2025

PUR
MER
END

Bijlage 1B

Programma van eisen ICT ‘Levering scanvoertuig parkeerhandhaving’

[19 december 2025 – versie 1.0]
Zaaknummer: 898540

1 Programma van Eisen

ICT1	**Scanauto met bijhorende koppelingen**
1	De opdrachtnemer levert een scanauto met bijbehorende koppelingen.
2	Op **01-05-2026** moet de door opdrachtnemer aangeboden oplossing in productie zijn.
3	De opdrachtnemer garandeert dat gedurende de contractperiode de aangeboden oplossing wordt onderhouden, ondersteund en doorontwikkeld
4	Bij gebruikmaking van dataverbindingen d.m.v. Simkaarten en bijbehorende data-abonnementen zal de opdrachtgever deze leveren vanuit een lopende en bindende raamovereenkomst met een provider. Machine to Machine verbindingen zijn hierin uitgezonderd.
5	De voorziening is volledig in het Nederlands in woord en geschrift.
ICT2	**Doelgroep gebruikers**
1	De door de opdrachtnemer geleverde oplossing geeft het recht tot gebruik van de voorziening door alle medewerkers van de opdrachtgever en uitvoeringsorganisaties voor zover deze taken uitvoeren voor de opdrachtgever.
ICT3	**Beschikbaarheid**
1	Het scansysteem is **99,8%** beschikbaar:
	• binnen de werktijden van de opdrachtgever van maandag tot en met zaterdag tussen 09:00 uur tot 21:00 uur
	• buiten de werktijden van de opdrachtgever uitgezonderd ICT 3.3
2	Onderhoudswerkzaamheden van opdrachtnemer vinden plaats in overleg met opdrachtgever.
3	Werkzaamheden door de opdrachtnemer worden altijd minimaal 14 werkdagen van tevoren gecommuniceerd.
4	Een uitzondering op punten ICT3.1, ICT3.2 en ICT3.3 zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn, informatiebeveiligingsincidenten en rampen.
ICT4	**Wijzigingenbeheer geïnitieerd door opdrachtnemer**
1	Alle wijzigingen worden door de opdrachtnemer altijd eerst getest voordat deze in productie worden genomen en worden via een wijzigingsprocedure bij opdrachtnemer doorgevoerd.
2	Relevante wijzigingen van de opdrachtnemer binnen de oplossing worden gelogd en zijn opvraagbaar door de opdrachtgever.
ICT5	**Technische beveiliging**
1	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.
2	De opdrachtnemer geeft hoge prioriteit aan het snel installeren van de laatste beveiligingspatches.
3	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.
4	De opdrachtnemer voert actief controles uit op systeemlogging.

