

Gemeente Eindhoven

Bijlage 1

**Programma van Eisen –
ANPR Camerahandhaving**

Colofon

Opdrachtgever
Titel rapport
Versie
Datum

Gemeente Eindhoven
Programma van Eisen– ANPR Camerahandhaving
1 (definitief)
27 januari 2025

Inhoudsopgave

1	Inleiding	Fout! Geen bladwijzernaam opgegeven.
1.1	Algemeen.....	Fout! Geen bladwijzernaam opgegeven.
1.2	Doel	Fout! Geen bladwijzernaam opgegeven.
1.3	Opzet	Fout! Geen bladwijzernaam opgegeven.
1.4	Definities en terminologie	Fout! Geen bladwijzernaam opgegeven.
2	Projectcontext	Fout! Geen bladwijzernaam opgegeven.
2.1	Huidige situatie.....	Fout! Geen bladwijzernaam opgegeven.
2.2	Randvoorwaarden en uitgangspunten	Fout! Geen bladwijzernaam opgegeven.
2.3	Leveringsomvang.....	Fout! Geen bladwijzernaam opgegeven.
2.4	Beheerprocessen	Fout! Geen bladwijzernaam opgegeven.
3	Functionele eisen.....	Fout! Geen bladwijzernaam opgegeven.
3.1	Algemene beheereisen.....	Fout! Geen bladwijzernaam opgegeven.
3.2	Eisen aan Camera's en masten	Fout! Geen bladwijzernaam opgegeven.
3.3	Eisen aan Kentekenherkenning	Fout! Geen bladwijzernaam opgegeven.
3.4	Eisen aan het Managementsysteem	Fout! Geen bladwijzernaam opgegeven.
3.5	Eisen aan communicatie en rapportage	Fout! Geen bladwijzernaam opgegeven.
3.6	Eisen aan de FAT, uitvoering en SAT	Fout! Geen bladwijzernaam opgegeven.
3.7	Eisen aan documentatie	Fout! Geen bladwijzernaam opgegeven.
3.8	Eisen aan beheer en onderhoud	Fout! Geen bladwijzernaam opgegeven.
3.9	Eisen privacy en informatiebeveiliging	Fout! Geen bladwijzernaam opgegeven.
3.10	Eisen netwerk	Fout! Geen bladwijzernaam opgegeven.
3.11	Eisen functioneel beheer	Fout! Geen bladwijzernaam opgegeven.

1 Inleiding

1.1 Algemeen

Voor u ligt het Programma van Eisen (PvE) met betrekking tot de levering, realisatie en gebruiksklare oplevering van een systeem voor ANPR Camerahandhaving op diverse locaties binnen gemeente Eindhoven. Dit PvE geeft de beschrijving van de eisen die de Opdrachtgever stelt aan het systeem. Het systeem dient derhalve gedurende de gehele technische levensduur volledig te voldoen aan de eisen die in dit PvE zijn opgenomen.

Het systeem voor ANPR Camerahandhaving dient het huidige bollard-systeem bij diverse geslotenverklaringen in Eindhoven te vervangen en daarnaast te fungeren voor de handhaving van de Zero-Emissiezone. Ingebruikname van de Camerahandhaving is gepland per 1 maart 2025. Vóór deze datum dient het systeem volledig operationeel te zijn opgeleverd.

1.2 Doel

Dit PvE beschrijft de eisen aan en vormt het toetsingskader voor het te leveren, installeren en gebruiksklaar op te leveren systeem voor ANPR Camerahandhaving op diverse locaties binnen gemeente Eindhoven.

1.3 Opzet

In hoofdstuk 2 wordt de projectcontext geschetst. Daarbij wordt aangegeven met welke specifieke uitgangssituatie rekening gehouden met worden. Hoofdstuk 3 gaat in op de onderdelen van het systeem voor ANPR Camerahandhaving, de daaraan gestelde eisen alsmede de door het systeem te behalen prestatie-eisen.

