Bijlage 1: Programma van Eisen

Door voor deze aanbesteding een inschrijving in te dienen, verklaart Inschrijver zich onvoorwaardelijk en volledig akkoord met onderstaande eisen. Eventuele voortvloeiende kosten uit onderstaande eisen dient u te verwerken in uw prijsopgave. Onderstaande eisen kunnen dus niet leiden tot extra kosten.

Algemene eisen	
1.	Opdrachtnemer conformeert zich aan de AVG en faciliteert dat VRD conform AVG kan werken.
2.	Opdrachtnemer staat ervoor in dat zijzelf, maar ook haar personeel en personeel van door haar ingeschakelde bedrijven, alle bedrijfsinformatie afkomstig van VRD die op enigerlei wijze ter kennis is gekomen of gebracht, geheimhoudt tegenover derden. Opdrachtnemer zal geen informatie over de door haar aan VRD geleverde diensten verstrekken aan derden, behoudens schriftelijke toestemming van de VRD, of in geval van een wettelijke verplichting.
3.	Opdrachtnemer stelt de VRD binnen een termijn van vier weken op de hoogte van iedere wijziging in de organisatiestructuur, juridische structuur en concern/holdingstructuur. Indien een wijziging in de organisatiestructuur, juridische structuur of concernstructuur gevolgen heeft voor de uitvoering van de overeenkomst, dient Opdrachtnemer aan te tonen dat de continuïteit en kwaliteit van de dienstverlening gewaarborgd blijven. Indien Opdrachtnemer deze waarborg niet kan bieden, behoudt VRD zich het recht voor de overeenkomst te beëindigen overeenkomstig de daarvoor geldende contractuele bepalingen.
4.	Opdrachtnemer voorziet in één (1) vast contactpersoon gedurende de gehele looptijd van de opdracht. Opdrachtnemer borgt gelijkwaardige vervanging bij afwezigheid van deze contactpersoon bij ziekte, verlof e.d.
5.	Opdrachtnemer garandeert een bereikbaar- en inzetbaarheid op werkdagen van 08.00-17.00 uur.
6.	Opdrachtnemer is transparant in zijn relaties met haar ketenpartners en/of professionals.
7.	Algemene verkoopvoorwaarden, branchevoorwaarden of andere voorwaarden van Opdrachtnemer worden uitdrukkelijk uitgesloten.
8.	Bijkomende kosten (bijv. reiskosten, reisuren, kilometervergoedingen, verblijfskosten e.d.) zijn onderdeel van de kosten/tarieven en kunnen niet separaat worden gefactureerd.
9.	VRD accepteert alleen digitale facturen en richt deze aan VRD. Opdrachtnemer vermeldt op de digitale factuur minimaal: - omschrijving/specificatie van de verrichtte dienstverlening; - afzonderlijke bedragen, alsmede het totaalbedrag; - de datum van dienstverlening; - het BTW bedrag; - btw-nummer; - KvK-nummer; - bankrekeningnummer. Tevens dient op de factuur te staan: - een contract-of inkoopordernummer; - persoonsgegevens of kostenplaatsen ter controle/doorbelasting.
10.	Bij beëindiging van de overeenkomst werkt Opdrachtnemer te allen tijde mee met VRD om een zo efficiënt en effectief mogelijke overgang te realiseren naar de nieuwe

	partij. Het tijdig beschikbaar stellen van de door VRD of nieuwe partij gevraagde documenten en gegevens maakt hier onderdeel van uit.
	Functionele eisen Software
11.	De applicatie stuurt minimaal 1 keer per 15 minuten de status van het device naar een backoffice server waar deze minimaal 60 dagen opgeslagen wordt.
12.	Na alarmering van het voertuig door de meldkamer start het systeem geheel automatisch de routenavigatie op met de efficiëntste route naar de incidentlocatie.
13.	Bij alarmering worden in de routeberekening busbanen, beweegbare paaltjes e.d. (vrijstellingen) meegenomen (route veiligheidsdiensten).
14.	Het is mogelijk om profielen aan te maken met daarin de afmetingen en gewichten van verschillende typen voertuigen. De profielen zijn per device toe te wijzen.
15.	In het navigatiesysteem wordt de berekende route aangepast op basis van het profiel dat is toegewezen aan het device.
