

Programma van Eisen voor de aanschaf van een Applicant Tracking System (ATS)

Inleiding

Veiligheidsregio Utrecht (VRU) is een overheidsorganisatie die verantwoordelijk is voor de crisisbeheersing, brandweertzorg, geneeskundige hulpverlening en rampenbestrijding in de regio Utrecht. Met ca. 700 medewerkers en ca. 1700 vrijwilligers is de VRU een belangrijke schakel in de veiligheidsketen. VRU streeft ernaar om een "great place to work" te zijn, waar medewerkers zich gewaardeerd, betrokken en gemotiveerd voelen. De ontwikkelingen op de arbeidsmarkt vragen om een effectief wervings- en selectieproces om zo de juiste talenten aan te trekken en te behouden.

Projectomschrijving

Doelstellingen

Het doel van dit project is om de wervingsprocessen te stroomlijnen en de kandidaat-ervaring te verbeteren. De huidige wervingsprocessen van VRU kunnen worden verbeterd met behulp van een modern en gebruiksvriendelijk ATS. Een goed ingericht ATS draagt bij aan het versterken van het werkgeversmerk door een positieve sollicitatie-ervaring te bieden die de reputatie van de organisatie als aantrekkelijke werkgever versterkt. Dit document zet de vereisten en verwachtingen van Veiligheidsregio Utrecht voor het nieuwe ATS uiteen.

Aantallen

Voor het gebruik van ATS heeft VRU de volgende aantallen gebruikers voor ogen:

1. 2 recruiters
2. ca. 2 communicatieadviseurs
3. ca. 140 vacature-houders, met name leidinggevenden
4. ca. 4 deelnemers in de selectiecommissie per vacature
5. ca. 1000 kandidaten/sollicitanten voor ca. 150 vacatures per jaar
6. 1 functioneel beheerder

Planning

Publicatie : dinsdag 14 mei 2024

Sluitingsdatum : maandag 27 mei 2024 9:00 uur

Vragenronde : opdrachtgever maakt geen gebruik van een vragenronde.

Algemene eisen

#	Omschrijving
1.	Opdrachtnemer conformeert zich aan de eisen van de GIBIT 2023 en ICT-kwaliteitsnormen voor de Veiligheidsregio 2023 (bijgevoegd).
2.	Opdrachtnemer en het ATS voldoen aan alle eisen zoals gesteld in de privacywetgeving Algemene Verordening Gegevensbescherming (AVG/GDPR) en andere relevante wet- en regelgeving op het gebied van privacy en gegevensbescherming.
3.	Voor het vastleggen van de afspraken m.b.t. de verwerking van gegevens wordt gebruik gemaakt van de verwerkersovereenkomst van VRU.
4.	Opdrachtnemer/leverancier van het aan te kopen systeem werkt mee aan het uitvoeren van een DPIA. Van opdrachtnemer wordt verwacht dat alle technische en organisatorische maatregelen genomen worden die naar de stand der techniek verwacht mogen worden, gebaseerd op de aard van de gegevens en de verwerking.
5.	Om te voorkomen dat privacy-gevoelige informatie wordt verspreid moet er de mogelijkheid zijn om de voorkomen dat documenten worden gedeeld buiten het ATS, bijv. door niet toestaan van doorsturen of downloaden.
6.	Opdrachtgever sluit na definitieve gunning een SLA af met Opdrachtnemer waarin nadere afspraken worden gemaakt over de te leveren dienstverlening, binnen de kaders van en in overeenstemming met het Programma van Eisen en de Overeenkomst.
7.	Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken servicelevels en het doorvoeren van veranderingen en verbeteringen (vastgelegd in evt. verbeterplannen) is regelmatig overleg op diverse organisatieniveaus noodzakelijk. Periodiek vindt overleg plaats tussen de VRU en Opdrachtnemer over deze dienstverlening. Daarnaast zullen in het kader van verlengingen van het contract evaluaties tussen beide Partijen plaatsvinden. Deze structuren worden vastgelegd in de SLA.
8.	Alle gegevens binnen de oplossing, dan wel ter beschikking gesteld aan de opdrachtnemer ten behoeve van de opdracht blijven te allen tijde eigendom van de VRU.
9.	Indien de overeenkomst eindigt, ongeachte de reden voor beëindiging, dienen alle eigendommen van de VRU, inclusief systeem en data, te worden overgedragen aan de opdrachtgever binnen een redelijke termijn.
10.	De oplossing wordt geleverd als SaaS-dienst, waarbij zowel het draaiende houden (operations) als het doorontwikkelen (development) door de Opdrachtnemer wordt uitgevoerd. Het technisch-beheer en applicatie-beheer ligt volledig bij de Opdrachtnemer. Het functioneel-beheer ligt zowel bij Opdrachtnemer, als bij de Opdrachtgever.
11.	Er zijn geen installaties nodig in de VRU-omgeving om gebruik te kunnen maken van de oplossing. Indien het voor de oplossing noodzakelijk is dat er wijzigingen plaatsvinden binnen de omgeving van de VRU, dan zijn hiervoor (ook in de testfase) de handleidingen voor systeembeheer beschikbaar en worden gespecificeerd voor de inrichting van de VRU.
12.	De opdrachtnemer levert de oplossing compleet en bedrijfsvaardig op.

