Volgnr.	ICT Eisen voor de levering van een Grondwatermonitoringsysteem	Eis/Wens
ICTe1	**GIBIT-Inkoopvoorwaarden**	
1	Opdrachtnemer gaat akkoord met de GIBIT-inkoopvoorwaarden van de gemeente Purmerend. De Gibit is leidend i.g.v. tegenstrijdigheden.	E
ICTe2	**SaaS oplossing Grondwatermonitoringsysteem**	
1	De opdrachtnemer garandeert dat gedurende de contractperiode de aangeboden oplossing wordt onderhouden, ondersteund en doorontwikkeld	E
2	Hosting betreft een voldoende beveiligde fysieke en logische omgeving – bestaande uit alle benodigde software (zoals virtualisatiesoftware, firewalls, technisch beheertooling en back-upsoftware) en hardware (zoals serverapparatuur, opslag, back-upapparatuur en netwerken) – beschikbaar stellen van het Grondwatermonitoringsysteem, inclusief het uitvoeren van het (technisch) beheer van deze omgeving.	E
3	Bij gebruikmaking van dataverbindingen d.m.v. Simkaarten en bijbehorende data-abonnementen is het mogelijk dat opdrachtgever deze kan leveren vanuit een lopende en bindende raamovereenkomst met een provider. Machine to Machine verbindingen zijn hierin uitgezonderd. In aanbieding dient u onderscheid te maken in door u geleverde of door opdrachtgever geleverde simkaarten tbv dataverbindingen	E
4	IPv4 en IPv6 dienen ondersteunt te worden en in staat zijn om te kunnen communiceren via IPv4-only, via IPv6-only en via dual-stack netwerken. Als de software netwerkparameters in haar lokale of remote server-instellingen bevat, dan moet de software ook de configuratie van IPv6-parameters ondersteunen. Alle functies die via IPv4 worden aangeboden moeten ook via IPv6 beschikbaar zijn. De opdrachtgever/eindgebruiker mag geen verschil ervaren wanneer de software via IPv4 of IPv6 communiceert, tenzij dit een expliciet voordeel voor de gebruiker oplevert. Het is niet toegestaan om vaste IPv6 adressen in de softwarecode op te nemen.	E
5	Het Grondwatermonitoringsysteem is een webbased oplossing en het front-end voor de medewerkers van de opdrachtgever bestaat uit een webapplicatie.	E
ICTe5	**Performance**	
1	De opdrachtnemer draagt zorgt voor een oplossing met voldoende (in praktijk gangbare en acceptabele) prestaties voor de eindgebruiker, hierbij moet worden uitgegaan van een normaal te verwachten concurrent eindgebruikers opdie die allen een voldoende gebruikerservaring hebben in gebruik van het systeem.	E
2	De opdrachtnemer voorkomt dat gebruik van gedeelde componenten door andere klanten in de infrastructuur de performance bedreigen.	E
ICTe6	**Wijzigingenbeheer geïnitieerd door opdrachtnemer**	
1	Wijzigingen door de opdrachtnemer doorgevoerd in de oplossing welke van invloed kunnen zijn op de data integriteit, informatieveiligheid, privacywetgeving, beschikbaarheid, toegankelijkheid, functionele werking, koppelvlakken, etc. worden vooraf besproken en goedgekeurd door de opdrachtgever. Wijzigingsprocedure met minimaal aandacht voor:	E
	- het administreren van significante wijzigingen (Release note)	E
	- impactanalyse van mogelijke gevolgen van de wijzigingen (Release note)	E
	- goedkeuringsprocedure voor wijzigingen	E
2	Alle wijzigingen worden door de opdrachtnemer altijd eerst getest voordat deze in productie worden genomen en worden via een wijzigingsprocedure doorgevoerd,	W
3	Relevante wijzigingen van de opdrachtnemer binnen de oplossing worden gelogd en zijn opvraagbaar door de opdrachtgever.	E
ICTe7	**Technische beveiliging**	
1	De opdrachtnemer zorgt voor een gedegen domeinscheiding tussen de oplossing van de opdrachtgever en andere domeinen.	E
2	De opdrachtnemer zorgt voor een oplossing verdeeld over meerdere geografisch gescheiden datacenters.	W
