

Programma van eisen

Aanbesteding ITSM applicatie – Gemeente Zeist

Inleiding

In dit Programma van eisen is beschreven waar de IT Service Management applicatie (ITSM-applicatie) aan moet voldoen. Het Programma van eisen is voorgelegd aan diverse stakeholders binnen de gemeente met als doel om een ITSM-applicatie aan te schaffen dat op een efficiënte en gebruiksvriendelijke manier de dienstverlening van opdrachtgever ondersteund en verder verbeterd. Efficiënt om ervoor te zorgen dat medewerkers bij het doen van een melding of behandelaars bij het behandelen van een melding worden voorzien van informatie en een eventuele oplossing. Gebruiksvriendelijk doordat het een overzichtelijke en intuïtieve interface biedt. Gebruikers kunnen snel hun weg vinden dankzij de consistente navigatie en duidelijke iconen. Foutmeldingen worden op een begrijpelijke manier weergegeven, en veelgebruikte functies zijn met minimale handelingen te bereiken.

Programma van eisen

nr	onderwerp	beschrijving
1	Algemeen	De ITSM-applicatie en alle bijbehorende diensten en producten worden in de Nederlandse taal geleverd. Medewerkers van de opdrachtnemer bieden ondersteuning in de Nederlandse taal in woord en geschrift.
2	Algemeen	De ITSM-applicatie kent geen maatwerk. Als toch een bepaalde functionaliteit specifiek voor deze aanbesteding is ontwikkeld of op een later moment tijdens de duur van de overeenkomst, dan wordt deze in de eerstvolgende release opgenomen als standaardfunctionaliteit van de ITSM-applicatie voor alle klanten.
3	Algemeen	In het geval van relevante nieuwe of gewijzigde Europese en rijks wet- en regelgeving zijn relevante updates uiterlijk één maand voor inwerkingtreding van deze regelgeving beschikbaar in de ITSM-applicatie.
4	Algemeen	De opdrachtnemer garandeert gedurende de gehele contractperiode de beschikbaarheid van onderhoud van de te leveren applicatie
5	Algemeen	De opdrachtnemer is verantwoordelijk voor de kwalificaties en screening (VOG) van het eigen personeel. De opdrachtgever kan vragen om inzicht hierin.
6	Algemeen	De applicatie dient te voldoen aan de eisen die door de Baseline Informatiebeveiliging Overheid zijn opgelegd.
7	Algemeen	De gehele applicatie, front-end en back-end, is doorzoekbaar op combinaties van (steek)woorden, bepaalde periode enz. De applicatie moet op basis van woorden of delen van woorden de juiste resultaten aanbieden aan de gebruiker.
8	Algemeen	De opdrachtgever krijgt de beschikking over een gescheiden productie- en testomgeving. De productie omgeving kan op verzoek worden gekopieerd naar de testomgeving.
9	Dienstverlening en support	De opdrachtnemer verzorgt een Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen en het indienen van wijzigingsvoorstellen. Ook geeft deze informatie over- en inzicht in de afhandeling daarvan.
10	Dienstverlening en support	De helpdesk is telefonisch bereikbaar op werkdagen (maandag tot en met vrijdag) tussen 08.00 en 18.00 (CET). Voor ondersteuning door de helpdesk van de opdrachtnemer worden geen aanvullende kosten in rekening gebracht.
11	Dienstverlening en support	De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen en incidenten m.b.t. de oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA).
12	Dienstverlening en support	De opdrachtnemer garandeert adequate back-up- en restorevoorzieningen van de ITSM-applicatie waardoor in geval van een gebeurtenis buiten de invloedssfeer van de opdrachtnemer (bijvoorbeeld een ramp of incident) het verlies van gegevens maximaal 8 uur bedraagt.
13	Dienstverlening en support	Er dient een actuele digitale handleiding beschikbaar te zijn over de werking van de applicatie specifiek voor medewerkers en behandelaren. Deze dient tijdens de contractduur actueel te worden gehouden door de opdrachtnemer.