16.	Bij een wijziging van de incidentlocatie door de meldkamer wordt de route aangepast na bevestiging van de chauffeur en/of automatisch na 15 seconden.
17.	Een route wijziging (zie eis 16) wordt aangegeven op het navigatiescherm.
18.	Na iedere route berekening wordt de ETA naar de backoffice server verzonden én doorgezet naar het Repressief Informatiesysteem (RIS) van VRD. Dit wordt gedeeld middels open standaarden.
19.	Bij wijzigen van de ETA met meer dan 30 seconden wordt de nieuwe ETA tijd naar de backoffice server verzonden én doorgezet naar het RIS van VRD
20.	Gedurende het incident dient de actuele locatie van de eenheid zonder vertraging gedeeld worden met de landelijke voertuigpositieserver (VPS) en rechtstreeks met het (toekomstig) RIS van VRD.
21.	Het systeem dient tijdens het navigeren een vloeiende gebruikerservaring te bieden, waarbij kaart- en navigatiebeelden zonder merkbare vertragingen, schokken of onderbrekingen worden weergegeven
22.	Het systeem kan via open standaarden koppelen met een systeem voor automatische statusplotting (‘uitgerukt’, ‘ter plaatse’ en ‘op de post’).
23.	De navigatieweergave is beschikbaar in 2D.
24.	Bij het handmatig invoeren van een locatie kan de functie 'route veiligheidsdiensten' worden uitgezet.
	Functionele eisen Beheer van de applicatie
25.	Een navigatie opdracht kan door beheer van VRD op afstand naar het systeem verstuurd worden.
26.	Status van de applicatie is door de beheerders van VRD op afstand te raadplegen en te beheren (zoals profielen wisselen en het aanpassen van gegevens in de kaart).
27.	De gereden route wordt gelogd en kan worden teruggekeken in het beheersysteem. Deze data kunnen ook geëxporteerd worden via open standaarden.
28.	Het systeem biedt ondersteuning voor beveiligde toegang tot de beheeromgeving van het systeem door middel van Single Sign-On (SSO) en ondersteunt meerdere beheerprofielen met rolgebaseerde autorisaties. Autorisatie van de oplossing is te koppelen aan de identiteitsvoorziening van VRD, in het kader van Single Sign On
29.	Historische data van de routenavigatie is tenminste 5 jaar door VRD te raadplegen (bijvoorbeeld voor evaluatie).
30.	Opdrachtnemer stelt gedurende de volledige contractperiode beveiligingsupdates en updates van de navigatieapplicatie beschikbaar en ondersteunt de implementatie hiervan.

31.	De applicatie levert realtime de online/offline status, de GPS-status, het accuniveau, de locatie van het device, de geïnstalleerde versie van de voertuignavigatie, de applicatiestatus en de laatste synchronisatie.
	Functionele eisen Kaartlagen
32.	VRD heeft de mogelijkheid om aanpassingen te doen in wegeigenschappen, zoals maximumsnelheid, doorrijhoogte en aslasten.
33.	VRD heeft de mogelijkheid om zelf wegen in te tekenen ten behoeve van alternatieve routes.
34.	VRD heeft de mogelijkheid om minimaal acht verschillende kaartlagen toe te voegen alsook POI's. Alle kaartlagen en POI's kunnen op afstand voorzien worden van een update (koppeling geoserver VRD). Deze aanpassingen blijven ook staan na een software update.
35.	Per soort POI is het mogelijk om te zoeken naar de dichtstbijzijnde en een specifieke POI.
36.	Kaartmateriaal is op het device geïnstalleerd, zodat offline navigatie mogelijk is.
	Functionele eisen Wegstremmingen
37.	VRD kan wegstremmingen met een begintijd en eindtijd aanmaken.
38.	Alle wegstremmingen worden na de eindtijd minimaal 60 dagen bewaard.
39.	Alle wegstremmingen worden maximaal 15 minuten na opslaan verwerkt in het systeem.
40.	Er is een koppeling met de NDW-data, zodat elke stremming automatisch in het systeem terecht komt.
41.	Er wordt automatisch een notificatie in de beheeromgeving gezet bij het automatisch in het systeem komen van een wegstremming.