Functionele eisen

#	Omschrijving
13.	Vacaturebeheer: Het systeem moet de mogelijkheid bieden om de reden van de vacatures vast te leggen, vacatures aan te maken, te bewerken, te kopiëren, te publiceren, te archiveren en te verwijderen. Gebruikers moeten vacaturedetails zoals selectiecommissie, functietitel, omschrijving, arbeidsvoorwaarden (bv salaris, uren) vereisten en locatie kunnen invoeren en beheren. Het lettertype, de tekengrootte, tekstkleur e.d. is eenvoudig te bewerken.
14.	Kandidaatbeheer: Het systeem heeft een centrale plek voor het beheren van alle kandidaatgegevens, inclusief cv's, contactgegevens, sollicitatiestatus, eerdere sollicitaties en communicatiegeschiedenis. Het is eenvoudig om notities en documenten toe te voegen aan het profiel van een kandidaat.
15.	Communicatie met kandidaten vanuit ATS: Gebruikers moeten in staat zijn om e-mails en agenda-afspraken te versturen, ontvangen en plannen vanuit het ATS zelf, waardoor directe communicatie met sollicitanten mogelijk is zonder het systeem te verlaten.
16.	Mogelijkheid voor het plaatsen van projecten/klussenbank/ voor interne opdrachten
17.	Tijdslimieten: Recruiters kunnen tijdslimieten instellen voor verschillende fasen van het wervingsproces waarbij zij een melding krijgen als de duur is verstreken, zoals de duur van een bepaalde fase in de funnel, de deadline voor sollicitaties en de planning van interviews.
18.	Talentpools: Het systeem biedt de functionaliteit om gekwalificeerde kandidaten op te slaan in zelf te benoemen talentpools voor toekomstige vacatures, zodat ze gemakkelijk kunnen worden teruggevonden en benaderd.
19.	Templates: Zelf ontwerpen en te beheren sjablonen/templates zijn beschikbaar voor vacatures, e-mails en andere communicatie, om consistentie en efficiëntie te bevorderen.
20.	Inrichting funnels: Recruiters moeten in staat zijn om verschillende wervingsfunnels of -workflows in te stellen als standaard, en op basis van specifieke vacatures of behoeften, om het wervingsproces te stroomlijnen en aan te passen aan verschillende situaties, inclusief de mogelijkheid voor het toevoegen van automatische mails en taken.
21.	Aanpasbaarheid, eigen beheer van gebruikers, rechten en instellingen: Het systeem moet recruiters in staat stellen om de instellingen, gebruikersrechten aan te passen zonder tussenkomst van een functioneel beheerder binnen VRU, of van de leverancier. Het systeem moet voor recruiters zodanig aanpasbaar zijn, dat zij hun eigen voorkeuren kunnen instellen en het systeem kunnen aanpassen aan hun specifieke behoeften en werkstromen wanneer het proces hierom vraagt.
22.	Rollen en autorisaties: Het ATS moet de mogelijkheid bieden om verschillende toegangsniveaus in te stellen op basis van de rol van de gebruiker tijdens het werving- en selectieproces (bijvoorbeeld HR-medewerker, manager, afdeling communicatie, recruiter, deelnemer selectiecommissie), zodat gebruikers alleen toegang hebben tot de functies en informatie die relevant zijn voor hun taken.
23.	Rapportages: Gebruikers zijn in staat om uitgebreide rapporten en analyses te genereren over verschillende aspecten van het wervingsproces, zoals het aantal vacatures, de prestaties van vacatures, de bron van sollicitanten en de doorlooptijden.
24.	AVG-features: Het systeem biedt functionaliteit om te voldoen aan de AVG-wetgeving, zoals het beheren van toestemmingen, het anonimiseren van gegevens en het bijhouden van gegevensbewaartermijnen.