1.4 Definities en terminologie

ANPR	Automatic Number Plate Recognition (= Kentekenherkenning)
Bedrijfstijden	De voor een locatie geldende tijdvensters, niet zijnde de uren behorend tot de voor die locatie geldende venstertijden, gedurende welke het systeem voor Camerahandhaving in bedrijf dient te zijn.
Betrouwbaarheidspercentage	Het percentage Hits waarvan het kenteken met een voldoende hoog Zekerheidspercentage is herkend en omgezet ($= P_{\text{BET}} / P_{\text{REG}}$).
Buitenlandse kentekens	Kentekens met een Landcode van een land binnen de EU (niet-zijnde Nederland), Groot-Brittannië, Zwitserland, Noorwegen, Rusland of Oekraïne.
Camera's	De apparatuur die geschikt is om (bewegende) beelden te registreren en voor opslag aan te bieden.

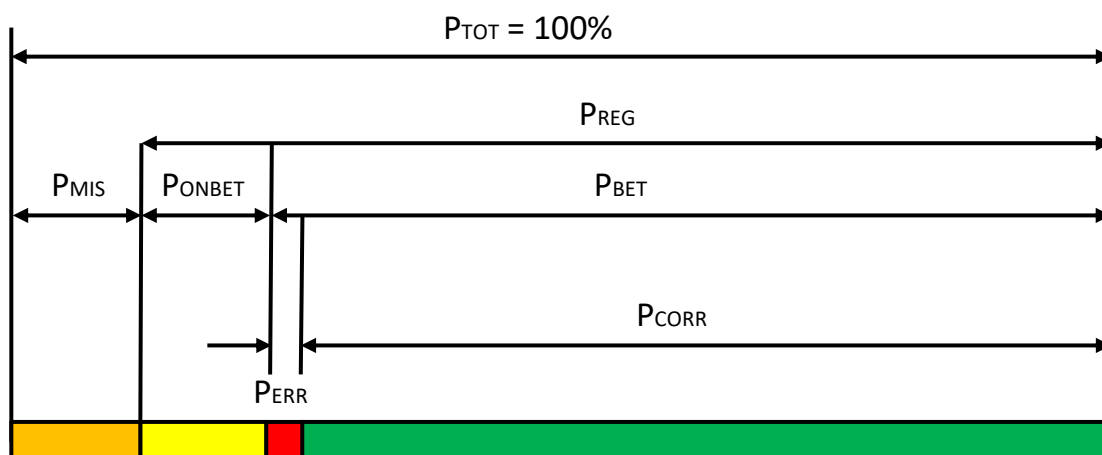
CJIB	Centraal Justitieel Incasso Bureau (CJIB), onderdeel van het Openbaar Ministerie dat de inning van administratiefrechtelijke boetes verzorgd.
Foutpercentage	Het percentage Betrouwbare Hits waarvan het kenteken bij beoordeling door een BOA onjuist blijkt te zijn herkend ($= P_{ERR} / P_{BET}$).
Hitrate	Het percentage motorvoertuigen dat wordt herkend, van alle passerende motorvoertuigen waarvan het kenteken volledig zichtbaar is bij passage van de scanlijn van een ANPR-camera ($= P_{REG} / P_{TOT}$).
IP	Afkorting van: Internet Protocol; protocol dat gebruikt wordt voor onderlinge communicatie.
Kentekendatabase	In- of externe database waarin alle kentekens met een toegangs- of passagerecht voor de locatie zijn geregistreerd.
Kentekenherkenning	Systeem dat de kentekens van voertuigen detecteert en deze aanbiedt voor verificatie bij de Kentekendatabase.
Landcode	De vermelding, op een kentekenplaat, van het land van herkomst van het betreffende kenteken. Het land van herkomst wordt middels een unieke code van 1, 2 of 3 karakters gedefinieerd.
Managementsysteem	Managementcentrale omvattend software (programmatuur), de interne database (en/of de verbinding met de externe database) waarin gegevens worden opgeslagen, inclusief interfaces voor de verbindingen met en tussen systemen.
NPR	Nationaal Parkeer Register, database in beheer bij RDW waarin op kenteken parkeer-, toegangs- en verblijfsrechten worden vastgelegd.
Webbased	Geschreven uitgaande van gestandaardiseerde applicatieservers en ontworpen vanuit het oogpunt om browseronafhankelijk toegankelijk te zijn via het Internet.
Zekerheidspercentage	Het percentage, automatisch gegenereerd door de Kentekenherkenning, waarin met zekerheid het beeld van het kenteken wordt omgezet in de juiste cijfer/letter-combinatie en landcode.

Hieronder wordt de voor de eisen aan de ANPR-apparatuur van toepassing zijnde terminologie gedefinieerd en toegelicht.