3	De opdrachtnemer hanteert een degelijk patchschema om alle componenten (zoals firmware, operating systems, applicaties) van de oplossing actueel te houden om verbeteringen door te voeren en bekende fouten op te lossen.	E

4	De opdrachtnemer geeft hoge prioriteit aan het snel installeren van de laatste beveiligingspatches.	E
5	De opdrachtnemer maakt gebruik van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen. Het realiseren hiervan leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillenden is te misbruiken.	E
6	Toegang tot de beheeromgeving van de oplossing voor medewerkers van de opdrachtgever is alleen mogelijk over een veilige verbinding.	W
7	Er wordt geen gebruik gemaakt van onbeveiligde internetverbindingen.	E
8	De opdrachtnemer zorgt ervoor dat opdrachtgever geen last heeft van onwenselijk gedrag van andere klanten (bijv. spamming vanuit eenzelfde IP-adres).	E
9	Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden. Oplossing voldoet aan de vereiste van het forum voor standaardisatie gedurende de looptijd van het contract.	E
10	De opdrachtnemer zorgt ervoor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door andere klanten die actief zijn binnen de systeemomgeving van opdrachtnemer.	E
11	De opdrachtnemer voert actief controles uit op systeemlogging.	E
12	Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig zijn, worden onmiddellijk gemeld aan en besproken met de opdrachtgever.	E
13	IT-voorzieningen en apparatuur bij opdrachtnemer zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen.	E
ICTe8	**Technisch beheer**	
1	Systeem en Technisch beheer wordt geheel verzorgd door opdrachtnemer.	E
2	Rollen en rechten van zowel de opdrachtnemer (technisch beheer) als de opdrachtgever (functioneel beheerders) zijn inzichtelijk. Gebruikers van opdrachtgever worden enkel aangemaakt door opdrachtnemer na opdracht van een bevoegd ambtenaar van de opdrachtgever.	E
3	Eindgebruikers hebben geen lokale administrator rechten nodig.	E
ICTe9	**Functioneel beheer**	
1	Voor het functioneel beheer van het systeem is geen programmeerkennis nodig (principe van klikken en niet tikken).	E
2	Het systeem voorziet in een scheiding tussen technisch- en functioneel beheer.	E
3	Voor het uitvoeren van functioneel beheer moet de functioneel beheerder zelf de autorisaties (rollen en rechten) en stamtabellen kunnen inrichten en beheren met begin- en einddatum en gebruikmakend van logfiles. Voorbeelden daarvan zijn het aanmaken en wijzigen van gebruikers, functierollen, stuur- en stamgegevens en het beheren van helpteksten.	E
4	De functioneel beheerder kan uit systeemlogging rapporten genereren. De oplossing beschikt over een niet-muteerbare audit-trail met daarin minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. Hierna kan deze worden verwijderd.	E
ICTe10	**OTAP-architectuur**	
1	De opdrachtnemer levert minimaal een gescheiden OTA en Productie omgeving + database(s) inclusief koppelingen. De opdrachtgever maakt gebruik van logisch gescheiden omgevingen.	W
2	De OTA-omgeving is voor zowel de beheerder als de gebruiker vrij te gebruiken.	W
3	Na de ingebruikname van de Productieomgeving zal de OTA-omgeving beschikbaar blijven als Testomgeving. De licentieverlening dient daarop zonder extra kosten voor de gemeente gebaseerd te zijn.	W
ICTe11	**Toegang Grondwatermonitoringsysteem via webapplicatie**	

1	De webapplicatie is resposive en toegankelijk en compatible met de meest recente browsers zoals hier opgesomd, en maximaal twee versies lager; a. Mozilla Firefox b. Google Chrome c. Safari d. Microsoft Edge	E