42.	Stremmingen via NDW-data zijn aan te passen door VRD.
	Functionele eisen Devices
43.	De applicatie is schaalbaar met het formaat van het device. (VRD voorziet zelf iPad mini's als de devices op de voertuigen met beheer via Microsoft Intune. Inbouw zal door een derde partij gebeuren.
44.	De aangeboden navigatiesoftware kan volledig functioneel worden geïnstalleerd en gebruikt op een door VRD beschikbaar gesteld device (zie vorige eis).
45.	Inschrijver geeft aan welke minimale hardware- en besturingssysteemeisen gelden voor het gebruik van de aangeboden navigatiesoftware.
46.	Inschrijver maakt bij inschrijving eventuele afhankelijkheden van specifieke hardware, firmware, besturingssysteemversies, Google-diensten of aanvullende softwarecomponenten kenbaar.
47.	De aangeboden navigatiesoftware ondersteunt het centrale beheer van de door VRD beschikbaar gestelde devices via Microsoft Intune en belemmert niet dat VRD deze devices op afstand kan vergrendelen, wissen of buiten gebruik stellen.
48.	De navigatiesoftware moet draadloos kunnen communiceren met vrachtwagen multimediasystemen.
	Non-functionele eisen
49.	De oplossing voldoet volledig aan toepasselijke Nederlandse wet- en regelgeving.
50.	De oplossing bestaat uit een centraal beheerde SaaS-backoffice in combinatie met een navigatieapplicatie die ook zonder actieve internetverbinding kan functioneren
51.	De SaaS-oplossing wordt technisch door Opdrachtnemer beheerd en onderhouden.
52.	Opdrachtnemer zorgt voor een doorlopende beschikbaarstelling van de meest recente versie van de oplossing gedurende de contractperiode, zonder inschrijving op toekomstige releases.
53.	Opdrachtnemer verstrekt licenties die op naam van VRD staan.

54.	De oplossing ondersteunt het gebruik op zowel reguliere werkplekken als mobiele apparaten (webapp of mobiele app) voor veelgebruikte functionaliteit.
55.	Oplossing ondersteunt open standaarden die het mogelijk maken brongegevens en gegenereerde navigatiegegevens te benaderen
56.	De oplossing biedt inzicht in uitgevoerde berekeningen/ algoritmes.
57.	Koppelingen en gebruikte brongegevens zijn te raadplegen in de Nederlandstalige documentatie die wordt meegeleverd bij oplevering van de applicatie.
58.	Toegang tot onderdelen van de oplossing is via een autorisatiemechanisme in te stellen. De oplossing ondersteunt rolgebaseerde autorisaties (Role Based Access Control), bijvoorbeeld via een autorisatiematrix. Autorisaties worden ingericht volgens het principe van minimale rechten, waarbij gebruikers uitsluitend beschikken over de toegangsrechten die noodzakelijk zijn voor de uitvoering van hun werkzaamheden
59.	De oplossing ondersteunt integratie en gegevensuitwisseling op basis van open standaarden, volgens 'Pas toe leg uit'-standaarden (verplicht) | Forum Standaardisatie.
60.	Opdrachtnemer borgt dataveiligheid, continuïteit en eigenaarschap van gegevens door adequate scheiding, back-up- en herstelvoorzieningen. Samengevat betekent dit: - Er is een logische/virtuele scheiding tussen omgevingen en isolatie van gegevens tijdens transport, verwerking en opslag zonder performance-hinder door gedeelde componenten. - Back-up en restore met een RTO van maximaal 24 uur en een RPO van maximaal 4 uur. - De back-uplocaties zijn geografisch gescheiden. - Opdrachtnemer maakt actief back-ups van zijn informatie en test periodiek (minimaal jaarlijks) of een restore succesvol is. Back-ups zijn versleuteld en gescheiden opgeslagen. - VRD is volledig eigenaar van alle gegevens en documenten met de mogelijkheid tot het verstrekken van exports (eigenhandig of op verzoek).
61.	Opdrachtnemer garandeert een hoge beschikbaarheid en performance van de oplossing, inclusief transparant onderhoud en continue monitoring. Samengevat omvat dit: - minimale beschikbaarheid van 99% per maand (exclusief onderhoud), met duidelijke afspraken over geplande en ongeplande downtime en voorafgaande melding/instemming bij werkzaamheden binnen werktijden; - uitvoering van functioneel beheer zonder verstoring voor gebruikers; - actieve monitoring en alarmering bij verstoringen, security-incidenten en afwijkingen.