Niet-Functionele eisen

Gebruiksvriendelijkheid

#	Omschrijving
25.	Mobiele toegang: Het ATS is compatibel met mobiele apparaten, zodat gebruikers toegang hebben tot het systeem vanaf verschillende apparaten, zoals PC's, smartphones en tablets, voor flexibiliteit en gebruiksgemak. Het systeem is responsive.
26.	Gebruikersbegeleiding: Het ATS moet voorzien in gebruikersbegeleiding en ondersteuning, zoals tooltips, helpdocumentatie en trainingsmateriaal, om gebruikers te helpen bij het effectief gebruik van het systeem.
27.	Digitale toegankelijkheid: Van de opdrachtnemer wordt verwacht dat zij bij ontwerp, realisatie, oplevering en doorontwikkeling van de oplossing voldoet en blijft voldoen aan de EN 301 549 standaard die gebaseerd is op de actueel geldende Web Content Accessibility Guidelines (WCAG) van W3C. Op dit moment is dat WCAG 2.1 niveau AA.
28.	Schaalbaarheid en Prestaties: Het ATS moet in staat zijn om te gaan met de hierboven genoemde aantallen.

Integraties

#	Omschrijving
29.	Integratie: Het ATS moet integraties ondersteunen met VRU systemen zoals HRM-software in gebruik binnen VRU (AFAS), Microsoft 365, intranet, de internetsite vru.nl, sociale media (bijv. LinkedIn, Indeed) en carrièrewebistes, zodat gegevens naadloos kunnen worden uitgewisseld tussen verschillende platforms.
30.	Integratie mailbox en agenda: Het systeem biedt integratie met de Exchange Online omgeving van VRU, met een hogere authenticatie dan Basic. Zie ook functionele eis hierboven.
31.	Specifiek m.b.t. de koppeling met AFAS: Het ATS moet de mogelijkheid bieden om alle informatie m.b.t. de aangenomen kandidaten op een bepaald moment in het proces naadloos door te zetten naar het HR-systeem AFAS voor verdere verwerking.

Beschikbaarheid

#	Omschrijving
32.	Er kan 24 uur per dag en 7 dagen per week gebruik worden gemaakt van de oplossing. De beschikbaarheid van de oplossing is voor minimaal 99,9 %, gemeten per maand, gegarandeerd.

Informatiebeheer

#	Omschrijving
33.	De applicatie voldoet en blijft voldoen aan de geldende Archiefwet en daaruit voortvloeiende regelingen.
34.	De in de applicatie opgeslagen data blijft duurzaam toegankelijk gedurende de looptijd van de overeenkomst, e.e.a. conform dit Programma van Eisen, behoudens conform protocol vernietigde data.
35.	Informatieobjecten en bijbehorende metadata dienen onherstelbaar vernietigd te kunnen worden op basis van de als zoekcriteria (metadata) opgegeven waardering/vernietigingstermijn.