Terminologie	Toelichting
Totaal Passages = P_{TOT}	Het totaal van de Passages van een ANPR-cameralocatie in een bepaalde periode. Hierbij dient onderscheid gemaakt te worden naar de relevante categorie zoals Voertuigen met een Nederlands kenteken, Buitenlandse voertuigen of bromfietsen/snorfietsen.
Gemiste registraties = P_{MIS}	Het aantal Passages dat de ANPR-camera niet heeft gedetecteerd en waarvan dus geen Passagegegevens zijn opgeleverd. Oranje in schematische weergave.
Totale aantal geregistreerde Passages ('Hits') = P_{REG}	Dit is het aantal Passages dat de ANPR-camera registreert in een bepaalde periode. Hierbij dient onderscheid gemaakt te worden naar de relevante categorie zoals Voertuigen met een Nederlands kenteken, Buitenlandse voertuigen of bromfietsen/snorfietsen.

Onbetrouwbaar gelezen kentekens = P_{ONBET}	Het aantal Passages in een bepaalde periode dat wel geregistreerd is maar waarvan het kenteken niet of met een te laag betrouwbaarheidspercentage gelezen is en als onbetrouwbaar is geclassificeerd door de Opdrachtnemer. Deze gegevens worden wel doorgegeven. Geel in schematische weergave.
Betrouwbare registraties ('Betrouwbare Hits') = P_{BET}	Dit is het aantal geregistreerde Passages in een bepaalde periode waarvan het kenteken met een voldoende hoog betrouwbaarheidspercentage is gelezen. Hierbij dient onderscheid gemaakt te worden naar de relevante categorie zoals Voertuigen met een Nederlands kenteken, Buitenlandse voertuigen of bromfietsen/snorfietsen.
Fout gelezen kentekens = P_{ERR}	Dit is het aantal registraties in een bepaalde periode waarvan de Opdrachtnemer heeft bepaald dat deze correct gelezen zijn maar die achteraf toch fout blijken te zijn. Rood in schematische weergave. Ten minste de volgende situaties gelden als een fout gelezen kenteken: • Een interpretatie van een willekeurige tekst als kenteken. • Een verkeerde interpretatie van een NL-kenteken. • Het foutief herkennen van één of meer karakters in een kenteken. • Het foutief herkennen van een herkomst-kreis in een Duits kenteken. • Het foutief herkennen van het land van herkomst. • Een dubbele registratie van dezelfde Passage.
Correct gelezen kentekens = P_{CORR}	Het aantal correcte door de Opdrachtnemer aangeleverde kentekens in een bepaalde periode. Groen in schematische weergave.
Nederlands(e) voertuig(en)	Voertuig(en) met een Nederlands kenteken.
Buitenlands(e) voertuig(en)	Voertuig(en) met een kenteken afkomstig uit landen die behoren tot de EU + Verenigd Koninkrijk, Zwitserland, Noorwegen Rusland en Oekraïne.

Schematisch ziet het bovenstaande er als volgt uit:



2 Projectcontext

2.1 Huidige situatie

Binnen de gemeente Eindhoven zijn momenteel op meerdere locaties met geslotenverklaringen automatische bollards en/of handbediende bollards aanwezig. Het betreft de binnenstad, winkelcentrum Meerrijk en de CaDo Noord-Brabantlaan-N2.

Binnenstad

De binnenstad van Eindhoven is sinds vele jaren ingericht als autovrij gebied. Momenteel kent de binnenstad van Eindhoven enkele voetgangerszones en 2 niet-verplichte fietsverbindingen. De toegang tot deze gebieden wordt beperkt door middel van automatische bollards.

Winkelcentrum Meerrijk

Winkelcentrum Meerrijk bevindt zich in de wijk Meerhoven aan de westzijde van Eindhoven, tussen de A2 en Eindhoven Airport. De openbare ruimte tussen de winkels is ingericht als een voetgangerszone. De toegang tot dit gebied wordt beperkt door één automatische bollard voor het ingaande verkeer en één automatische bollard voor het uitgaande verkeer. Bovendien zijn enkele toegangen beperkt tot langzaam verkeer en hulpdiensten, welke zijn afgesloten met verwijderbare palen.

