

Bijlage 1 Programma van Eisen

Toelichting: in deze bijlage moeten de minimeisen worden opgenomen die het NIPV stelt aan de opdracht. De onderwerpen kunnen worden aangepast naar wens.

Geschiktheidseisen:

1. Kwaliteitsmanagementsysteem: ISO9001 of vergelijkbaar
2. Business Continuity Management ISO22301
3. Certificering Milieubeheer/ Duurzaam hosting ISO14001 of vergelijkbaar
4. Informatiebeveiliging: ISO27001 of vergelijkbaar
5. Informatiebeveiliging: BIO-compliance
6. Clouddiensten: ISO 27017 certificering, een SOC 2 type 2 verklaring en een ISAE3402 verklaring.
7. Optioneel: ISA E3402 Type II

Toelichting:

In deze bijlage staan de minimeisen opgenomen die Opdrachtgever stelt aan de opdracht. Dit zijn Knock-outeisen. Aan deze eisen dient Opdrachtnemer minimaal te voldoen om in aanmerking te komen voor beoordeling van de offerte van Opdrachtnemer.

Nr.	Algemene eisen	NIPV	BRW
1.	Opdrachtnemer is in staat om per 15 november 2026 de websiteomgeving van het NIPV in beheer te nemen.	x	x
2.	Opdrachtnemer levert haar diensten en documenten te allen tijde in de Nederlandse taal tenzij daar per situatie in overleg met het NIPV van mag worden afgeweken.	x	x
3.	Opdrachtnemer voert bij aanvang van de opdracht een due diligence uit op de bestaande websiteomgeving van opdrachtgever en deelt hiervan de resultaten en risico's met de opdrachtgever		x
4.	Opdrachtnemer neemt de huidige website-omgevingen as-is (OTAP) over van de huidige leverancier en migreert deze vóór 15 november 2026 naar een door Opdrachtnemer te leveren Public Cloudhostingomgeving.	x	x
5.	Opdrachtnemer doorloopt met het NIPV na deze migratie een acceptatietest op basis van nader overeen te komen acceptatiecriteria om de juiste en volledige werking van de huidige website-omgevingen as-is in de nieuwe Cloudhostingomgeving te verifiëren.	x	x
6.	Opdrachtnemer ondersteunt actief de aanpassing van alle DNS-settings en overige instellingen om de bestaande websites vanuit de nieuwe omgeving te ontsluiten.	x	x

7.	Opdrachtnemer verzorgt vanaf de Acceptatie doorlopend het Functioneel en Technisch beheer tenminste op basis van de Service Levels zoals deze in het voorbeeld Functioneel Beheer Service Level Agreement (SLA) zijn aangeleverd.	x	x
8.	Opdrachtnemer richt haar servicemanagement in overleg met Functioneel Beheer en de projectleider(s) in op basis van de servicemanagementomgeving van Opdrachtgever.	x	x
9.	De leverancier beschikt minimaal en aantoonbaar over de volgende expertises: Digitale Toegankelijkheid, gebruiksvriendelijkheid, vindbaarheid en (online) marketing. En kan website opleveren/onderhouden die voldoen aan de regels voor digitale toegankelijkheid waar overheidswebsites aan dienen te voldoen.	x	x

Nr.	Content Management systeem	NIPV	BRW
10.	De bestaande multi-site omgeving wordt as-is overgenomen en beheerd binnen het bestaande CMS.	x	x
11.	De bestaande multi-site omgeving wordt overgenomen zonder onderbreking voor de eindgebruiker	x	x
12.	De bestaande multi-site omgeving wordt overgenomen op basis van de benodigde gegevens (toegang en inloggegevens, bestanden en database, licenties en abonnementen voor plugins, documentatie, etc.)	x	x
13.	De opdrachtnemer beschikt over aantoonbare kennis en capaciteit om nieuwe subsites aan te maken binnen de huidige multi-site omgevings. Deze subsites kunnen in huisstijl en functionaliteiten afwijken van NIPV.nl/Brandweer.nl.	x	x

