Bijlage 9
Concept Programma van eisen

Nederlands Instituut Publieke Veiligheid
Postbus 7112
2701 AC Zoetermeer

Colofon

Titel:	Bijlage 9 Concept Programma van eisen
Datum:	1 september 2025
Vertrouwelijkheid:	Vertrouwelijk
Status:	Concept
Versie:	0.1
Kenmerk:	NIPV2025-MMO-04146
Auteurs:	

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.

Inhoudsopgave

1 Programma van Eisen 3
1.1 Algemeen eisen 3
1.2 Security eisen 4
1.3 Service Level Agreement eisen 5
1.4 Hosting eisen 6
1.5 Verkeersplein eisen 7

1 Programma van Eisen

De eisen zoals opgenomen in dit document gelden als uitvoeringseisen. Het betreft een initiële versie van het Programma van Eisen. Deze eisen kunnen gewijzigd worden naar aanleiding van de diverse onderhandelrondes in de Gunningsfase.

1.1 Algemeen eisen

Algemene eisen	
Eis Algemeen 1	Medewerkers van de inschrijver die voor het NIPV worden ingezet, dienen een Verklaring Omtrent het Gedrag (VOG) te overleggen die niet ouder is dan drie maanden. Deze VOG moet betrekking hebben op de volgende profielen. 11: Bevoegdheid tot het raadplegen en/of bewerken van systemen. 12: Omgaan met gevoelige of vertrouwelijke informatie. 13: Beschikken over kennis van veiligheidssystemen, controlemechanismen en verificatieprocessen. 14: Het verlenen van diensten, zoals advies, beveiliging, schoonmaak, catering, onderhoud, enzovoort.
Eis Algemeen 2	De inschrijver erkent dat alle aangekochte software, de Tenant en domeinnamen eigendom zijn en blijven van het NIPV. Dit geldt ook bij beëindiging van de overeenkomst. De inschrijver helpt bij een goede en snelle overdracht. Op verzoek van het NIPV maakt de inschrijver een exitplan. Hierin staat hoe de dienstverlening stopt, hoe data en documenten worden overgedragen en hoe kennis wordt gedeeld. De overdracht gebeurt binnen een afgesproken termijn en tegen redelijke kosten. Het exitplan komt in het Dossier van Afspraken en Procedures (DAP).
Eis Algemeen 3	In het kader van een ABDO-accreditatie dient het hoofdkantoor van de inschrijver gevestigd te zijn in het Europees deel van het Koninkrijk der Nederlanden.
Eis Algemeen 4	Alle (self)serviceportalen waarmee het NIPV te maken kan krijgen, zijn in de Nederlandse taal.
Eis Algemeen 5	Alle communicatie van de Inschrijver naar het NIPV vindt plaats in de Nederlandse taal (C1; zie ook https://detaalbrigade.nl/taalniveaus/) tenzij anders afgesproken.
Eis Algemeen 6	Het NIPV behoudt zich het recht voor om een externe partij een audit uit te laten uitvoeren op de gehele dienstverlening (of delen van) zoals is afgesproken in de overeenkomst.
Eis Algemeen 7	Inschrijver levert gedurende de voorbereiding, implementatie, livegang en nazorg één vaste, integraal verantwoordelijke projectleider, die verantwoording aflegt aan het NIPV.
Eis Algemeen 8	Inschrijver zal bij de uitvoering van de diensten alle noodzakelijke zorg betrachten om te vermijden dat (nader) forensisch onderzoek niet goed meer kan worden

	uitgevoerd of de resultaten daarvan niet goed (meer) zouden kunnen worden vertrouwd.