5	Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig zijn, worden onmiddellijk gemeld aan en besproken met de opdrachtgever.
6	De voorziening maakt gebruik van een NTP-server om de tijd te bepalen. Waaronder het systeem automatisch zomer- en wintertijd en tevens de datum in geval van schrikkeljaren corrigeert.
ICT6	**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.
2	De gegevens van opdrachtgever worden alleen in de EER opgeslagen in overeenstemming met de eisen van de AVG.
3	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 nieuwste versie van het 'model standaard verwerkersovereenkomst VNG' worden gebruikt.
4	De infrastructuur en organisatie van leverancier zijn adequaat beveiligd volgens ISO 27001. Leverancier is bij gunning en gedurende looptijd overeenkomst gecertificeerd voor ISO 27001 en overhandigt het certificaat met verklaring van toepasselijkheid ten tijde van het sluiten van de overeenkomst. Het certificaat wordt geleverd in het engels en de verklaring van toepasselijkheid in het nederlands.
5	Vulnerability assessments (security scans) worden periodiek uitgevoerd (minimaal 1 x per jaar).
5.1	De opdrachtgever heeft toestemming om zelf een pentest te (laten) uitvoeren.
6	Rapportages voor zover direct van invloed voor opdrachtgever omtrent de veiligheid van de oplossing worden gedeeld met de opdrachtgever.
7	De aangeboden oplossing legt een audittrail vast over het gebruik.
7.1	Deze audittrail bevat alle handelingen m.b.t. gebruikersautorisaties en functioneel gebruik (van medewerkers van opdrachtnemer) van gevraagd systeem zoals raadplegen, aanmaken, muteren en verwijderen van informatie.
7.2	Vastlegging vindt minimaal plaats op gebruikersniveau en -rol, tijdstip en verrichte actie. De logging is opvraagbaar door opdrachtgever bij opdrachtnemer waarbij opdrachtnemer deze z.s.m. aanlevert.
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.
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.
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.
10	De opdrachtnemer verleent medewerking aan het uitoefenen van controle door of namens opdrachtgever op bewaring en gebruik van data en naleving van procedures.
11	De opdrachtnemer garandeert een adequate back-up- en restorevoorziening waarbij er geen sprake is van dataverlies en de dienstverlening op de gecreëerde data binnen 24 uur kan worden gecontinueerd.
12	Opdrachtnemer hanteert een sterk wachtwoordbeleid conform de BIO2 vereisten die aan de overheid worden gesteld. Voor toegang tot alle data binnen de scanvoorziening.
12.1	Wachtwoorden in de voorziening worden nooit in plaintext opgeslagen of verstuurd. Basic Authentication is niet toegestaan.
13	De voorziening voldoet aan de actuele vereisten gesteld in de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Daarbij gaat opdrachtgever op dit moment uit van TLS 1.2.
14	Voor veilige bestandsuitwisseling via mail tussen opdrachtgever en opdrachtnemer accepteert opdrachtnemer de oplossing die opdrachtgever biedt welke compliant is aan de NTA 7516 (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.
15	De opdrachtnemer zorgt voor een gedegen technische beveiliging (voor het verwerken van persoonsgegevens) in relatie tot specifieke wetgeving. Denk bijvoorbeeld aan de Wpg (Wet politiegegevens).
16	Het systeem voldoet aan de vereisten die de AVG stelt. Dit houdt in dat opdrachtgever zelf de bewaartermijnen kan instellen, rekening houdend met afwijkende bewaartermijnen in de AVG.
17	Indien de leverancier werkzaamheden op afstand dient te verrichten kan via Teamviewer toegang tot het domein van Purmerend worden verkregen. Ondersteuning is hierbij op een afgesproken moment waarbij de werkzaamheden onder supervisie van opdrachtgever worden uitgevoerd.
18	Opdrachtgever eist dat enkel het beeldmateriaal dat betrekking heeft op de taak waarvoor de scanauto wordt ingezet wordt geleverd aan de back-office applicatie. Opdrachtgever wenst dus expliciet dat beeldmateriaal door een niet tijdig in of uitschakelen van de camera maakt dat er beeldmateriaal wordt aangeleverd aan de back-office. Beeldmateriaal wordt alleen geleverd indien de backoffice applicatie daartoe verzoekt.
19	Opdrachtgever vereist van opdrachtnemer proactief advies tijdens de inrichting voor de mogelijkheden die aanwezig zijn om dataminimalisatie te realiseren.
20	De bewaartermijn van het beeldmateriaal in het voertuig bedraagt niet langer dan 24 uur.
21	Het voertuig is voorzien van automatische signalering aan de chauffeur indien de scanvoorziening haar verbinding verliest gedurende de werkzaamheden of indien data overdracht naar de back-office applicatie nog niet heeft plaatsgevonden bij verlaten voertuig.
22	De totale scanvoorziening is voorzien van encryptie, minimaal SHA 256.

23	Datadragers in de scanvoorziening zijn afdoende fysiek beveiligd (bijvoorbeeld geplaatst in een metale behuizing) om pogingen van vandalisme en diefstal zo maximaal als mogelijk te voorkomen.
ICT7	**Technisch beheer**
1	Systeem en Technisch beheer wordt geheel verzorgd door opdrachtnemer.
2	Opdrachtnemer conformeert zich aan de de definitie dat onder Technisch beheer de werkzaamheden worden verstaan die nodig zijn voor het waarborgen van de ononderbroken goede werking van de oplossing.
3	Opdrachtnemer conformeert zich aan de de definitie dat onder Technisch beheer de werkzaamheden worden verstaan van het installeren en (v.w.b. technische aspecten) testen van nieuwe en verbeterde versies, die beschikbaar komen naar aanleiding van onderhoud, in de gehele OTAP-straat.
4	Opdrachtnemer conformeert zich aan de definitie dat onder Technisch beheer tevens de werkzaamheden worden verstaan van het continu en actief monitoren van o.a. de beschikbaarheid, capaciteit, continuïteit, back-up, beveiliging en data-integriteit.
ICT8	**Koppelvlakken**
1	De opdrachtnemer organiseert de afstemming en realisatie van de koppelingen (gegevensuitwisseling) met andere noodzakelijke applicaties van de opdrachtgever. De opdrachtgever heeft een ondersteunende rol.
2	Koppeling tussen de backoffice applicatie en de scanvoorziening geschiedt op basis van een VPN-verbinding.
ICT9	**Architectuur**
1	Opdrachtnemer levert technische architectuurplaten van de oplossing en houdt deze gedurende de overeenkomst actueel.
1.1	De opdrachtnemer levert een technische architectuurplaat op hoofdlijnen met alle componenten, koppelvlakken, disaster/recovery en uitwijk (geografisch gescheiden datacenters).
2	De opdrachtnemer levert voor de oplevering minimaal de volgende documentatie: a. de architectuur van de applicatie b. datamodelspecificatie van de koppelvlakken
3	De opdrachtnemer draagt zorg voor een installatieverslag na elke installatie. Daarin is in elk geval opgenomen: een netwerktekening met gebruikte protocollen en poorten.
ICT10	**Support SLA**
1	Medewerkers van opdrachtnemer bieden ondersteuning in de Nederlandse taal in woord en geschrift.
2	Opdrachtnemer levert voor de oplevering in de productieomgeving een Nederlandstalige handleiding voor de medewerkers van de opdrachtgever en houdt deze gedurende de looptijd van de voorziening c.q. overeenkomst actueel.
3	Opdrachtnemer beschikt over een helpdesk welke medewerkers van de opdrachtgever van **maandag tot en met zaterdag van 9:00 tot 21:00 per telefoon** te woord kan staan.
4	Opdrachtnemer conformeert zich aan de gestelde eisen tot het handelen bij verstoringen in de scanvoorziening. Zie tabblad 'Verstoringen bedr.kritisch'