Continuïteit en conformiteit

#	Omschrijving
36.	De opdrachtnemer verplicht zich om in het geval van een calamiteit of ramp die de kritische processen van opdrachtnemer raakt, de afgesproken dienstverlening aan VRU binnen 48 uur te continueren. NB Deze eis heeft betrekking op de dienstverlening van opdrachtnemer, niet op de oplossing. Een calamiteit wordt in dit kader gedefinieerd als een ongewenste gebeurtenis die zodanige negatieve gevolgen heeft dat de voortgang van de kritische bedrijfsprocessen van de opdrachtnemer wordt verstoord en de maximale uitvalduur van deze kritische bedrijfsprocessen dreigt te worden overschreden.
37.	De opdrachtnemer garandeert d.m.v. backup & restore-procedures dat gegevensverlies maximaal 12 uur kan bedragen.
38.	De opdrachtnemer verplicht zich de data redundant op te slaan in geografisch gescheiden fysieke locaties. Deze locaties bevinden zich niet binnen dezelfde dijkkring.
39.	De opdrachtnemer houdt de aangeboden oplossing proactief in lijn met de landelijke afgesproken standaarden die betrekking hebben op ICT-standaarden.
40.	De aangeboden oplossing volgt de ontwikkelingen binnen moderne browser- technologie, zoals nu HTML5 en CSS3 evenals de toekomstige mogelijkheden en ontwikkelingen.
41.	Opdrachtnemer treft voldoende maatregelen teneinde continuïteit van de website te kunnen garanderen, zelfs in het geval waar normaliter een overmachtssituatie zou heersen (bijvoorbeeld bij rampen, calamiteiten, of faillissement van opdrachtnemer). In zulke situaties moet Opdrachtgever de mogelijkheid hebben om zelf, of door derden, beheer, onderhoud en ontwikkeling aan de website te laten plegen.
42.	De oplossing is toegankelijk en onafhankelijk van tijd en plaats (via bedrijfsnetwerk en direct-access) te gebruiken.
43.	Het is mogelijk individuele informatieobjecten vanuit de back-up te herstellen zonder dat de gehele inhoud van de oplossing teruggezet dient te worden.
44.	De oplossing is bereikbaar via IPv4 en IPv6.

Informatiebeveiliging

#	Omschrijving
45.	De opdrachtnemer maakt bij de opslag van persoonsgegevens gebruik van fysieke opslag en verwerking binnen de Europese Unie (EU) en zorgt ervoor dat doorgifte van gegevens naar landen buiten de Europese Unie uitgesloten is.
46.	Opdrachtnemer zorgt voor adequate functiescheiding en daarmee in overeenstemming zijnde Identity & Access Management zodat slechts bevoegd personeel toegang heeft tot de data. Daarbij zijn verschillende permissie/rechten-niveaus door de Opdrachtgever te configureren na oplevering.
47.	Opdrachtnemer is verantwoordelijk voor het gebruik, de behandeling, de bescherming en uitwisseling van vertrouwelijke gegevens die gedeeld worden met zijn onderaannemers. Daarbij is een door Opdrachtgever goedgekeurde verwerkingsovereenkomst van kracht voor opdrachtnemer en onderaannemers.