2	Voor een webbased applicatie gelden de onderstaande eisen: a. Volledig HTML5 ondersteuning, en b. Het gebruik van JAVA is niet toegestaan zonder toestemming vooraf van de opdrachtgever. c. Het gebruik van plug-ins is in afwijking op deze eis niet toegestaan zonder goedkeuring vooraf van de bevoegde ICT-manager van de opdrachtgever. d. Het gebruik van OpenGL of DirectX is niet toegestaan.	E
3	De toegang tot de webapplicatie maakt gebruik van een versleutelde (HTTPS) verbinding.	E
4	De webapplicatie controleert voor elk http-verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	E
5	De webapplicatie voldoet aan de beveiligingseisen die de NCSC/GOVCERT stelt aan de 5 kernpunten voor de beveiliging van webapplicaties: patching, invoervalidatie, uitvoervalidatie, sessieonderhoud, en databasegebruik. Zie hiervoor https://docplayer.nl/10466800-Checklist-beveiliging-webapplicaties.html	E
6	In geval van levering van een app dient deze te voldoen aan de actuele vereisten gesteld in de NCSC ICT-beveiligingsrichtlijn voor mobiele apps.	E
ICTe12	**Informatieveiligheid**	
1	De opdrachtnemer houdt zich aan alle wet- en regelgeving (Nederlandse en Europese) aangaande privacybescherming m.b.t. de door hem geleverde oplossing en diensten. Denk bijvoorbeeld aan rechten van betrokkenen, anonimiseren, dataminimalisatie, verwijderen van gegevens, bewaartermijnen, etc.. Alle wet- en regelgeving zoals de GDPR/AVG zijn leidend i.g.v. tegenstrijdigheden met andere eisen, wensen of voorstellen van opdrachtnemer.	**E**
2	De gegevens van opdrachtgever worden alleen in EER opgeslagen in overeenstemming met de eisen van de AVG.	E
3	Indien systeem persoonsgegevens verwerkt zal tussen de opdrachtgever en opdrachtnemer wordt een verwerkersovereenkomst afgesloten conform het 'model standaard verwerkersovereenkomst VNG'. Ten tijde van het afsluiten van de verwerkersovereenkomst zal door partijen de laatste versie van het ‘model standaard verwerkersovereenkomst VNG’ worden gebruikt.	E
4	De infrastructuur en organisatie van de inschrijver zijn adequaat beveiligd volgens ISO 27001:2017 of vergelijkbaar. Inschrijver is bij gunning gecertificeerd voor ISO 27001, of zal zijn gecertificering binnen een jaar na gunning van de opdracht. Gevraagde certificaten/rapportages dienen opgeleverd te worden als nederlandstalig document.	E
5	Vulnerability assessments (security scans) worden periodiek uitgevoerd (minimaal 1 x per jaar).	E
5.1	De opdrachtgever heeft toestemming om zelf een pentest te (laten) uitvoeren.	E
6	Rapportages omtrent de veiligheid van de oplossing worden gedeeld met de opdrachtgever.	E
7	De aangeboden oplossing legt een audit-trail vast over het gebruik van het Grondwatermonitoringsysteem	E
7.1	Deze audit trail bevat alle handelingen m.b.t. gebruikersautorisaties en functioneel gebruik (van medewerkers van opdrachtgever) van gevraagd systeem zoals raadplegen, aanmaken, muteren en verwijderen van informatie.	E
7.2	Vastlegging vindt minimaal plaats op gebruikersniveau en -rol, tijdstip en verrichte actie en is inzichtelijk voor zowel de functioneel beheerders als de CISO van de opdrachtgever.	E
7.3	Het systeem ondersteunt dat de logbestanden ten behoeve van de audittrail gedurende een door de opdrachtgever nader te bepalen periode bewaard worden waarna het mogelijk is deze uit het systeem te verwijderen.	E
8	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. worden vervangen.	E

9	De 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 direct aan de opdrachtgever worden gerapporteerd.	E
10	De opdrachtnemer verleent medewerking aan het uitoefenen van controle door of namens opdrachtgever op bewaring en gebruik van data en naleving van procedures.	E
