

Bijlage 6 Programma van Eisen

1.1 Algemene eisen

	Inhoud
1.1	Inschrijver draagt zorg voor een voor VRZHZ naadloze overgang van huidige de dienstverlener naar Inschrijver, zonder dat de website ZHZveilig.nl en de huidige AlertServer tijdens de transitie (en ingebruikname van het CICT) op enig moment niet bereikbaar is voor de buitenwereld.
1.2	De website ZHZveilig.nl en het CICT voldoen aan de Functionele beschrijving zoals opgenomen in de bijlagen.
1.3	Inschrijver werkt op basis van resultaatverplichting
1.4	Alle in het kader van dit project gebouwde programmatuur, content en maatwerkfunctionaliteit, inclusief auteursrechten en intellectueel eigendom, voor zover deze rechten niet bij derden liggen, worden direct bij de ontwikkeling eigendom van de VRZHZ. Sources, code(s), documentatie, databases, content en statistieken blijven te allen tijde eigendom van VRZHZ.
1.5	Inschrijver zorgt te allen tijde voor de goede werking en performance van de website ZHZveilig.nl en het CICT.
1.6	Inschrijver levert en beheert een Test- en Productie omgeving, waarbij Inschrijver een gangbare change management methode hanteert. De impact van veranderingen op bestaande functionaliteiten worden uitvoerig getest op basis van gezamenlijk vast te stellen acceptie- en testcriteria. Inschrijver neemt bij aanvang van de Opdracht initiatief voor het opstellen van deze criteria.
1.7	Alle relevante zaken op het gebied van hosting, Systeem en technisch applicatiebeheer, onderhoud en ontwikkeling zijn adequaat gedocumenteerd en zijn bij oplevering voorzien van adequate handleidingen. Documentatie en handleidingen staan te allen tijde, zowel tijdens als na de contractuur, ter beschikking van VRZHZ. Bij iedere wijziging wordt de documentatie door Inschrijver geactualiseerd.
1.8	Webredacteuren / contentbeheerders van de VRZHZ kunnen te allen tijde gewenste content toevoegen of aanpassen op een gebruiksvriendelijke manier via een Dummy-proof CMS – systeem dat toegankelijk is voor gemiddelde communicatiemedewerker zonder html of javascript kennis.
1.9	Kosten voor hosting en beheer (incl. Btw) worden in rekening gebracht vanaf 01-01-2024.

1.2 *Ontwikkeling*

	Inhoud
2.1	Inschrijver voert alle testen tot functionele acceptatietest uit. Vanaf functionele acceptatietest valt het testen onder de verantwoordelijkheid van VRZHZ.
2.2	Inschrijver plant de benodigde testcapaciteit adequaat in conform VRZHZ's processen en tijdslijnen. Testplannen en testprotocol worden door de Inschrijver aangeleverd en i.s.m. de VRZHZ definitief vastgesteld.
2.3	Herstelwerkzaamheden naar aanleiding van uitgevoerde testen vallen onder de verantwoordelijkheid van de Inschrijver.
2.4	De code dient conform geldende "best practices" programmeerstandaarden (genormaliseerd, modulair, goede documentatie) opgebouwd te worden.