#	Omschrijving
48.	Opdrachtnemer zorgt voor minimaal 256 bits versleuteling volgens Advanced Encryption Standard (AES) voor opslag en transport van gevoelige gegevens.
49.	De opdrachtnemer treft maatregelen om de kans op hackeraanvallen en/of kwaadaardige software te minimaliseren, waaronder minimaal het in gebruik hebben en up-to-date houden van technologieën als firewalling, antivirus, IDS, IPS, hardening en encryptie.
50.	Opdrachtnemer zorgt voor patchmanagementbeleid, zodat alle ICT-componenten zijn gehard tegen aanvallen.
51.	De opdrachtnemer zorgt voor (fysieke en logische) toegangsbeveiliging en brand- en wateroverlastpreventie van de IT-systemen.
52.	De oplossing heeft en houdt tijdens de loop van het contract een 100% score op internet.nl
53.	Opdrachtnemer voldoet en blijft voldoen aan de eisen zoals geformuleerd door https://www.forumstandaardisatie.nl/open-standaarden waaronder het gebruik van HTTPS en HSTS voor webverkeer.
54.	De opdrachtnemer maakt gebruik van een door Opdrachtgever voorgeschreven SSL-certificaat.
55.	Alle door opdrachtnemer aangeboden diensten vallen binnen een door opdrachtnemer of zijn onderaannemers gebruikt ISMS (Information Security Management System), dat gecertificeerd is conform de ISO27001.
56.	De SoA (Statement of Applicability) van opdrachtnemer behorend bij de ISO27001 wordt voor VRU inzichtelijk gemaakt (evt. meegestuurd), of opdrachtnemer geeft inzicht in de relevante beheersmaatregelen die zijn ingesteld binnen zijn organisatie.
57.	De opdrachtnemer voert periodiek (minimaal 1x per jaar) een pentest en kwetsbaarheidenscan uit op de aangeboden omgevingen. Opdrachtnemer verschaft over de uitvoering en de resultaten een jaarlijkse rapportage aan de VRU.
58.	Eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. dergelijke beveiligingstest/-audits dienen te worden meegenomen bij de doorontwikkeling van de oplossing (als onderdeel van het onderhoud) en zo nodig op de kortst mogelijke termijn te worden gepatcht.
59.	Beveiligingspatches voor de oplossing worden zo snel als technisch mogelijk geïnstalleerd.
60.	In de rapportage over de dienstverlening is informatiebeveiliging een specifiek onderdeel. Bij het opstellen van de SLA wordt bepaald over welke KPI's er gerapporteerd wordt.
61.	Indien opdrachtnemer software ontwikkelt (zelf of via onderaannemers), hanteert opdrachtnemer aantoonbaar het principe "security by design" en "privacy by design".
62.	De webapplicaties die opdrachtnemer aanbiedt, zijn ingericht conform de richtlijnen van het NSCS (Nationaal Cyber Security Centrum) "ICT-Beveiligingsrichtlijnen voor Webapplicaties - Verdieping".
63.	Opdrachtnemer heeft met alle onderaannemers een contract met hierin een clause informatiebeveiliging/geheimhouding.
64.	Opdrachtnemer heeft een actieve incidentprocedure m.b.t. de communicatie rondom informatiebeveiligingsincidenten met haar klanten. De VRU wordt door de opdrachtnemer benaderd als zij een incident constateren.
65.	De VRU sluit met opdrachtnemer een verwerkersovereenkomst af die ook van toepassing is op eventuele onderaannemers van opdrachtnemer indien dit nodig mocht zijn als verwerker van persoonsgegevens.