14	Dienstverlening en support	Om de afspraken in de SLA te monitoren zal er jaarlijks minimaal 2 keer overleg plaatsvinden tussen opdrachtnemer en opdrachtgever.
15	Medewerker portaal	Het medewerker portaal voldoet aan de eisen voor digitale toegankelijkheid (WCAG 2.2)
16	Medewerker portaal	Het medewerker portaal kan verwijzingen opnemen naar andere applicaties of websites.
17	Medewerker portaal	Er is een medewerker portaal waarin onder andere de voortgang van de melding is te volgen.
18	Kennisbank	De applicatie moet een kennisbank beschikbaar stellen waarin standaard oplossingen en FAQ's kunnen worden geregistreerd. De kennisbank is toegankelijk voor medewerkers en behandelaren. In de kennisbank worden verwijzingen naar documenten (beleidsstukken, procedures, werkinstructies; Pdf- Word- Excel- PowerPoint bestanden) ontsloten.
19	Meldingen/wijzigingen	De applicatie biedt de mogelijkheid om meldingen te typen tot incident, wijziging, major melding op basis van de ITIL richtlijnen/definities. Het moet mogelijk zijn om meldingen om te zetten naar de verschillende typeringen.
20	Meldingen/wijzigingen	Het is binnen de ITSM-applicatie standaard mogelijk om minimaal de navolgende gegevens bij een melding vast te leggen: datum en tijd van aanmelden van de melding, categorie melding

		(gekozen uit een vooraf gedefinieerde lijst), de gegevens van de melder, persoon waar de melding betrekking op heeft (kan anders zijn dan de melder), beschrijving van de melding en de manier van aanmelden, fysieke locatie, ruimte of kamer waar de melding betrekking op heeft indien van toepassing, koppeling naar relevante middelen (CMDB).
21	Meldingen/wijzigingen	Wanneer er een melding wordt gemaakt, worden direct de aan de indiener verbonden gegevens ingevuld.
22	Meldingen/wijzigingen	Medewerkers kunnen meldingen doen, vragen stellen, wijzigingsverzoeken indienen, status opvragen via het medewerkersportaal of rechtstreeks in de back-end.
23	Meldingen/wijzigingen	De applicatie biedt een planningsbord (of anders) waar meldingen kunnen worden gepland en gevolgd zodat de voortgang en prioriteit van melding en wijziging wordt bewaakt.
24	Meldingen/wijzigingen	Binnen een melding (incidentmeldingen en wijzigingsmeldingen) dient de historie (wie heeft wat gedaan) zichtbaar te zijn.
25	Meldingen/wijzigingen	Meldingen moeten ingericht kunnen worden met een hoofdmelding en daaronder de mogelijkheden tot deelmeldingen. Deze deelmeldingen moeten uitgezet kunnen worden aan andere behandelaars. De hoofd-melding kan pas afgesloten worden als de deelmeldingen op gereed staan.
26	Meldingen/wijzigingen	De applicatie moet functionaliteit hebben om meldingen in te schalen op verschillende prioriteiten, bijvoorbeeld laag, middel, hoog en kritiek.
27	Meldingen/wijzigingen	Communicatie via de mail of via het medewerkersportaal over een melding wordt rechtstreeks aan een melding toegevoegd.
28	Meldingen/wijzigingen	De applicatie is te gebruiken op elk mobiel apparaat. Dit geldt voor het doen van meldingen door gebruikers als voor het afhandelen door behandelaars.
29	Meldingen/wijzigingen	De applicatie biedt de mogelijkheid voor behandelaars om meerdere meldingen in 1 keer te kunnen afsluiten/wijzigen.
30	Meldingen/wijzigingen	Gemaakte meldingen kunnen eenvoudig geëscaleerd/doorgezet worden naar een (behandel)groep. Zowel intern als extern (naar leveranciers).