1.2 Security eisen

Eisen ten aanzien Security	
Eis Security 1	De dienstverlening voldoet aan de open (verplichte) standaarden van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/verplicht) en de richtlijnen van het NCSC met betrekking tot encryptie. Op het moment van aanbesteden is de eis dat men aan TLS 1.2 of 1.3 voldoet.
Eis Security 2	De af te nemen omgevingen bieden ondersteuning voor Single Sign On vanuit de NIPV-omgeving.
Eis Security 3	Het NIPV maakt gebruik van een externe Identity manager die wij TGV (Toegang Gezamenlijke Voorzieningen) noemen. De inschrijver kan een connectie via Google Cloud interconnect naar deze service leveren en onderhouden. De startdatum en looptijd wordt door het NIPV aangegeven.
Eis Security 4	De inschrijver ondersteunt dat toegang tot de omgeving ingeregeld zal worden via ons TGV systeem op basis van OIDC inclusief Multi Factor Authenticatie (MFA).
Eis Security 5	De inschrijver werkt mee een Data Protectie Impact Assessment voor aanvang van de werkzaamheden.
Eis Security 6	Inschrijver draagt er zorg voor dat data van het NIPV onderweg en in rust (transit en at rest) encrypted is. Inschrijver werkt mee om data ook tijdens gebruik (in use) encrypted te houden.
Eis Security 7	Alle gebruikersinterfaces van de oplossing worden beveiligd met Multi-Factor Authentication met credentials van het NIPV.
Eis Security 8	Data is op zeer korte termijn naar andere locatie of andere inschrijver te migreren in geval van aantoonbare noodzaak.
Eis Security 9	Een netwerk sensor van het NCSC of andere leverancier mag in het (private Cloud) datacenter worden geïnstalleerd. Inschrijver ondersteunt bij werkzaamheid hiervan (firewall/Netwerk instellingen).
Eis Security 10	Antivirus en malware scanning wordt uitgevoerd op de gehele dienstverlening van hosting tot dataverkeer.
Eis Security 11	Inschrijver gaat in de security architectuur uit van het Zero trust principe.
Eis Security 12	Inschrijver zorgt voor DDOS-beveiliging en verzorgt risicobeperking services.
Eis Security 13	Inschrijver laat minimaal jaarlijks een pentest uitvoeren door een onafhankelijke en voor genoemde pentest gecertificeerde partij op de gehele hosting, uitgezonderd het back-up systeem. Het integrale rapport zal proactief worden opgeleverd bij het

	NIPV en, waar nodig, onder begeleiding van aan verbeterplan. Opdrachtnemer acteert op bevindingen van de rapporteur.
Eis Security 14	Eisen m.b.t. communicatie over incident en beveiligingsincidenten: • Inschrijver heeft een actieve incidentprocedure m.b.t. de communicatie rondom informatiebeveiliging richting zijn klanten. • Beveiligingsincidenten worden binnen de afgesproken tijd gemeld aan het NIPV volgens de afspraken die worden vastgelegd in het DAP en de SLA. • In de maandelijkse en jaarlijkse rapportages is informatiebeveiliging een specifiek onderdeel. Nadere invulling hiervan wordt eveneens vastgelegd in het DAP.
Eis Security 15	Inschrijver gebruikt een beheermodel/framework waarmee invulling wordt gegeven aan de ISM-processen. Inschrijver zorgt tevens voor inrichting van onderliggende processen in zijn organisatie.

1.3 Service Level Agreement eisen

Eisen ten aanzien van de Service Level Agreement	
Eis Service Level Agreement 1	De volledige dienstverlening is schaalbaar en af te nemen op verschillende SLA niveaus per omgeving. Dit niveau kan tussentijds worden verhoogd of verlaagd.
Eis Service Level Agreement 2	Het hoogste SLA niveau kan kunnen worden aangevuld met de ABDO-accreditatie.
Eis Service Level Agreement 3	Inschrijver levert maandelijks een SLA rapport met betrekking tot de afgenomen dienstverlening.
Eis Service Level Agreement 4	De infrastructuur dient hoog beschikbaar te zijn, gemonitord te worden en indien nodig dient er incident management te worden geleverd op de productie omgeving. Op de omgeving dient de inschrijver tenminste technische ondersteuning te leveren tijdens kantoortijden. Dit moet kunnen worden uitgebreid naar andere SLA niveaus.
Eis Service Level Agreement 5	Het NIPV levert een crisismanagement systeem (LCMS) dat 24x7 beschikbaar moet blijven voor de afnemers, maar zeker ten tijde van GRIP situaties. Inschrijver kan een oplossing aanbieden voor de hosting van de NIPV-klant infrastructuur zodat deze beschikbaar blijft bij een incident. Deze eis geldt ook wanneer er uitval van het datacentrum is door natuurverschijnselen of externe defecten zoals kabelbreuk of stroomuitval. Bij de oplossing ligt de nadruk op de beschikbaarheid (High available).
Eis Service Level Agreement 6	Inschrijver test periodiek de werking van de fail-over en back-up systemen. Zoals vastgelegd in de SLA.
Eis Service Level Agreement 7	Inschrijver voert regelmatig (in overleg) kwetsbaarheden scans uit op de gehele hosting. Het rapport hiervan zal transparant aan het aanspreekpunt van het NIPV worden opgeleverd.

Eis Service Level Agreement 8	Bij gevonden kwetsbaarheden uit de eis hierboven (30) levert inschrijver naast de rapportage een plan van aanpak waarin wordt aangegeven welke maatregelen/oplossingen worden getroffen en binnen welke periode deze oplossing, in samenspraak wordt geïmplementeerd. De eventuele kosten worden duidelijk vooraf kenbaar gemaakt middels een offerte.
Eis Service Level Agreement 9	Inschrijver is in staat voor de afgenomen hosting dienst voldoende logging beschikbaar te stellen voor het aanleveren van een audit trail in geval dat een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens (AP).
Eis Service Level Agreement 10	Inschrijver heeft in de aangeboden datacenters de mogelijkheid om in de colocatie rackspace af te nemen in de vorm van een exclusief voor het NIPV bestemd 19” rack. NIPV kan ook in de toekomst altijd meer (exclusief) rackspace afnemen.
Eis Service Level Agreement 11	Inschrijver kan IP-adressen leveren op basis van IPV4 of IPV6.