CaDo Noord-Brabantlaan – N2

De Noord-Brabantlaan heeft een ongelijkvloerse kruising met de N2/A2 aan de westzijde van Eindhoven. Ter hoogte van deze kruising ligt een parallelweg langs de Noord-Brabantlaan, die de N2 verbindt met de wijk Meerhoven. Om de maximale aanrijtijden te kunnen halen, is ten behoeve van de hulpdiensten een doorsteek (CalamiteitenDoorsteek, oftewel CaDo) gemaakt tussen de Noord-Brabantlaan en deze parallelweg. De CaDo is afgesloten door middel van 2 bollards.

Al enige tijd zijn reconstructiewerkzaamheden gaande in de binnenstad, waarbij de bollards worden verwijderd en niet meer teruggeplaatst. De Gemeente Eindhoven wil de automatische en handbediende bollards vervangen door een systeem voor Camerahandhaving om de leefbaarheid en verblijfskwaliteit in de achterliggende gebieden blijvend te garanderen. Voor de CaDo geldt dat de camerahandhaving bedoeld is om sluipverkeer staduitwaarts op de Noord-Brabantlaan richting N2-A2 tegen te gaan.

Momenteel zijn ontheffingen in omloop, welke buiten de venstertijden een passagemogelijkheid bieden voor één of meerdere bollards. De geldigheid van de lopende ontheffingen eindigt per 31 december 2024. Alle ontheffinghouders dienen een nieuwe ontheffing aan te vragen voor het nieuwe systeem. Deze aanvraag verloopt via het gemeentelijke e-loket, de ontheffingen worden opgenomen in het Nationaal Parkeer Register (NPR) van RDW.

Milieuzone

Eindhoven kent momenteel een milieuzone binnen de “Ring”. Deze ring bestaat uit Beukenlaan, Marconilaan, Kronehoefstraat, Pastoriestraat, Onze Lieve Vrouwestraat, Insulindelaan, Jeroen Boschlaan, Piuslaan, Leostraat, Boutenslaan, Limburglaan en Botenlaan. De handhaving op de milieuzone vindt momenteel plaats door BOA-controles te voet. Per 1 januari 2025 wordt de huidige milieuzone omgezet in een Zero-Emissiezone voor bedrijfsauto's en vrachtauto's en een milieuzone voor dieselpersonenauto's

Voor de milieuzone zijn ontheffingen in omloop. Voor de Zero-Emissiezone wordt aangesloten bij het landelijke Centraal Loket. Alle verleende ontheffingen worden opgenomen in het Nationaal Parkeer Register (NPR) van RDW.

2.2 Randvoorwaarden en uitgangspunten

Visie Opdrachtgever

Gemeente Eindhoven wenst dat de voetgangersgebieden door bezoekers als gastvrij wordt beschouwd, als gebieden waar eenieder welkom is. Tegelijkertijd wenst de Gemeente voor de bewoners binnen deze gebieden een leefbare woonomgeving te bieden. Beperking van het autoverkeer door middel van selectieve toegang dient op een gastvrije manier bij te dragen aan de leefbaarheid van de voetgangersgebieden.

Voor wat betreft de CaDo wenst Gemeente Eindhoven dat de verkeersveiligheid op de Noord-Brabantlaan en de toerit naar en afrit van de N2 wordt geborgd. Dit houdt in dat sluijverkeer via de CaDo ongewenst wordt geacht.

Gemeente Eindhoven heeft de ambitie om in 2030 binnen het gebied binnen de Ring een Zero-Emissiezone voor alle mobiliteit in te stellen. De per 2025 in te voeren Zero-Emissiezone is een opstap naar deze ambitie, waarbij een effectief systeem van toezicht en handhaving van groot belang wordt geacht.

Wet en Regelgeving

Zowel de Apparatuur zelf als de Opdrachtnemer bij installatie- en onderhoudswerkzaamheden, dient te voldoen aan alle in Nederland geldende wet- en regelgeving, waaronder ARBO- en veiligheidsregels en NEN-normeringen (waaronder NEN1010 en NEN3140).

Projectomvang

De globale omvang van dit project behelst:

- De levering, implementatie en gebruiksklare oplevering van een systeem voor ANPR-Camerahandhaving (inclusief back-office en handhavingsfunctionaliteit) voor de Zero-Emissiezone en RVV-bebording C1 en G7.
- Het gedurende minimaal 10 jaar verzorgen van het technisch beheer en onderhoud en doorvoeren van alle softwarematige updates en upgrades van de geleverde systemen, waarvoor een SLA wordt aangeboden teneinde de bedrijfszekerheid te garanderen.
- Het bieden van een continuïteitsgarantie voor minimaal 10 jaar op het voortdurend conform de gestelde eisen kunnen functioneren van het geleverde systeem.