Nr.	Plug-ins, functionaliteiten en nieuwe ontwikkelingen	NIPV	BRW
	<i>Onder een plug-in verstaat het NIPV in WordPress beschikbare functionaliteiten die door de beoogde redactie en functioneel beheer kunnen worden gebruikt voor onderhoud, beheer, redactie, publicatie, koppeling en optimalisatie van de website.</i>		
14.	De opdrachtnemer heeft ervaring met het beheer, updaten en modificeren van de volgende plug-ins: 1. ACF Content Analysis voor Yoast SEO & Better Search 2. Advanced Custom Fields PRO & Gravity Forms Add-on 3. Comaxx Cookie Banner 4. Comaxx LiveBlog 5. ComaxxEduframe	x	

	6. ElasticPress 7. GravityForms & reCAPTCHA add-on 8. Imagify & Imagify Skip PDF Auto-Optimization 9. Publishpress Capabilities 10. Spotler Mail+ Forms 11. TablePress 12. Ubeeo ATS 13. Under Construction 14. WP Mail SMTP 15. WP Rocket 16. WPS Hide Login 17. Yoast Duplicate post 18. Yoast SEO & Yoast SEO Premium		
15.	De opdrachtnemer heeft ervaring met het beheer, updaten en modifieren van de volgende plug-ins: Zie bijlage 1A voor de plugins van brandweer.nl en subsites.		x
16.	Opdrachtnemer maakt voor nieuwe functionaliteiten waar mogelijk altijd gebruik van standaard Wordpress-approved oplossingen.	x	x
17.	Nieuwe plug-ins en functionaliteiten worden geleverd volgens de meest recente Digitale Toegankelijkheidsrichtlijnen. Opdrachtnemer neemt deze eisen proactief mee in de offerring en tijdens implementatie (WCAG 2.1 niveau AA).	x	
18.	Opdrachtnemer beschikt over de kennis en kunde om nieuwe plug-ins en functionaliteiten per subsite te modifieren.	x	
19.	Bij het testen van (nieuwe) plug-ins en functionaliteiten waar persoonsgegevens voor vereist zijn, maakt opdrachtnemer geen gebruik van productiedata. Gebruikte persoonsgegevens die nodig zijn voor testen worden geanonimiseerd.	x	x

Nr.	Hosting	NIPV	BRW
20.	De opdrachtnemer draagt zorg voor de hosting van de ontwikkel-, test-, acceptatie en productieomgeving van de websites van opdrachtgever.	x	x
21.	Hosting vindt plaats op servers binnen de EU (EER)	x	x
22.	De opdrachtnemer ondersteunt bij het correct archiveren van de websiteomgeving conform de Archiefwet. Het NIPV maakt hiervoor gebruik van Archiefweb.	x	x
23.	Opdrachtnemer heeft een anti DDoS voorziening ingeregeld.	x	x
24.	Er wordt minimaal 1x per jaar een penetratietest uitgevoerd op de servers van de opdrachtnemer waar de multi-site omgeving van het NIPV/Brandweer.nl op draait.	x	x

Nr.	Security eisen	NIPV	BRW
	<i>De security eisen die nu al aanwezig zijn op het platform en waarvan redelijkerwijs vanuit gegaan mag worden dat deze bij wisseling van opdrachtnemer worden overgenomen, zijn in dit onderdeel niet opnieuw opgenomen. Zie hiervoor eis nr. 6 - Content Management systeem.</i>		
25.	De opdrachtnemer is verantwoordelijk voor het beheer en tijdig verlengen van de certificaten (HTTPS en HSTS).	x	x
26.	Opdrachtnemer monitort doorlopend de websiteomgevingen van opdrachtgever middels een Security Operations Centre (SOC) en/of Security Incident & Event Management (SIEM) of vergelijkbaar.		X
27.	Informatiebeveiligingsincidenten, zoals datalekken, worden binnen 4 uur na constatering door opdrachtnemer bij het NIPV gemeld.	x	X
28.	Opdrachtnemer biedt de mogelijkheid aan Opdrachtgever om de rollen en rechtenstructuur van alle websites te beheren en hier wijzigingen in aan te kunnen brengen.	x	x
29.	Er is multi-factor authenticatie aanwezig om in te loggen op de beheeromgeving van het platform. Opdrachtgever is eigenaar van de gebruikte sleutels en deze worden ook bewaakt door Opdrachtgever.	x	x
30.	Opdrachtnemer garandeert dat data van het NIPV strikt gescheiden is van andere klanten.	x	x
31.	Bij beëindiging contract wordt data van NIPV aantoonbaar verwijderd (waar nodig na overdracht).	x	x
32.	3 maanden vóór beëindiging van de overeenkomst werkt Opdrachtnemer mee aan een exit-scenario waarin de websiteomgevingen van Opdrachtgever worden overgedragen naar een opvolger van Opdrachtnemer.	x	x
33.	De opdrachtnemer voert minimaal jaarlijks aantoonbaar een recovery test uit.	x	x
34.	Ontwikkelingen die invloed hebben op de beveiliging van de websiteomgeving, worden in de testfase aan een penetratietest onderworpen.	x	
35.	NIPV heeft het recht om een audit / onafhankelijk onderzoek te (laten) uitvoeren.	x	x
36.	De opdrachtnemer beschikt over een ESCROW regeling.	x	x
37.	Alle clouddiensten verbonden met de multi-site omgeving van het NIPV, volgen het Cloud Security Privacy Control Framework van JenV.	x	x