5	Opdrachtgever (contractmanager) is verantwoordelijk voor het actueel houden van een contactenmatrix op functieniveau van alle betrokken medewerkers van opdrachtgever. Opdrachtnemer is verantwoordelijk voor het aanleveren van de contactenmatrix op functieniveau van alle betrokken medewerkers van opdrachtnemer, rekening houdende met achtervang van de betrokken medewerkers bij afwezigheid. Periodiek wordt de contactenmatrix door opdrachtnemer en opdrachtgever gecontroleerd. In de contactenmatrix worden minimaal de volgende gegevens bijgehouden: functienaam, naam, tel.nr en emailadres
ICT11	**Opleiding**
1	De opdrachtnemer biedt inhouse (op locatie gemeente Purmerend) gebruikerstrainingen voor eindgebruikers.
2	Trainingen worden in het Nederlands gegeven; documentatie is in het Nederlands beschikbaar.
ICT12	**Overdracht gegevens/data bij beëindiging overeenkomst**
1	Alle gegevens in de voorziening zijn en blijven te allen tijde eigendom van opdrachtgever en mogen door opdrachtnemer niet voor andere dan de overeengekomen doeleinden worden gebruikt. Bij beëindiging van de overeenkomst draagt opdrachtnemer zorg dat alle data binnen (24/48 uur) is overgedragen en levert een schriftelijke bevestiging van vernietiging door opdrachtnemer aan opdrachtgever.

De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de Oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De opdrachtgever bepaalt de prioriteit van incidenten. Ten aanzien van de ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:

Categorie	Type (ver)storing	Omschrijving
1	Kritiek	Voorziening is volledig niet beschikbaar
2	Groot	Voorziening is deels niet beschikbaar
3	Klein	Kleine verstoringen
4	Vraag	Gebruikers of beheerdersvragen

De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de Oplossing. De Opdrachtnemer maakt voor de gemeente inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.

Categorie	Reactietijd	Oplostijd
1	0 – ½ uur (24/7)	Work-around binnen 4 uur, Oplossing binnen 8 uur
2	1 uur (24/7)	Work-around binnen 8 uur op werkdagen, Oplossing binnen 24 uur op werkdagen

3	24 uur (op werkdagen tussen 09:00 en 21:00 uur)	Work-around binnen 2 werkdagen, Oplossing in volgende reguliere versie
4	24 uur (op werkdagen tussen 09:00 en 21:00 uur)	Antwoord binnen 1 week

De opdrachtnemer meldt beveiligingsincident direct aan de opdrachtgever. Waarbij een incident wordt geclassificeerd en de volgende termijnen voor herstel worden gerealiseerd.

Classificatie	**Omschrijving**	**Hersteltijd**
Extreem	Extreem hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke catastrofale gevolgen op het gebied van financien, reputatie etc.	4 uur
Hoog	Hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke (significante) financieel, reputatie etc. gevolgen.	1 dag
Midden	Middelmatig risico op gecompromitteerde beveiligingsinrichting met minimale financieel, reputatie etc. gevolgen.	1 week
Laag	Laag risico op gecompromitteerde beveiligingscontrole met meetbare negatieve impact als resultaat.	2 weken

2 Ondertekening

Voor akkoord:
Naam:
Functie:
Handtekening

Organisatie:

Bezoekadres
Purmersteenweg 42
1441 DM Purmerend

Postadres
Postbus 15
1440 AA Purmerend