1.3 *Architectuur eisen*

	Inhoud
3.1	Nieuw te ontwikkelen software dient zich te houden aan de architectuurprincipes conform de VERA 2.0. Bij nieuwe ontwikkelingen dient contact te worden opgenomen met de VRZHZ over architectuur om te toetsen of de nieuwe ontwikkelen past binnen architectuur principes, beleidslijnen, modellen en standaarden zie hiervoor https://www.veraonline.nl/
3.2	Inschrijver ontwikkelt uitsluitend maatwerkfunctionaliteit indien de standaardfunctionaliteit naar mening van de VRZHZ niet voldoet en uitsluitend na goedkeuring van de VRZHZ.
3.3	De gehele oplossing kent een architectuurmodel waarin het mogelijk is om inhoud van andere systemen te hergebruiken of inhoud voor andere systemen beschikbaar te stellen.
3.4	De gehele oplossing van het Risico- en crisiscommunicatie platform kent een architectuurmodel waarin gebruik wordt gemaakt van standaard koppelvlakken.
3.5	De functionaliteiten voldoen aan de wettelijke vereisten voor informatiebeveiliging en de standaard NEN 27001.
3.6	De website ZHZVeilig.nl, CICT en nieuw te ontwikkelen functionaliteiten voldoen aan vigerende Europese wet- en regelgeving en houdt rekening met Europese wet- en regelgeving met betrekking tot bescherming persoonsgegevens, borging van privacy, als ook rechten tot inzage en wijziging van personen met betrekking tot hun eigen persoonsgegevens (AVG/GDPR).

	Inhoud
3.7	Inschrijver laat jaarlijks een Attack & Penetration Test uitvoeren door een (hierin gespecialiseerde) onafhankelijke externe partij, rapporteert de bevindingen hiervan en past zijn systemen indien nodig aan. De auditkosten zijn voor de VRZHZ tenzij er uit de audit blijkt dat er dusdanige verwijtbare fouten gemaakt zijn, dan komen deze kosten (audit- en herstelkosten) voor rekening van Inschrijver. Deze kosten maken geen onderdeel uit van de jaarlijkse contractkosten. Uitkomsten uit kwetsbaarheidsscans en pentesten worden één op één met de VRZHZ gedeeld. Eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. dergelijke beveiligingstest/-audits dienen te worden meegenomen bij de doorontwikkeling van de websites (als onderdeel van het onderhoud) en zo nodig op de kortst mogelijke termijn te worden gepatcht.
3.9	Inschrijver zorgt voor adequate functiescheiding en daarmee in overeenstemming zijnde Identity & Acces Management zodat slechts bevoegd personeel toegang heeft tot de data. Daarbij zijn verschillende permissie/rechten niveaus door de VRZHZ te configureren na oplevering.
3.10	Voor gebruikers die bekend zijn in de Active Directory van de VRZHZ 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 VRZHZ werkplek wordt een gebruiker automatisch ingelogd zonder login prompt.
3.11	De Inschrijver draagt zorg voor gebruikersauthenticatie alvorens gebruikers toegang tot de data verkrijgen. Hieronder verstaan wij een gebruikersnaam en sterk wachtwoord, conform het geldende VRZHZ-wachtwoordbeleid.
3.12	De oplossing voorziet naast de genoemde SSO methodiek tevens in een alternatieve authenticatiemethode voor gebruikers op basis van een gebruikersnaam en wachtwoord. De mogelijkheid tot afdwingen van sterke wachtwoorden, conform het VRZHZ-wachtwoordbeleid, is aanwezig.

1.4 **Techniek**

	Inhoud
4.1	Het Risico- en crisiscommunicatie platform dient op basis van een proven concept, met name op de eisen voor de piekbelasting en de 24/7 beschikbaarheid, beschikbaar te zijn.
4.2	Er wordt gewerkt met open standaarden zie https://www.forumstandaardisatie.nl/open-standaarden (sectie verplicht, aanbevolen).

1.5 **Beheer**

	Inhoud
5.1	Inschrijver verzorgt het technisch applicatiebeheer en het systeembeheer van het platform conform de KPI's (in de SLA) en de afspraken in de (DAP)
5.2	Reguliere updates en module updates worden in samenspraak met de VRZHZ, als vastgesteld in de DAP, uitgevoerd.
5.3	Wijzigingen/ aanpassingen worden via een gescheiden Test en Productieomgeving, als vastgesteld in de DAP, uitgevoerd. VRZHZ kondigt ruim van tevoren aan wanneer een oefening wordt uitgevoerd
5.4	Inschrijver heeft een ingericht service portaal waar de VRZHZ 24/7 problemen en opdrachten kan melden. Tevens kan in dit portaal de voortgang van deze incidenten en wijzigingsmeldingen digitaal worden geraadpleegd en gevolgd.
5.5	Naast het service portaal verzorgt de Inschrijver een servicedesk, 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 9.00 uur tot 18.00 uur op werkdagen. Buiten deze tijden wordt een calamiteitenregeling door Inschrijver beschikbaar gesteld.