31	Meldingen/wijzigingen	De applicatie laat visueel zien als meldingen nieuw zijn of later dan de SLA afgehandeld zijn.
32	Meldingen/wijzigingen	De applicatie laat duidelijk zien wie waarop wacht en welke actie moet worden ondernomen. De applicatie ondersteunt diverse status overgangen, zoals 'wacht op leverancier', 'wacht op klant', 'in behandeling', 'opgelost', 'afgesloten'. De behandelaars kunnen de status van een melding aanpassen.
33	Meldingen/wijzigingen	De behandelaar moet interne en externe aantekeningvelden kunnen splitsen, zodat de melder alleen de hoognodige informatie ziet.
34	Meldingen/wijzigingen	In de applicatie moet het mogelijk zijn om bijlagen te uploaden in meldingen (onafhankelijk van de bestandsextensie/type).
35	Meldingen/wijzigingen	Uniforme antwoorden op meldingen zijn door de behandelaars in te stellen en gemakkelijk te plaatsen.
36	Meldingen/wijzigingen	Meldingen moeten gekoppeld kunnen worden aan middelen in het CMDB zodat je vanuit het CMDB ziet welke meldingen hebben plaatsgevonden.
37	Middelenbeheer	De applicatie heeft een CMDB voor het vastleggen van middelen die gekoppeld kunnen worden aan medewerkers, objecten of andere middelen.
38	Middelenbeheer	Het is mogelijk om in het CMDB per middel te zien welke meldingen er op dit item zijn binnengekomen.
39	Middelenbeheer	De applicatie geeft een visuele weergave van de samenhang en koppelingen tussen de verschillende middelen. De samenhang en koppelingen kunnen visueel gemaakt worden. Bv. voor een architectuurplaat.
40	Middelenbeheer	De applicatie biedt de mogelijkheid om certificaten vast te leggen en op de einddatum te signaleren.
41	Rapportage	Het systeem kan managementrapportages en/of dashboards genereren over openstaande en afgehandelde incidenten/wijzigingen, doorlooptijden, trendontwikkelingen. De rapportages kunnen worden omgezet naar excel. De rapportage moet kunnen worden samengesteld op basis van alle beschikbare velden.
42	Functioneel beheer	De applicatie biedt standaard workflows gebaseerd op best practice ervaringen (conform ITIL). Deze workflows zijn aanpasbaar door de opdrachtgever.
43	Functioneel beheer	De autorisaties in de applicatie worden rol gebaseerd ingericht op basis van de taak in het proces. Functiescheiding in de autorisaties aanbrengen is mogelijk. Deze autorisaties worden door de opdrachtgever beheerd.
44	Functioneel beheer	Opdrachtgever heeft de mogelijkheid om statussen (benamingen, tijdsbepalingen etc.) te kunnen toevoegen/aanpassen/verwijderen.
45	Functioneel beheer	Per proces is het instelbaar om notificaties (e-mail) naar behandelaars te sturen. Tevens wordt de doorlooptijd per melding geregistreerd.
46	Functioneel beheer	Er moet ingesteld kunnen worden dat meldingen die onder bepaalde criteria (onderwerpen, HRM gerelateerde meldingen, CMDB items, beveiligingsincidenten) slechts voor een geselecteerde groep gebruikers zichtbaar zijn. Dit zowel op het scherm als in rapportages.
47	Functioneel beheer	Het is mogelijk om het medewerker portaal in de eigen huisstijl in te richten.
48	Techniek	Het is mogelijk om medewerkers buiten de provisioning om, op te voeren in de applicatie.

49	Techniek	De applicatie is SAAS en kan via Microsoft authenticator koppelen met Azure Active Directory.
50	Techniek	Voor dagelijks gebruik door alle medewerkers volstaat een actuele webbrowser (ten minste alle volgende: Edge/Firefox/Chrome). De browser is qua versie/updates maximaal 3 maanden oud en wordt ondersteund door ontwikkelaar.