62.	Opdrachtnemer stelt VRD in staat tot uitgebreid testen binnen de oplossing en ondersteunt een beheerste go-live.
63.	De oplossing bevat een testomgeving om wijzigingen te kunnen testen voordat deze naar de operationele omgeving gaan.
64.	De oplossing biedt een consistente, geïntegreerde en webgebaseerde gebruikersinterface, geschikt voor werken op afstand en ondersteuning van gangbare browsers.
65.	De reactie- en oplostijden bij storingen zijn: - Prioriteit 1 (kritiek): de oplossing is niet beschikbaar of een kritische functionaliteit werkt niet waardoor de primaire bedrijfsvoering wordt belemmerd. Reactietijd: maximaal 1 uur. Oplostijd: maximaal 4 uur.

	- Prioriteit 2 (hoog): een belangrijke functionaliteit werkt niet of slechts gedeeltelijk, waardoor gebruikers hun werkzaamheden niet of beperkt kunnen uitvoeren. Reactietijd: maximaal 1 uur. Oplostijd: maximaal 24 uur.
66.	Opdrachtnemer beoordeelt en bevestigt standaard wijzigingsverzoeken (change-aanvragen) binnen maximaal 72 uur na ontvangst. De uitvoeringstermijn wordt vastgesteld overeenkomstig de in de aanbestedingsleidraad opgenomen SLA
67.	Opdrachtnemer stelt het volgende beschikbaar: - een uitgebreide module voor functioneel beheer; - een volledig digitale en actuele handleiding; - logging en tracing van de bewerkingen die zijn uitgevoerd door de functioneel beheerders.
68.	VRD kan in de oplossing gebruikersaccounts aanmaken, wijzigen en intrekken. De oplossing biedt overzichten van autorisaties op applicatieniveau van individuele gebruikers/groepen.
69.	Opdrachtnemer levert een servicedesk met duidelijke servicelevels en continue aandacht voor security en privacy. Samengevat omvat dit: - één centrale servicedesk (telefoon, e-mail en webportaal), bereikbaar op werkdagen, met onbeperkt melden van incidenten en standaard wijzigingen zonder extra kosten; - vastgelegde responstijden en oplostijden per prioriteitsniveau, inclusief Root Cause Analysis bij kritische en hoge incidenten; - 24/7 security-monitoring via SOC of gelijkwaardig, met proactieve detectie en opvolging van beveiligingsincidenten. - Opdrachtnemer meldt informatiebeveiligingsincidenten en datalekken die invloed hebben of kunnen hebben op informatie van VRD of de dienstverlening aan VRD binnen 24 uur na constatering
70.	Over het informatiebeheer geldt: - De oplossing komt tegemoet aan de standaard duurzame bestandsformaten en metadata-standaarden. - De opgeslagen informatieobjecten in de applicatie blijft duurzaam toegankelijk gedurende het gebruik van de applicatie, tenzij informatie volgens protocol vernietigd wordt. - De oplossing legt per informatieobject metagegevens vast voor de bewaartermijn. De datum voor het vernietigen of overbrengen (naar e-depot) van informatie wordt daarbij automatisch berekend. - Informatieobjecten en bijbehorende metadata kunnen onherstelbaar worden vernietigd. - Van de vernietiging dient door opdrachtnemer een verklaring te worden opgeleverd waarin minimaal wordt aangegeven om welke informatie het gaat, dat de vernietiging volledig is uitgevoerd en wat het datavolume ervan is. - Opdrachtnemer garandeert dat bij een backup-recovery geen gegevens terug in productie worden gezet die formeel al vernietigd zijn. - Bij een export kunnen de data en metadata in een gangbaar machinaal leesbaar bestandsformaat meegeleverd worden, zoals XML.
71.	Opdrachtnemer werkt mee aan een onafhankelijke audit op de opzet, het bestaan en de werking van beheersmaatregelen voor informatiebeveiliging en privacy. Opdrachtnemer voert periodiek onafhankelijke informatiebeveiligingsaudits uit waarmee de getroffen maatregelen worden aangetoond. De audit kan door of namens VRD worden uitgevoerd. In overleg kan een ISAE 3000 type 2-rapportage en/of een ISAE 3402-rapportage worden gevraagd, voor zover relevant voor de dienstverlening.