1.6 **Beschikbaarheid**

Inhoud																								
6.1	Geplande downtime van de website ZHZVeilig.nl bij voorkeur op maandagochtenden tussen 5.00 en 7.00 uur. Communicatie en uitvoer wordt in de DAP vastgesteld. Het Risico- en crisiscommunicatie platform is 24/7 beschikbaar waarbij de volgende beschikbaarheid uitgangspunten gelden: Inschrijver conformeert zich bij het bepalen van de prioriteringen van verstoringen aan ZHZVeilig.nl aan de onderstaande beschrijvingen. <table><tr><td colspan="2"></td><td colspan="2">Urgentie</td></tr><tr><td colspan="2"></td><td>Hoog</td><td>Laag</td></tr><tr><td rowspan="2">Impact</td><td>Hoog</td><td>Prioriteit 1</td><td>Prioriteit 2</td></tr><tr><td>Laag</td><td>Prioriteit 2</td><td>Prioriteit 3</td></tr></table> <table><tr><th>Prioriteit</th><th>Beschrijving</th></tr><tr><td>1</td><td>de software en/ of content en/of dienstverlening is in het geheel niet beschikbaar en dit dient direct te worden hersteld. Beveiligingsincidenten (fout of lek in de beveiliging) vallen eveneens onder deze prioriteit</td></tr><tr><td>2</td><td>onderdelen van de software en/of content en/of dienstverlening zijn niet of substantieel minder beschikbaar Indien een datalek geconstateerd wordt.</td></tr><tr><td>3</td><td>informatievragen, opmerkingen, klachten.</td></tr></table>			Urgentie				Hoog	Laag	Impact	Hoog	Prioriteit 1	Prioriteit 2	Laag	Prioriteit 2	Prioriteit 3	Prioriteit	Beschrijving	1	de software en/ of content en/of dienstverlening is in het geheel niet beschikbaar en dit dient direct te worden hersteld. Beveiligingsincidenten (fout of lek in de beveiliging) vallen eveneens onder deze prioriteit	2	onderdelen van de software en/of content en/of dienstverlening zijn niet of substantieel minder beschikbaar Indien een datalek geconstateerd wordt.	3	informatievragen, opmerkingen, klachten.
		Urgentie																						
		Hoog	Laag																					
Impact	Hoog	Prioriteit 1	Prioriteit 2																					
	Laag	Prioriteit 2	Prioriteit 3																					
Prioriteit	Beschrijving																							
1	de software en/ of content en/of dienstverlening is in het geheel niet beschikbaar en dit dient direct te worden hersteld. Beveiligingsincidenten (fout of lek in de beveiliging) vallen eveneens onder deze prioriteit																							
2	onderdelen van de software en/of content en/of dienstverlening zijn niet of substantieel minder beschikbaar Indien een datalek geconstateerd wordt.																							
3	informatievragen, opmerkingen, klachten.																							

