wordt versleuteld volgens de geldende standaarden gedurende de looptijd van de overeenkomst. Voor in transit is dit op dit moment TLS 1.2 en TLS 1.3, voor data at rest Advanced Encryption Standard (AES)-256.
I26	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
~~I27~~	~~Het Systeem is Digitoegankelijk volgens EN 301 549 met WCAG 2.1, https://forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21~~
I28	Leverancier is zonder enig voorbehoud verantwoordelijk voor backup, restore, recovery en uitwijk met betrekking tot het gehele Systeem. Hierbij geldt een Recovery Point Objective van maximaal 24 uur en een Recovery Time Objective van maximaal 4 uur.
I29	Voor het uitvoeren en afhandelen van niet-standaard wijzigingen, levert inschrijver 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 inschrijver zijn werkzaamheden starten.
I30	Nieuwe releases moeten er in ieder geval voor zorgen dat de functionaliteit, zoals beschreven in deze aanbestedingsdocumentatie, 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.
I31	Nieuwe releases worden standaard voorzien van releasenotes vooraf, welke minstens 5 werkdagen voorafgaand aan de release worden verstrekt aan de Opdrachtgever. De releasenotes omvatten ten minste: instructiemateriaal,

	informatie over eventuele impact op koppelingen, informatie over eventuele impact op certificaten en informatie over gewijzigde functionaliteit.
I32	Nieuwe 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 Opdrachtgever 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 productie belemmerende bevindingen wordt, totdat adequaat herstel en het testen hiervan heeft plaatsgehad, gezamenlijk een uitrolmoment bepaald.
I33	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 het de aangeboden Systeem in relatie tot management- en gebruikers- en beheerbehoeften van de Opdrachtgever.
I34	De inschrijver 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 inschrijver beschikbaar gesteld (van toepassing zijnde op de incidenten met prioriteit TOP zoals onderstaand beschreven). In de SLA geeft inschrijver de omgang, respons- en oplostijden aan voor aangemelde incidenten. Daarbij wordt tevens de calamiteitenregeling beschreven.
I35	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 digitaal worden geraadpleegd en gevolgd.
I36	Op basis van de urgentie en impact onderscheidt inschrijver 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 Opdrachtgever altijd leidend in de bepaling van de prioriteit van de melding en daarmee zelfstandig sturend voor de onderstaand beschreven reactie-, oplos- en statusupdate-tijden.
I37	In het proces tussen het optreden van een incident en de definitieve oplossing onderscheidt inschrijver 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 inschrijver. Reactietijd: de maximale tijd tussen het indienen van een melding tot het aannemen van de melding door één van de oplosgroepen van inschrijver. 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.

I38	Gepland onderhoud vindt plaats buiten reguliere kantoortijden (07.00 uur – 17.00 uur) en alleen na toestemming van de organisatie. Het geplande onderhoud moet tenminste 2 weken en waar mogelijk 5 weken van te voren worden aangekondigd. De huidige werkwijze is dat updates minimaal 5 weken waar mogelijk van te voren ingepland en aangevraagd moeten worden bij het CAB (Change Advisory Board). Na goedkeuring kan de update uitgevoerd worden.
I39	Het Systeem is op basis van DNS (Domain Naming Service) ingericht.
I40	Autorisaties worden uitgegeven conform Active Directory management hiërarchie en Office 365 (OneDrive, Teams, etc.)
I41	Het Systeem ondersteunt alle gangbare browsers, minimaal 1 na laatste versie: Firefox, Safari, Chrome, Edge

Systeem

Nr.	Eis
S1	Het Systeem wisselt objectgegevens uit met de Geovoorziening: Giskit Basiskaart via het horizontaal berichtenverkeer StUFGeoIMGeo.
S2	Het Systeem wisselt via WFS gegevens uit met de interne raadpleegomgeving: Giskit Tabula.
S3	Het Systeem wisselt gegevens uit met de externe portalen; gwsw.nl (via OroX) en pdok.nl (via services).
S4	Het Systeem wisselt via API gegevens uit met het beheersysteem voor Gemalen: SAM.
S5	Het Systeem wisselt via API gegevens uit met het beheersysteem voor Spelen: Playmapping.
S6	Het Systeem wisselt via API gegevens uit met het beheersysteem voor Verlichting: LMS.
S7	Het Systeem wisselt gegevens uit met het beheersysteem voor Water: Baggerbase.
S8	Het Systeem wisselt via API gegevens uit met de WION-applicatie GOconnectIT voor de registratie van boven- en ondergrondse netten (WIBON).
~~S9~~	~~Binnen het Systeem kunnen gegevens van de waarnemingsapp voor Flora en Fauna geraadpleegd worden.~~
S10	Het Systeem kan gebruikt worden op mobiele apparatuur.

Functioneel

Nr.	Eis
F1	Objecten moeten conform IMBOR 2022 geregistreerd worden in het Systeem, en de releases/versies die op dit IM volgen.
F2	Het Systeem beschikt over functionaliteit om gegevens over te nemen uit de revisieomgeving.
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 en oblique luchtfoto'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 van het Norminstituut Bomen.
M2	Bij het Beheer van Civiele constructies wordt gebruikt gemaakt van de CUR119 en NEN2767.
M3	Bij het Beheer van Faunavoorzieningen wordt gebruik gemaakt van de Nationale databank Flora en Fauna (NDFF).
M4	Bij het Beheer van Groen wordt gebruik gemaakt van de Groenbeheersystematiek van het CROW.
M5	Bij het Beheer van Riolering en Stedelijk water wordt gebruik gemaakt van het Gegevenswoordenboek Stedelijk Water (GWSW).
M6	Bij het Beheer van Wegen wordt gebruik gemaakt van de Algemene Beheersystematiek Verhardingen en CROW-publicatie 185 – Handboek Aansprakelijkheid Openbare Ruimte