51	Techniek	Gebruik of afhankelijkheid van webbrowser plug-ins (Java/Flash/Silverlight etc.) is in verband met informatieveiligheid, beheer en onderhoud niet toegestaan.
52	Techniek	De ITSM-applicatie draait volledig in het datacenter van opdrachtnemer
53	Techniek	Voor toegang tot de applicatie wordt op geen enkele manier gebruik gemaakt van remote-desktop oplossingen zoals Citrix / Microsoft RDP etc. (zie ook eis 54 'zero footprint').
54	Techniek	We gaan uit van 'zero footprint' op de werkplek van de gebruiker. De ITSM-applicatie heeft geen lokale installatie van software nodig op de werkplek om te functioneren en/of toegang te krijgen tot de applicatie. Dit geldt voor alle processen, bijvoorbeeld ook voor het bewerken van documenten.
55	Techniek	De applicatie valideert invoerdata tijdens invoering in de applicatie interface zoals bijvoorbeeld een datum.
56	Techniek	De ITSM-applicatie maakt gebruik van een responsive webdesign zonder kwaliteit in te leveren op leesbaarheid van tekst met behoud van alle functionaliteiten.
57	Techniek	De gemiddelde laadtijd van een pagina is minder dan 3 seconden.
58	Techniek	Opdrachtnemer zorgt ervoor dat Opdrachtgever geen last heeft van onwenselijk gedrag van andere klanten (bijv. spamming vanuit eenzelfde ipadres).
59	Techniek	Opdrachtnemer voorkomt dat gebruik van gedeelde componenten door andere klanten in de infrastructuur de performance bedreigen.
60	Techniek	De applicatie is 24/7 beschikbaar, behalve bij aangekondigd periodiek onderhoud buiten werktijden. .
61	Techniek	In de ITSM-applicatie kan met meer dan 100 gebruikers tegelijkertijd worden gewerkt zonder merkbaar performanceverlies
62	Techniek (standaarden en koppelingen)	Het is mogelijk om via een API koppeling de applicatie te koppelen aan andere software applicaties die ook API koppelingen accepteren.
63	Techniek (standaarden en koppelingen)	De opdrachtnemer waarborgt dat de aangeboden ITSM-applicatie niet meer dan één major versie achterloopt ('neerwaartse comptabiliteit') zoals de webrichtlijnen en de landelijke standaarden, zoals de Zaak- en documentservices resp. StUF-BG, RGBZ, ImZTC en RSGB die voor de ITSM-applicatie van toepassing zijn. Aanpassingen in de hierboven genoemde standaarden worden door de opdrachtnemer verwerkt binnen 12 maanden nadat deze niet meer door VNG Realisatie als geldende standaard worden ondersteund. Daarna wordt de oude versie van de standaard nog minimaal 12 maanden ondersteund.
64	Techniek (standaarden en koppelingen)	Indien de Opdrachtgever ervoor kiest om tussen de ITSM-applicatie en andere systemen basisgegevens uit te wisselen, gebeurt dit conform het sectormodel StUF –BG v 2.04 of StUF-BG v 3.10.
65	Techniek (standaarden en koppelingen)	Indien binnen de looptijd van het contract een nieuwe StuF-versie wordt uitgebracht dient u deze binnen 1 jaar na vaststelling van de nieuwe StuF-versie te ondersteunen.
66	Techniek (standaarden en koppelingen)	Databases zijn volledig toegankelijk voor inleesacties (zoals t.b.v. Cognos of PowerBI).
67	Techniek (standaarden en koppelingen)	De opdrachtnemer levert documentatie inzake koppelingen met andere systemen, alsmede van de architectuur van de applicatie.
68	Techniek (security)	Two-factor authentication is aan te zetten als vereiste voor toegang tot de applicatie. Hierbij is het mogelijk om op basis van een lijst IP adressen (whitelist) dit te onderdrukken voor gebruikers die aanmelden vanuit die IP adressen. Two-factor authenticatie verloopt via een OTP smscode en/of Microsoft authenticator.