38.	Bij storingen en incidenten wordt door de opdrachtnemer binnen vijf werkdagen een root cause analysis (storingsrapport) verstuurd. Daarin worden ten minste oorzaak, gevolg, oplossing en aanbevelingen benoemd.	x	x
-----	--	---	---

Nr.	Privacy eisen	NIPV	BRW
39.	De opdrachtnemer ondertekent de door het NIPV ter beschikking gestelde verwerkersovereenkomst.	x	x
40.	Bij het verwerken van persoonsgegevens wordt het principe van dataminimalisatie gehanteerd.	x	x
41.	De opdrachtnemer voldoet aan de Algemene Verordening Persoonsgegevens (AVG).	x	x
42.	De opdrachtnemer zorgt ervoor dat het gegevensbeschermingsbeleid , privacy- en cookiestatement aan de technische kant goed is ingeregeld. Tracking cookies worden bijv. pas ingeladen nadat het cookiestatement is geaccepteerd. <i>Opdrachtgever ziet toe op een privacy- en cookiestatement dat up-to-date is en voldoet aan wet- en regelgeving.</i>	x	x

Nr.	Service management (SLA) & Dossier Afspraken en Procedures	NIPV	BRW
	<i>In de SLA worden de afspraken met betrekking tot de kwaliteit van de dienstverlening opgenomen. De DAP is een aanvulling op dit document, met een gedetailleerd overzicht van afspraken en procedures in de (crisis)communicatie.</i>		
43.	De opdrachtnemer werkt middels een vooraf overeengekomen SLA, met dezelfde looptijd als de looptijd van de raamovereenkomst. Daarin zijn minimaal de volgende onderdelen opgenomen: 1. Scope van de dienstverlening, met als onderdelen: a. Beheer en onderhoud van het WordPress CMS en de geïnstalleerde plug-ins. b. Hosting van de acceptatie- productieomgeving en ondersteunende infrastructuur. c. Technisch beheer van het webhosting platform. De volgende onderdelen vallen buiten scope: d. Beheer van domeinnamen (DNS) e. Diensten gerelateerd aan online marketing f. Beheer van e-mail 2. Beheeractiviteiten, met een minimale uitsplitsing van en de kosten voor:	x	x