Tot dit project behoort niet:

- Het leveren en plaatsen van bebording nabij de Cameralocaties.
- Het leveren en implementeren van een e-loket en/of vergunningapplicatie.
- Het verwijderen van de bestaande bollards en bebording.
- Het leveren van eventueel benodigde simkaarten t.b.v. data-communicatie, deze worden indien van toepassing door de Opdrachtgever beschikbaar gesteld.
- Het operationeel en functioneel beheer.

Randvoorwaarden

De volgende randvoorwaarden zijn van toepassing:

- Het systeem dient voor 1 juni 2025 volledig operationeel te worden opgeleverd.
- De vaste Camera's kunnen worden aangesloten op 230V-voedingskasten, voor zover deze op de huidige locaties aanwezig en beschikbaar zijn.

- Ongeacht of 230V-voedingskast beschikbaar is, is de Opdrachtnemer voor elke locatie verantwoordelijk voor de tijdige realisatie en de coördinatie van een voedingsaansluiting. De kosten voor de realisatie van deze aansluitingen komen voor rekening van de Opdrachtgever.
- De te leveren back-office inclusief handhavingsfunctionaliteit dient als een SAAS-oplossing te worden aangeboden.

2.3 Leveringsomvang

Het te leveren systeem bestaat op hoofdlijnen uit de volgende onderdelen:

- ANPR-camera's
 - o Tenminste 20 vaste locaties voor voetgangersgebied binnenstad
 - o 2 vaste locaties voor CaDo Noord-Brabantlaan
 - o 2 tot 4 vaste locaties voor voetgangersgebied Meerrijk
 - o 12 vaste en 3 verplaatsbare locaties voor Zero-Emissiezone
- 1 Managementsysteem met opslagfunctie inclusief handhavingsfunctionaliteit
- Licenties voor ten minste 30 BOA's t.b.v. het uitvoeren van beoordelingen, waarbij ten minste 5 BOA's tegelijkertijd beoordelingen kunnen uitvoeren.
- Interfaces met het NPR, het Kentekenregister en de verwerkingsmodule van CJIB.

2.4 Beheerprocessen

Ten aanzien van de beheerprocessen maakt Opdrachtgever onderscheid naar operationele, functionele en technische beheerprocessen van het systeem.

Operationeel beheer

Het operationeel beheer van het te leveren systeem betreft alle werkzaamheden die betrekking hebben op de primaire bedrijfsvoeringsprocessen (het geautomatiseerd bepalen van mogelijk overtredingswaardige situaties, het beoordelen van mogelijk overtredingswaardige situaties). Hierbij kan bijvoorbeeld gedacht worden aan het genereren van rapportages. De Opdrachtgever wenst het operationeel beheer volledig zelf te kunnen uitvoeren.

Functioneel beheer

Het functioneel beheer van het te leveren systeem betreft het, waar nodig, actualiseren van de input op basis waarvan het systeem zijn functionaliteit vervult. Hierbij kan bijvoorbeeld gedacht worden aan het autoriseren van BOA's om beoordelingen uit te voeren of het softwarematig tijdelijk of permanent wijzigen van tijdvakken waarbinnen (individuele) Camera's geactiveerd zijn of het op afstand in- dan wel uitschakelen van (individuele) Camera's. De Opdrachtgever wenst het functioneel beheer volledig zelf te kunnen uitvoeren.

Technisch beheer

Onder technisch beheer wordt verstaan het in technische zin zorgen voor de operationele beschikbaarheid van het systeem. Naast preventief en correctief onderhoud aan hard- en softwarematige componenten, behoort hiertoe ook het doorvoeren van softwareupdates en –upgrades. De Opdrachtgever wenst het technisch beheer volledig te laten verzorgen door de Opdrachtnemer.

3 Functionele eisen

In dit hoofdstuk zijn de functionele eisen aan het te leveren systeem voor Camerahandhaving opgenomen. Het te leveren systeem dient te functioneren als handhavingsmiddel voor controle op het inrijdend verkeer in de verkeersluwe gebieden en de Zero-Emissiezone en het passerend verkeer niet-zijde hulpdiensten langs de CaDo.