#	Omschrijving
66.	De VRU heeft te allen tijde recht op het uitvoeren van een onafhankelijke externe audit op het gebied van informatiebeveiliging, of opdrachtnemer laat door een onafhankelijke externe partij een dergelijke audit uitvoeren (minimaal 1x per jaar) en deelt de uitkomst transparant met de VRU.
67.	In het rapport of de bijlage bij de uitkomst van de audit staat wat er is geconstateerd, welke maatregelen opdrachtnemer gaat nemen en binnen welke periode dit zal zijn uitgevoerd.
68.	Opdrachtnemer heeft een actieve procedure "meldplicht datalekken". Opdrachtnemer informeert de VRU hierover onmiddellijk na constateren en geeft aan welke eisen opdrachtnemer aan de VRU hierover stelt. Wanneer er sprake is van een datalek vanuit de oplossing door een lek in de software/programmatuur dan dient de opdrachtnemer hier direct actie op te ondernemen en de VRU hierop te attenderen. Indien de oorsprong van de oorzaak betrekking heeft op de infrastructuur van VRU dan zal de opdrachtnemer de VRU daarop direct moeten attenderen alsmede te adviseren wat de VRU daaraan kan doen.
69.	Opdrachtnemer overlegt eerst met de VRU in het geval opdrachtnemer een datalek constateert voordat opdrachtnemer een melding maakt bij de Autoriteit Persoonsgegevens (AP).
70.	Opdrachtnemer is in staat voor de afgenomen dienst voldoende logging beschikbaar te stellen voor het aanleveren van een audit trail in geval een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens (AP). Dit in overeenstemming met de Selectielijst gemeenten en intergemeentelijke organen 2020 en de BIO.
71.	In het geval van aanval/security breach dient opdrachtnemer verzamelde data ter beschikking te stellen. De data dienen na aanval nog beschikbaar te zijn. Opdrachtnemer stelt de verzamelde data beschikbaar voor eventueel onderzoek bij een derde partij. Dit in overeenstemming met de Selectielijst gemeenten en intergemeentelijke organen 2020 en de BIO.
72.	De VRU heeft toestemming de componenten/diensten die onderdeel zijn van dienstverlening van opdrachtnemer aan de VRU permanent op te nemen in kwetsbaarheden-scanners van VRU.
73.	De oplossing is voorzien van DDOS-bescherming.

Authenticatie en autorisaties

#	Omschrijving
74.	Het is mogelijk autorisaties in te richten per individuele gebruiker, per gebruikersgroep en/of per organisatieonderdeel.
75.	Het systeem heeft een helder rechten- en rollensysteem (toegang en autorisatie). Er moet voor aparte gedeeltes van de site apart lees- en/of schrijfrechten kunnen worden toegekend aan individuele (en groepen) gebruikers.
76.	Een gebruiker kan meerdere rollen hebben binnen de oplossing. Hij of zij kan toegang hebben tot meerdere autorisatieniveaus.
77.	Als de oplossing gebruik maakt van standaard autorisatirollen levert de opdrachtnemer een autorisatiematrix op, met daarin de standaardrollen en welke functies die rol mag uitvoeren b.v. invoeren, muteren, publiceren, verwijderen etc.
78.	Aan iedere gebruiker kunnen automatisch basis-autorisaties worden toegewezen.
79.	Het is mogelijk specifieke profielen/rollen in te richten voor autorisaties.

#	Omschrijving
80.	Voor gebruikers die bekend zijn in de Active Directory van de VRU die toegang zoeken tot de oplossing geldt “single sign-on” (SSO) via ADFS met behulp van SAML2 (SHA-2) of ADFS met behulp van OpenID Connect. Vanaf een VRU-werkplek wordt een gebruiker automatisch ingelogd zonder login prompt.
81.	Autorisaties kunnen door de functioneel-/applicatiebeheerders worden ingesteld, beheerd en gecontroleerd.
82.	Alle functionele beheertaken met betrekking tot de oplossing kunnen worden uitgevoerd terwijl gebruikers zijn ingelogd.
83.	Er kunnen voor de verschillende registratievormen door de beheerder specifieke registraties ingericht worden met eigen metadata. Hier kan dan ook een vaste vertrouwelijkheid op gezet worden.
84.	De oplossing dwingt het gebruik af van lange en/of complexe wachtwoorden (wachtwoord van minimaal 64 karakters moet mogelijk zijn). Gebruik van speciale tekens is hierbij vereist.
85.	De opdrachtnemer draagt zorg voor gebruikersauthenticatie alvorens gebruikers toegang tot de data verkrijgen. Hieronder verstaan wij een gebruikersnaam en sterk wachtwoord, conform het geldende VRU-wachtwoordbeleid.
86.	Binnen de aangeboden oplossing kan de beheerder een overzicht genereren van alle gebruikers met toegekende autorisaties.
87.	De mogelijkheid tot afdwingen van sterke wachtwoorden, conform het VRU-wachtwoordbeleid, is aanwezig.
88.	Eventuele niet-VRU gebruikers moeten de mogelijkheid hebben om ook gebruik te kunnen maken van Multi-Factor Authentication (MFA).
89.	Autorisaties op rollen en andere groepen kunnen genest worden. Dit betekent bijvoorbeeld dat een rol een andere rol kan bevatten. Voorbeeld: een redacteur kan algemene redactierechten hebben, maar ook rechten voor specifieke onderdelen van de website, terwijl een andere redacteur die rechten niet heeft, maar b.v. weer andere acties op de site kan doen.