11	De opdrachtnemer garandeert adequate backup- en restorevoorzieningen van de oplossing waarbij in geval van een gebeurtenis buiten de invloedsfeer van de opdrachtnemer (bijvoorbeeld een ramp of incident) de afgesproken dienstverlening binnen 48 uur kan worden gecontinueerd en waarbij het verlies van gegevens maximaal 1 werkdag kan bedragen.	E
12	In geval van toegang tot het Grondwatermonitoringsysteem vanuit het netwerk van opdrachtgever wordt gebruik gemaakt van SSO. In geval van toegang tot het Grondwatermonitoringsysteem van buiten het netwerk van opdrachtgever wordt gebruik gemaakt van multifactor authenticatie.	E
13	Als op het Grondwatermonitoringsysteem enkel vanaf het lokale netwerk ingelogd kan worden, dan dwingt het systeem een wachtwoord af van ten minste acht vrij te kiezen karakters waaronder het gebruik van een hoofdletter, cijfer en leesteken.	E
13.1	Het systeem dwingt 2 factor af voor inloggen vanaf buiten het netwerk opbasis van koppeling met ADFS van opdrachtgever	W
13.2	Er wordt gebruik gemaakt van Microsoft Authenticator indien er geen ADFS koppeling mogelijk is.	E
13.3	Het systeem ondersteunt het afdwingen van een maximale gebruiksduur van een wachtwoord. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.	E
13.4	De applicatie moet een functie hebben waarmee time-outs op het aantal foutieve inlogpogingen worden ondersteund. Onderscheid moet gemaakt kunnen worden tussen het inloggen vanaf het lokale netwerk of vanaf het internet. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.	E
13.5	De applicatie moet gebruikers en beheerders de mogelijkheid geven om hun wachtwoord te kunnen wijzigen. Beheerders van de opdrachtgever moeten de wachtwoorden van gebruikers kunnen wijzigen.	E
13.6	Het gebruik van de wachtwoorden van het Grondwatermonitoringsysteem in de organisatie moet door beheerdersaccounts gecontroleerd/beheerd kunnen worden.	E
13.7	Indien Grondwatermonitoringsysteem van buiten ons netwerk benaderbaar is, dan moet de applicatie zichzelf na een door opdrachtgever in te stellen termijn aan in-activiteit vergrendelen.	E
13.8	Wachtwoorden in het Grondwatermonitoringsysteem worden nooit in plaintext opgeslagen of verstuurd.	E
13.9	Het Grondwatermonitoringsysteem forceert een verandering van wachtwoord bij het eerste gebruik (ingebruikname) van het systeem door indivuele gebruikers. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT-manager van opdrachtgever, worden afgeweken.	E
14	Het Grondwatermonitoringsysteem voldoet aan de actuele vereisten gesteld in de NCSC beveiligingsrichtlijnen voor webapplicaties.	E
15	Het systeem voldoet aan de vereisten die de AVG en de archiefwet stelt.	E
16	Voor veilige bestandsuitwisseling via email tussen opdrachtgever en opdrachtnemer accepteert opdrachtnemer de oplossing die opdrachtgever biedt (op dit moment Zivver). Indien leverancier een oplossing ter beschikking heeft kan dit na goedkeuring van bevoegd ICT-manager van de opdrachtgever als alternatief dienen.	E
ICTe13	**Koppelvlakken**	
1	Er is een actief LDAP (AD-FS) koppelvlak met de AD van de opdrachtgever voor gebruikersbeheer (gebruiker, inlognaam en wachtwoord, account active/ disabled).	toelichting

1.1	Opdrachtnemer ondersteunt het gebruik van AD Authenticatie ADFS staat voor Active Directory Federation-services, is een oplossing van Microsoft voor Single sign-on en web-gebaseerde authenticatie voor systemen en applicaties. De opdrachtgever maakt gebruik van Microsoft ADFS i.c.m. met Azure Multi-Factor Authentication. Protocollen die hierbij worden ondersteund zijn: • OpenID Connect (voorkeur) • OAuth (voorkeur) • WS-Federation, • WS-Trust, • SAML	toelichting
2	Indien van toepoassing oorganiseerd de opdrachtnemer de afstemming en realisatie van de koppelingen (gegevensuitwisseling) met andere noodzakelijke applicaties van de opdrachtgever. De opdrachtgever heeft een ondersteunende rol	E