	Inhoud		
	Website ZHZVeilig.nl		
	Prioriteit	Maximale responstijd	Oplossingstermijn
	1	30 minuten	Work-around binnen 4 uur
	2	2 uur	Oplossing binnen 8 uur
	3	1 werkweek	Work-around binnen 8 uur
	Crisis / Incident Communicatie Tool (CICT)		
	Prioriteit	Maximale responstijd	Oplossingstermijn
	1	10 minuten	Work-around 24/7 binnen 15 minuten
	2	10 minuten	Oplossing binnen 4 uur
	3	1 werkweek	Work-around 24/7 binnen 30 minuten
Maximale responstijd is de tijd waarbinnen de melding door VRZHZ gedaan wordt en door Inschrijver gestart wordt met het zoeken van een oplossing. Oplossingstermijn is de tijd, na melding door VRZHZ, waarbinnen een oplossing of werkbare work-around, door Inschrijver, tot stand komt en geaccepteerd is door de VRZHZ.			
6.2	Werkzaamheden aan het Risico- en crisiscommunicatie platform mogen de beschikbaarheid van de CICT niet beïnvloeden. M.a.w. onderhoud mag niet leiden tot downtime. Releasematig onderhoud wordt altijd gefaseerd uitgevoerd op een testomgeving en kent (in geval van eventuele aanpassing van interfaces van doelsystemen) een bouwfase , testfase, acceptatiefase, en in productie name fase.		

1.7 Communicatie

	Inhoud
7.1	Inschrijver wijst één vaste contactpersoon aan welke als eerste aanspreekpunt voor VRZHZ fungeert.
7.2	Opdrachtnemer informeert VRZHZ tijdig indien er sprake is van opvolging, dan wel vervanging van de vaste contactpersoon, echter uiterlijk één (1) maand van tevoren. Bij tijdelijke afwezigheid van de vaste contactpersoon vanwege bijvoorbeeld vakantie of ziekte wordt er te allen tijde een vervanger aangesteld die bekend is met VRZHZ en de gemaakte afspraken. VRZHZ zorgt voor een vervangend contactpersoon indien de samenwerking naar het oordeel van VRZHZ niet goed verloopt.

	Inhoud
7.3	Op gezette tijden zullen er overleggen gehouden worden tussen Inschrijver en VRZHZ. Inschrijver neemt hiertoe initiatief: 1. Beoordeling en voortgang op gemaakte contractafspraken in het SLA. 2. Een keer per jaar (uiterlijk 4 maanden voor het einde van het eerste contractjaar en de daaropvolgende jaren van de Raamovereenkomst), dient een strategisch overleg plaats te vinden tussen Inschrijver en VRZHZ. 3. Tijdens het jaarlijks overleg worden in ieder geval de volgende onderwerpen besproken: a) Evalueren van en zoeken naar oplossingen voor structurele problemen; b) Ontwikkelen en realiseren van ideeën gericht op bijv.: innovatie/ kostenverlaging; c) Vaststellen ontwikkelafspraken voor de komende periode/ contractjaar; d) Servicelevelrapportage 4. Veranderingen in de organisatie, zowel bij VRZHZ als bij Inschrijver; 5. Optie tot verlenging van de Overeenkomst. VRZHZ heeft het recht om de voornoemde termijnen in overleg met Inschrijver indien noodzakelijk te wijzigen.
7.4	Inschrijver rapporteert aan de VRZHZ over de in de SLA overeengekomen servicelevels en KPI's. Periodiek wordt gerapporteerd over de afgesproken indicatoren met aggregatieniveau van 1 kalendermaand, bijv. • Beschikbaarheid Risico- en crisiscommunicatie platform • Aantal calls, openstaand en afgehandeld; • Hoeveelheid gemelde incidenten, classificatie en oplostijden verdeeld naar categorie; • Aantal escalaties, inclusief evaluatie. • P1 storingen inclusief opvolging en geleerde lessen

1.8 **Design aanpassingen**

	Inhoud
8.1	Inschrijver geeft, door middel van het invullen van de Bijlage 10 Prijzenblad ZHZVeilig 'Prijzen' een gedetailleerd inzicht in de voor deze opdracht te hanteren prijzen en tarieven.
8.2	Meertaligheid is een eis die tijdens fase 1 van de bouw van de nieuwe website verwerkt moet worden. In eerste instantie moet de site te benaderen zijn in het Nederlands. In een volgende fase zullen ook meerdere talen in overweging worden meegenomen. In fase 1 al wel de techniek hierop voorbereiden, zodat het slechts een implementatie proces is om meer talen toe te voegen in fase 2.