1.4 Hosting eisen

Eisen ten aanzien van dienstverlening hosting in Azure en private Cloud	
Eis Hosting 1	Inschrijver gaat akkoord met de mogelijkheid om in de toekomst de hosting omgeving te accrediteren voor ABDO. Indien deze accreditatie niet wordt behaald, heeft het NIPV de mogelijkheid om de overeenkomst te beëindigen en zal een vooraf bepaald fallback-scenario in werking treden.
Eis Hosting 2	Inschrijver gaat akkoord met een toekomstige mogelijkheid om de betrokken werknemers te screenen voor ABDO-accreditatie.
Eis Hosting 3	Eisen voor de datacenters: • Aangesloten bij de Dutch Datacenter Association (DDA). • Ingericht en werkzaam als Tier 3 datacentra. • De datacentra dienen in Nederland te staan. • Zijn carrier neutraal. • Zijn tenminste beveiligd tegen ongeoorloofde fysieke toegang en hanteren een beheersingsprotocol bij calamiteiten bijvoorbeeld overstroming, aardbeving, chemische ramp en/of vliegtuigramp. • Heeft minimaal twee internetontsluitingen waarvan AMS-IX er een is. • Voldoen aan TIA 942-2010 normen.
Eis Hosting 4	Eisen voor Azure: • Azure dient in Nederland (regio West-Europa) gehost te worden.
Eis Hosting 5	Inschrijver kan de Azure omgeving en de standaard Microsoft Azure diensten als volledige dienst leveren volgens Hub-Spoke model en met ingerichte Landing zone waarbij het NIPV de Tenant licentie levert.
Eis Hosting 6	De inschrijver kan een Hybride Azure Cloud omgeving aanbieden met een directe verbinding via Expressroute.
Eis Hosting 8	De omgeving kan many write aan.

Eis Hosting 9	De inschrijver kan dedicated Virtual machines met Windows en Linux leveren in een (dedicated) private cloud omgeving. (OS is Minimaal N-1).
Eis Hosting 10	Voor de levering van clouddiensten beschikt de inschrijver over de ISO 27017 certificering.
Eis Hosting 11	De inschrijver beschikt over een ISAE3402 verklaring of SOC 2 Type II-verklaring. (geeft inzicht of de interne processen op het gebied van informatiebeveiliging en sourcing op orde is). Clouddiensten volgen het Cloud Security Privacy Control Framework v1.0 4-10-2022 van JenV.
Eis Hosting 12	Inschrijver is verantwoordelijk voor een architectuuroverzicht van de geleverde omgevingen.

1.5 Verkeersplein eisen

Eisen ten aanzien Verkeersplein	
Eis Verkeersplein 1	Het gevraagde ten aanzien van het Verkeersplein kan worden afgenomen als volledig ondersteunde dienst.
Eis Verkeersplein 2	De NIPV Applicaties en databronnen kunnen via internet en via het Verkeersplein ontsloten worden.
Eis Verkeersplein 3	Applicaties en databronnen kunnen ontsloten worden via een besloten en beveiligd netwerk d.m.v. IPSec site to site VPN-verbindingen over het internet en besloten glasvezelverbindingen.
Eis Verkeersplein 4	Het Verkeersplein netwerk moet onafhankelijk van het publieke internet kunnen functioneren. (Bv i.c.m. Diginetwerk)
Eis Verkeersplein 5	De af te nemen omgevingen bieden ondersteuning voor aansluiting met Public clouddiensten.
Eis Verkeersplein 6	De af te nemen omgevingen bieden ondersteuning voor aansluiting op Diginetwerk.
Eis Verkeersplein 7	Het Verkeersplein is schaalbaar (op basis van periodieke rapportages): - Bandbreedte op alle koppelvlakken en verbindingen, schaalbaar van 5MB tot en met 10GB; - U kunt de verkeersstromen inregel op basis van QoS (Quality of Service) Internet feed, schaalbaar van 5MB tot en met 10GB
Eis Verkeersplein 8	De af te nemen omgevingen bieden ondersteuning voor aansluiting vanuit de netwerken van NIPV-klantapplicatie afnemers. (zoals bv. Veiligheidsregio's en crisispartners).
Eis Verkeersplein 9	De oplossing is carrier neutraal.

Eis Verkeersplein 10	De af te nemen omgevingen bieden ondersteuning voor aansluiting op de Azure, private cloud en on prem omgevingen van NIPV.