Ondersteuning

#	Omschrijving
90.	De opdrachtnemer van de oplossing verzorgt een Nederlandstalige 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 8.00 uur tot 18.00 uur op werkdagen. In de SLA geeft inschrijver de omgang, respons- en oplostijden aan met aangemelde incidenten.
91.	De helpdesk is ook beschikbaar via een webportaal. 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.
92.	Van iedere melding is de prioriteit en voortgang zichtbaar. Een melding wordt alleen in overleg met de VRU gesloten.
93.	Opdrachtnemer hanteert een prioriteitenmethode of een andere methode waarbij er direct hulp wordt geboden bij incidenten met hoge impact en hoge urgentie, d.w.z. issues waarbij de oplossing niet werkt voor meer dan 1 persoon.

#	Omschrijving
94.	Opdrachtnemer verplicht zich ondersteuning te bieden aan de VRU (m.n. functionele beheerders) rondom het beheer en onderhoud van de functionaliteit van de oplossing en de daarin gebruikte bedrijfsinformatie, d.w.z. het instellen van de (functionele) parameters en de inhoud van databases.
95.	Opdrachtnemer verplicht zich ervoor te zorgen dat ondersteunende documentatie voor gebruikers en beheerders compleet, correct en up-to-date is.
96.	De opdrachtnemer biedt Nederlandstalige opleidingen en opleidingsdocumentatie aan. Deze zijn actueel en gebaseerd op de door de opdrachtnemer aangeboden versie van de oplossing. Dit geldt ook bij updates van de oplossing.
97.	De oplossing dient dusdanig eenvoudig en gebruikersvriendelijk te zijn dat er weinig tot geen opleiding voor een “eindgebruiker” noodzakelijk is. De opdrachtnemer biedt voor de eindgebruikers digitale uitleg voor die elementen die ingewikkelder blijken. Dit alles in afstemming met de VRU.
98.	De opdrachtnemer staat toe dat de digitale gebruikershandleiding van de oplossing wanneer niet beschikbaar via de oplossing) op het interne netwerk van de VRU beschikbaar wordt gesteld.
99.	De opdrachtnemer levert handleidingen en het opleidingsmateriaal op aan functioneel beheerder vóór de start van de implementatie.

Gunningscriteria:

1. Functionele wensen

1.	Omschrijving
1.	Notitieveld voor het invullen van achtergrondinformatie over de vacature n.a.v. de vacature intake.
2.	Sollicitantenervaring: Speciaal voor sollicitanten moet het sollicitatieproces binnen het ATS eenvoudig en gebruiksvriendelijk zijn. Dit omvat het gemakkelijk kunnen vinden en reageren op vacatures, een intuïtief sollicitatieformulier, duidelijke communicatie over de voortgang van de sollicitatie en een vriendelijke gebruikersinterface.
3.	Interne communicatie: Het systeem moet functies bevatten voor gemakkelijke communicatie tussen gebruikers, zoals het geven van beoordelingen, delen van notities, opmerkingen en feedback over kandidaten binnen het systeem
4.	Intuïtieve interface: Het ATS moet een intuïtieve en gemakkelijk te begrijpen interface hebben voor alle gebruikersgroepen. Dit betekent dat de navigatie logisch moet zijn en dat functies gemakkelijk toegankelijk moeten zijn.

2. Implementatieplan

#	Omschrijving
	De opdrachtnemer dient voor de uitvoering van het project een implementatieplan op te stellen.

3. Prijs