	a. Technisch beheer, het beheer en onderhoud van de infrastructuur, ook wel webhosting genoemd. b. Applicatiebeheer, het beheer en onderhoud van het WordPress CMS en plugins. c. Ondersteuning van functioneel beheer, bij het beheer en onderhoud van de functies van de software. d. Maandelijkse servicemanagement rapportage en – overleg. 3. Storingsbeleid, met als minimaal opgenomen onderdelen: a. Prioriteitenmatrix. b. Responstijden. c. Oplos- en responstijden tijden op basis van inspanningsverplichting. d. Wijze van ondersteuning. e. Wijze van inschakelen. 4. Procedure bij informatiebeveiligingsincidenten. 5. Releasekalender, met minimaal de volgende onderdelen: a. Onderscheid tussen technische en functionele releases en de afspraken bij beide type releases. b. Manier en tijdspanne waarin wijzigingen worden doorgevoerd. c. Afspraken rondom spoedprocedures. 6. Servicenormen, met minimaal de volgende onderdelen opgenomen: a. Gemeten beschikbaarheid. b. Gemeten laadsnelheid webpagina 7. Afspraken rondom vertrouwelijkheid en veiligheid. De onderdelen die hiervoor benoemd moeten worden, staan in de tabel 'Security eisen'. Wijzigingen binnen de SLA zijn, na wederzijds goedkeuren, op elk moment door te voeren. Onderstaande nummers gaan in op specifieke minimumvereisten die in de SLA terug moeten komen.		
44.	De prioriteitenmatrix is als volgt ingedeeld: 1. Impact a. Lage impact: Alleen voor (NIPV-)medewerkers die de website beheren b. Medium impact: Alleen voor bepaalde gebruikers c. Hoge impact: Voor alle gebruikers 2. Urgentie, met als minimale randvoorwaarden een: a. Lage urgentie: maximale onbereikbaarheid van 3 dagen b. Medium urgentie: maximale onbereikbaarheid van 1 dag c. Hoge urgentie: Elke vorm van onbereikbaarheid is te lang. Bij een prio 1 melding (hoge impact, medium urgentie of medium impact, hoge urgentie) biedt de opdrachtnemer 24/7 dienstverlening. Daarnaast geldt hierbij een responstijd van maximaal 1 uur binnen kantoortijden.	x	x
45.	De volgende eisen zijn van toepassing op de releases en releasekalender:	x	x

	1. Er vindt minimaal eens per maand een release plaats, waarin de meest recente WordPress en plug-in updates worden meegenomen. Eventuele doorontwikkelingen worden zoveel als mogelijk tijdens dit vaste releasemoment gepland. 2. In overleg zijn aanvullende releases mogelijk, bijvoorbeeld bij specifieke doorontwikkelingen of kritieke updates waar haast bij geboden is. 3. Releases vinden altijd eerst plaats op de acceptatie (test) omgeving. Tussen release op acceptatie en productie zitten minimaal 5 werkdagen. 4. Bij releases waar een langere downtime dan gebruikelijk wordt verwacht, wordt het NIPV minimaal een week van tevoren ingelicht.		
46.	De volgende eisen zijn van toepassing op de servicenormen: 1. De gemiddelde beschikbaarheid (up-time) per kalendermaand is 99,9%, exclusief gepland onderhoud. In de maandelijkse servicerapportage wordt de up-time steeds meegenomen. 2. De gemeten laadsnelheid en wanneer sprake is van onbeschikbaarheid, met als randvoorwaarden: a. Maximaal 2 seconden bij 90% van de metingen. b. Maximaal 3 seconden bij 99% van de metingen. c. Vanaf 10 seconden is er sprake van onbeschikbaarheid.	x	x
47.	De opdrachtnemer werkt middels een vooraf overeengekomen SLA/DAP, met dezelfde looptijd als de raamovereenkomst. Daarin zijn minimaal de volgende onderdelen opgenomen: 1. Rollen en verantwoordelijkheden van leverancier, tussenleverancier en klant 2. Communicatieafspraken, contactinformatie alle partijen. 3. Escalatiematrix. Hierin is opgenomen welke persoon op welke momenten worden benaderd in het geval escalatie noodzakelijk is. 4. Afspraken en gebruikte software voor monitoring.	x	x

Nr.	Prijzen	NIPV	BRW
48.	De opdrachtnemer mag voor de SLA en de DAP een maximum maandbedrag rekenen van €3.400,- per maand. Deze prijzen staan vast gedurende de volledige looptijd van de overeenkomst. Met als enige uitzondering een jaarlijkse verhoging van de door het CBS gepubliceerde prijsindexcijfers dienstenprijzen.	x	
49.	De opdrachtnemer mag voor haar dienstverlening een maximum uurtarief van €122,- hanteren. Dit uurtarief staat vast gedurende de volledige looptijd van de overeenkomst. Met als enige uitzondering een jaarlijkse verhoging van de door het CBS gepubliceerde prijsindexcijfers dienstenprijzen.	x	x