3	De opdrachtgever maakt gebruik van Cognos voor BI-toepassingen en het Grondwatermonitoringsysteem dient deze te ondersteunen. Andere rapportagetools zijn in afwijking op deze eis alleen toegestaan na een akkoord vooraf van de bevoegd Teammanager ICT.	E
3.1	De applicatie ondersteunt Microsoft Office; Excel voor het exporteren en importeren van gegevens van en naar Excel en rapportages naar Word. De extensies .doc en .xls worden niet geaccepteerd. De opdrachtgever maakt gebruik van MS Office, het Grondwatermonitoringsysteem moet hiermee compatible zijn.	E
3.2	Indien van toepassing wordt de email functie van Outlook 365 (Exchange Online) ondersteund met gebruikmaking van de Microsoft Graph API. (EWS als protocol kan nu nog tijdelijk in afwijking op de eis van Graph worden ondersteund maar alleen toegestaan na een akkoord vooraf van de bevoegd manager ICT.	E
4	De in de applicatie opgeslagen data is zonder tussenkomst van de opdrachtnemer direct benaderbaar voor bevraging door de opdrachtgever (b.v. door het publiceren van beveiligde API's)	E
5	Voor gebruik van Azure SQL gelden de volgende voorwaarden: De database wordt beveiligd door een firewall(rules) zodanig dat deze alleen door de applicatie kan worden benaderd, volgens de actuele best practices van Microsoft. • IP-filtering • Authenticatie • Beperkte toegang tot dataset	E
5.1	Voor oplossingen die van buiten benaderbaar zijn gelden TEVENS de eisen genoemd in de ICT Beveiligingsrichtlijnen voor webapplicaties van het NCSC. In het bijzonder hoofdstuk Uitvoeringsdomein>>Webapplicaties.	E
ICTe15	**Architectuur**	
1	Opdrachtnemer levert technische architectuurplaten van de oplossing en houdt deze gedurende de overeenkomst actueel.	E
1.1	De opdrachtnemer levert een technische architectuurplaat op hoofdlijnen met alle componenten, koppelvlakken, disaster/recovery en uitwijk (geografisch gescheiden datacenters).	E
2	De opdrachtnemer levert voor de oplevering minimaal de volgende documentatie: a. de architectuur van de applicatie b. datamodelspecificatie van de koppelvlakken	E
ICTe16	**Support SLA**	
1	Medewerkers van opdrachtnemer bieden ondersteuning in de Nederlandse taal in woord en geschrift.	E
2	Opdrachtnemer levert voor de oplevering in de productieomgeving een Nederlandstalige handleiding voor de medewerkers van de opdrachtgever op.	E
3	Opdrachtnemer beschikt over een helpdesk welke medewerkers van de opdrachtgever van maandag tot en met vrijdag van 8:00 tot 17:00 per telefoon te woord kan staan.	E
4	Opdrachtnemer conformeert zich aan de gestelde eisen tot het handelen bij verstoringen. Voorbeeld zie Werkblad 'Vereisten bij verstoringen'' Dit tabblad dient in alle procdures ingevuld te worden en meegestuurd. NB deze eis moet afgestemd met de opdrachtgever	E

5	Opdrachtnemer is verantwoordelijk voor het aanleveren en actueel houden van een contactenmatrix op functieniveau van alle betrokken medewerkers van zowel de opdrachtnemer als de opdrachtgever.	E
ICTe17	**Opleiding**	
1	De opdrachtnemer biedt inhouse (op locatie gemeente Purmerend) gebruikerstrainingen voor zowel functioneel beheerders als eindgebruikers.	W
2	Trainingen worden in het Nederlands gegeven; documentatie is in het Nederlands beschikbaar.	E
ICTe18	**Overdracht gegevens/data bij beëindiging overeenkomst**	
1	Alle gegevens in Grondwatermonitoringsysteem zijn en blijven te allen tijde eigendom van opdrachtgever en mogen door opdrachtnemer niet voor andere doeleinden worden gebruikt. Bij beëindiging van de overeenkomst worden alle gegevens overgedragen aan de opdrachtgever in een standaard uitwisselformaat.	E