69	Techniek (security)	De Opdrachtgever blijft te allen tijde eigenaar van de data en de opdrachtnemer stelt alle data binnen de ITSM-applicatie beschikbaar aan de Opdrachtgever bij afloop van het contract. Deze data wordt niet voor andere doeleinden gebruikt door de opdrachtnemer.
70	Techniek (security)	De opdrachtnemer garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. vervangen.
71	Techniek (security)	Om specifieke beheerrechten te krijgen binnen de ITSM-applicatie is een bewuste actie door een (andere) beheerder verplicht.
72	Techniek (security)	Indien een medewerker wisselt van gebruiker naar beheerder als rol, dan is dit expliciet zichtbaar in de interface van de applicatie.
73	Techniek (security)	De ITSM-applicatie ondersteunt role based access: rechten en autorisaties binnen de ITSM-applicatie zijn gekoppeld aan een rol. Een gebruiker is lid van een rol en kan lid zijn van meerdere rollen.
74	Techniek (security)	Authenticatie moet verlopen via Microsoft Azure AD van de Opdrachtgever. Dit op basis van SAML 2.0 / ADFS 3.0. Kosten hiervan zijn volledig inbegrepen in de aanbieding.
75	Techniek (security)	Na authenticatie via de Azure Active Directory, hebben gebruikers door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van de ITSM-applicatie, uiteraard voor zover ze daartoe zijn geautoriseerd. Met SSO hoeft de gebruiker niet apart in te loggen in de ITSM-applicatie nadat de gebruiker is aangemeld op het netwerk / zijn gemeentelijke werkplek (via

		Active Directory). Alleen om specifieke beheerrechten te krijgen is het toegestaan dat er een handmatige login nodig is.
76	Techniek (security)	Gegevens die van en naar het systeem worden getransporteerd, in welke vorm dan ook, dienen beveiligd te worden door middel van encryptie. Hierbij dient gebruik te worden gemaakt van het SSL protocol op basis van TLS 1.2 of beter of gelijkwaardig
77	Techniek (security)	Gegevens binnen het systeem dienen versleuteld opgeslagen te worden waarbij minimaal gebruik wordt gemaakt van AES-256.
78	Techniek (security)	Bij het opslaan van wachtwoorden is hashing en salting gebruikt.
79	Techniek (security)	Binnen de OTA-omgevingen wordt geen gebruik gemaakt van productiedata. De opdrachtnemer faciliteert testdata via scripts of andere wijze zodat gegevens niet herleidbaar zijn naar bijv. personen.
80	Techniek (security)	Er wordt minimaal een test- en productieomgeving beschikbaar gesteld (totaal 2 omgevingen) inclusief alle in dit PvE geëiste koppelingen. De testomgeving geeft te allen tijde een representatie van de productieomgeving en moet continu beschikbaar zijn.
81	Techniek (security)	Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10.
82	Techniek (security)	Alle verkeer verloopt via https (waar relevant).
83	Techniek (security)	Op het moment van ingebruikname in productie, dienen alle standaard wachtwoorden (waaronder administrator) aangepast te worden.
84	Techniek (security)	Er is op geen enkele wijze sprake inlogmogelijkheden voor opdrachtnemer (backdoor) waar opdrachtgever niet van op de hoogte is. Toegang tot de omgeving wordt altijd vooraf overlegd.
85	Techniek (security)	De testomgeving werkt geïsoleerd en is niet gekoppeld aan de productieomgeving.
86	Techniek (security)	Een actieve sessie met de software heeft een instelbare timeout (deze staat standaard op 15 minuten).
87	Techniek (security)	De infrastructuur en organisatie van de opdrachtnemer zijn adequaat en op elk moment met certificering en rapportages aantoonbaar beveiligd volgens ISO/IEC 27001 en 27002 of vergelijkbaar en voldoen aan de voorwaarden genoemd in de Algemene verordening Gegevensbescherming (AVG).
88	Techniek (security)	De opslag en verwerking van gegevens vindt plaats binnen Nederland en alle infrastructuur bevindt zich fysiek in een datacenter in Nederland.