1.9 Prijzen/tarieven

	Inhoud
9.1	Inschrijver geeft, door middel van het invullen van de Bijlage 10 Prijzenblad ZHZVeilig een gedetailleerd inzicht in de voor deze opdracht te hanteren prijzen en tarieven.
9.2	De prijs dient/de tarieven dienen 'all-in' te zijn. Facturatie van additionele kosten is niet toegestaan. Daaronder zijn bijvoorbeeld, maar niet uitsluitend, begrepen: de salariskosten, de overheadkosten (als onder meer huisvesting en salariskosten van niet productief personeel), de kosten voor ondersteunend werk, de kosten voor het gebruik van apparatuur (als onder meer pc's, die worden gemaakt ten gevolge van de opdracht en de winst, de verzekeringskosten, reis- en verblijfkosten, etc. De tarieven dienen te worden uitgedrukt in euro's.
9.3	De opgegeven prijzen bij 'implementatie' zijn op basis van fixed-price.

1.10 (Informatie)veiligheid

	Inhoud
10.1	Accounts: Er zijn verschillende gebruikersrollen met rechten Contentbeheer website Contentbeheer CICT en Gebruikers CICT(woordvoerders) De rollen en rechten worden toegewezen aan de hand van een autorisatiematrix.
10.2	Alle door u aangeboden diensten vallen binnen een door u (of uw subcontractors) gecertificeerd ISMS (Information Security Management System) conform de ISO27001.
10.3	Uw SoA (Statement of Applicability) behorend bij de ISO27001 is voor ons inzichtelijk (meegestuurd) of u geeft inzicht in de relevante beheersmaatregelen die u heeft ingesteld binnen uw organisatie.
10.4	Indien u software ontwikkelt (zelf of via subcontractors) hanteert u aantoonbaar het principe "security by design".
10.5	De Test- en productieomgeving van het Risico- en crisiscommunicatie platform zijn ingericht conform de richtlijnen van het NCSC (Nationaal Cyber Security Centrum) "ICT-Beveiligingsrichtlijnen voor Webapplicaties - Verdieping".
10.6	U heeft met al uw onderaannemers een contract met hierin een clause informatiebeveiliging/geheimhouding.
10.7	U heeft een actieve crisisprocedure m.b.t. de communicatie rondom informatiebeveiliging crisissen met uw klanten.
10.8	U heeft (indien nodig) een actieve procedure "meldplicht datalekken", u informeert ons over welke eisen u aan ons hierover stelt.

	Inhoud
10.9	Indien Inschrijver een datalek, welke betrekking heeft op onze omgeving, constateert informeert Inschrijver met VRZHZ via privacy@vrzhz.nl voordat Inschrijver een melding maakt bij de Autoriteit Persoonsgegevens (AP).
10.10	U bent in staat voor de afgenomen dienst voldoende logging beschikbaar te stellen voor het aanleveren van een audittrail in geval een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens (AP) (specificeer wat u hiervoor heeft ingericht)
10.11	Voor archivering van de website moet de site beschikbaar zijn voor dagelijkse harvesting door archiefweb.eu
10.12	In het geval van aanval/security breach dient de Inschrijver verzamelde data ter beschikking stellen. De data dient minimaal 60 dagen na aanval nog beschikbaar te zijn. U stelt de verzamelde data beschikbaar voor eventueel onderzoek bij een derde partij.
10.13	Dataverkeer: het dataverkeer moet versleuteld zijn, minimaal TLS1.2.
10.14	De Inschrijver maakt bij de opslag van persoonsgegevens gebruik van fysieke opslag en verwerking binnen de Europese Unie (EER) en zorgt ervoor dat doorgifte van gegevens naar landen buiten de EER uitgesloten is.
10.15	Inschrijver 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.
10.16	De VRZHZ 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.
10.17	De oplossing is voorzien van DDOS bescherming.
10.18	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.