	De managementsamenvatting van de meest recente audit wordt desgevraagd aan VRD beschikbaar gesteld.
72.	Gegevens van VRD worden niet gebruikt voor het trainen van AI-modellen. Gebruik van gegevens van VRD voor productverbetering of benchmarking is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van VRD.
73.	Opdrachtnemer van clouddiensten beschikt aantoonbaar over informatiebeveiligingsmaatregelen die gelijkwaardig zijn aan beheersdoelen van de ISO-27017 richtlijn.
74.	Opdrachtnemer beschikt over een gecertificeerd managementsysteem voor informatiebeveiliging, bijvoorbeeld ISO-27001.
75.	Opdrachtnemer heeft de best practices voor informatiebeveiligingsmaatregelen in lijn met bijvoorbeeld ISO-27002 ingericht.
76.	Opdrachtnemer waarborgt dat vertrouwelijke informatie van VRD tijdens transport via netwerken en tijdens opslag wordt versleuteld met actuele en passende versleutelingsstandaarden. Alle communicatie tussen devices, backendsystemen en externe koppelingen wordt versleuteld, waarbij voor TLS-verbindingen minimaal TLS 1.2 wordt toegepast
77.	Opdrachtnemer heeft gedrags- en geheimhoudingscode voor zijn personeel.
78.	Opdrachtnemer zorgt ervoor dat het personeel wordt opgeleid tot een passend niveau van informatiebeveiligings- en privacy bewustzijn (bewustwordingstrainingen).
79.	Opdrachtnemer beschikt over een proces voor het screenen van personeel.
80.	Opdrachtnemer beschikt over een methode om zijn continuïteit en dienstverlening aan VRD te borgen.
81.	Opdrachtnemer gebruikt de door VRD verstrekte persoonsgegevens uitsluitend voor het doel van de uitvoering van de opdracht en niet voor andere (commerciële) doeleinden en deelt data van VRD alleen met derden na schriftelijke toestemming van VRD.
82.	Opdrachtnemer waarborgt dat informatie van VRD uitsluitend binnen de Europese Economische Ruimte (EER) wordt opgeslagen en verwerkt
83.	Opdrachtnemer beschikt over een gedocumenteerd proces voor het registreren en opvolgen van beveiligingsincidenten en handelt conform dit proces.
84.	Opdrachtnemer past Security-by-Design-principes toe bij het ontwikkelen en onderhouden van IT-systemen en software en beschikt hiervoor over een gedocumenteerd proces. Opdrachtnemer past passende basismaatregelen voor informatiebeveiliging toe, waaronder sterke authenticatie, automatische schermvergrendeling en toegangsbeheer volgens het principe van minimale rechten. Voor toegang tot beheerfunctionaliteiten en systemen die informatie van VRD verwerken, wordt Multi-Factor Authentication (MFA) toegepast.
85.	Opdrachtnemer voert minimaal maandelijks vulnerability scans uit op alle IT-systemen, en lost bevindingen met vaste oplostermijnen op.
86.	Opdrachtnemer voert beveiligingsupdates adequaat uit op alle IT-systemen en zorgt ervoor dat alle endpoints (PC's, Laptops, Servers, Firewall…) adequaat beveiligd zijn.
87.	Opdrachtnemer zorgt voor logging en monitoring van de ICT-systemen die informatie van VRD verwerken. Relevante beheeractiviteiten worden geregistreerd in een auditlog. VRD heeft de mogelijkheid om de voor haar dienstverlening relevante auditlogging te raadplegen.
88.	Opdrachtnemer laat ten minste eenmaal per twee jaar een passende penetratietest uitvoeren op de voor VRD relevante systemen en dienstverlening.

89.	Opdrachtnemer verstrekt VRD de uitkomsten van de meest recente penetratietest, ten minste in de vorm van een overzicht van het aantal bevindingen op de niveaus kritiek, hoog en medium. Opdrachtnemer vermeldt daarbij de herstelmaatregelen en de termijnen waarbinnen de bevindingen worden afgehandeld
90.	Opdrachtnemer beschikt, bij het ontwikkelen van een eigen IT-systeem/software, over een proces waarin het ontwerp van het IT-systeem/software is gedocumenteerd.