89	Techniek (security)	De ITSM-applicatie ondersteunt DNSSEC voor de webservices.
90	Techniek (security)	Opdrachtnemer zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen aan de Opdrachtgever worden gerapporteerd.
91	Techniek (security)	Er is een totaaloverzicht beschikbaar van autorisaties van zowel Opdrachtnemer als Opdrachtgever.
92	Techniek (security)	De logging biedt voldoende inzicht in de uitwisseling, en selecties van gegevens om het gebruik van een gegeven door een applicatie te kunnen achterhalen en hierop te signaleren of acteren.
93	Techniek (security)	Een logregel bevat minimaal: · een tot een natuurlijk persoon herleidbare gebruikersnaam of ID; · de gebeurtenis; · waar mogelijk de identiteit van het werkstation of de locatie; · het object waarop de handeling werd uitgevoerd; · het resultaat van de handeling; · de datum en het tijdstip van de gebeurtenis.
94	Techniek (security)	De logging is voor een periode van minimaal 3 jaar beschikbaar te maken.
95	Techniek (security)	De logging is alleen beschikbaar voor daartoe geautoriseerde medewerkers van de opdrachtgever.
96	Techniek (security)	De logging is read-only. Het muteren en verwijderen van log-records is niet toegestaan.
97	Techniek (security)	Als er een Third Party Mededeling is (verklaring van een onafhankelijke externe deskundige met een oordeel over de maatregelen die de opdrachtnemer heeft getroffen) dan kan de Opdrachtgever deze inzien.
98	Techniek (security)	Audit informatie over de toegang tot gegevens is eenvoudig en kosteloos te raadplegen door de opdrachtgever.
99	Techniek (security)	Opdrachtnemer verleent medewerking indien de opdrachtgever een audit/pentest wil uitvoeren
100	Techniek (security)	Opdrachtnemer handelt in overeenstemming met de AI act wetgeving.
101	Techniek (security)	Tussen opdrachtgever en opdrachtnemer wordt een verwerkersovereenkomst afgesloten volgens het standaard model van de VNG.
102	Integratie en schaalbaarheid	De ITSM-applicatie ondersteunt het gebruik van gangbare fysieke asset tags (streepjescode en/of QR code) voor het opzoeken van een middel.

103	Integratie en schaalbaarheid	Integratie met de opdrachtnemer voor bulk import van nieuw geleverde hardware, maar ook niet gerelateerde IT-items zoals meubilair. Dit mag via een CSV of Excel import.
104	Integratie en schaalbaarheid	De ITSM-applicatie heeft een koppelvlak zodat gegevens zowel geïmporteerd als geëxporteerd kunnen worden op basis van API's .
105	Integratie en schaalbaarheid	Integratie met de leverancier van ons huidige intranet oplossing (Embrace) voor het aanmelden van nieuwe meldingen en aanvragen, op de persoonlijke intranet startpagina is een overzicht te tonen van openstaande huidige meldingen/aanvragen van de gebruiker.
106	Integratie en schaalbaarheid	Er is zitten geen limieten op het aantal middelen binnen het CMDB
107	Integratie en schaalbaarheid	Er is een integratie met leverancier PQR, waarmee meldingen die ingevoerd worden in de ITSM-applicatie van opdrachtgever automatisch worden doorgezet naar leverancier (gebruikt Autotask PSA) en bewaakt kunnen worden in de eigen ITSM-applicatie.
108	Integratie en schaalbaarheid	Er zitten geen limieten aan het aantal gebruikers, behandelaren en administrator accounts
109	Integratie en schaalbaarheid	Bij overschrijding van het aantal actieve licenties voor gebruikers of beheerders (of welke limiet dan ook die onder licenties valt) blijft de applicatie onverminderd beschikbaar voor gebruik voor opdrachtgever. Opdrachtnemer signaleert dit en benadert opdrachtgever om dit op te pakken.