3.1 Algemene beheereisen

- 3.1.1 Alle onderdelen van het systeem dienen aantoonbaar in de aangeboden vorm elders reeds werkend te zijn opgeleverd.
- 3.1.2 De functionele eisen uit dit PvE dienen alle met de SAAS oplossing van de opdrachtnemer te kunnen worden gerealiseerd. De benodigde aanvullende software-oplossingen dienen expliciet te worden benoemd bij de inschrijving.
- 3.1.3 Het systeem dient door de Opdrachtgever vrij configureerbaar te zijn ten aanzien van ten minste de Bedrijfstijden, venstertijden, coulancetijden en categorie van overtreding, zowel per afzonderlijke locatie als voor groepen van locaties als alle locaties tezamen.
- 3.1.4 Alle data die binnen het systeem worden opgeslagen, worden eigendom van Opdrachtgever. Opdrachtnemer is en blijft verantwoordelijk voor de correcte opslag van de data, er mag geen data verloren gaan.
- 3.1.5 Alle documentatie en toelichtingen, zowel op papier als digitaal, van het systeem zijn volledig in de Nederlandse taal gesteld.
- 3.1.6 Alle fysieke sloten, cilinders en sleutels dienen te zijn voorzien van een SKG-certificaat. Alle benodigde sleutels dienen in 3-voud te worden meegeleverd. De sloten dienen zelfvoorzienend te zijn qua energiebehoefte.
- 3.1.7 Opdrachtnemer dient te garanderen dat het systeem volledig voldoet aan de vereisten van AVG. Opdrachtnemer gaat zonder voorbehoud akkoord met de Verwerkersovereenkomst inclusief addendum, zoals opgenomen in de aanbestedingsdocumentatie.
- 3.1.8 Het systeem biedt de mogelijkheid voor het instellen van minimaal 3 autorisatieniveaus; op elk niveau dienen uitsluitend autorisaties op naam te kunnen worden aangemaakt. Opdrachtgever dient zelfstandig autorisaties te kunnen instellen, muteren en beëindigen.
- 3.1.9 Bij de levering behoort opleidingen/trainingen van minimaal 1 dag op locatie bij de Opdrachtgever voor training, uitleg en "learning on the job" voor de technisch en operationeel beheerders (maximaal 5 personen) alsmede de beoogde gebruikers van de handhavingsfunctionaliteit (maximaal 25 personen).

3.2 Eisen aan Camera's en masten

- 3.2.1 De Camera's staan op dan wel zijn bevestigd aan een mast, op een hoogte van minimaal 4,00 boven het omliggende maaiveld.
- 3.2.2 De Camera's voor de Zero-Emissiezone dienen met bevestigings- of klembeugels bevestigd te worden aan een bestaande mast voor openbare verlichting. Beschadigingen aan deze masten dienen hierbij te worden voorkomen door toepassing van neopreen tussen de beugels en masten. In bijlagen 1a en 1b zijn de aan te houden locaties opgenomen.
- 3.2.3 De te leveren masten dienen te zijn voorzien van inklimbeveiliging.

- 3.2.4 Het is toegestaan de te leveren masten te voorzien van een kantelmechanisme ten behoeve van beheerdoeleinden, doch uitsluitend indien voor de inschakeling van dit kantelmechanisme discussloten met specifieke, niet-algemeen verkrijgbare sleutels toegepast dienen te worden dan wel daaraan gelijk te stellen instrumenten. Alle discussloten dienen met één sleutel geopend te kunnen worden.
- 3.2.5 De toe te passen Camera's voor de voetgangersgebieden en de CaDo dienen IP-based te zijn en van voldoende resolutie om duidelijk afleesbare kentekens en contouren van het voertuig te presenteren (conform vereiste parket CVOM), ongeacht de weersomstandigheden of dag-/nachtsituatie.
- 3.2.6 De toe te passen Camera's voor de Zero Emissie-zone dienen IP-based te zijn en van voldoende resolutie om duidelijk afleesbare kentekens en contouren van het motorvoertuig te presenteren (conform vereiste parket CVOM), ongeacht de weersomstandigheden of dag-/nachtsituatie.
- 3.2.7 De Camera's voor de voetgangersgebieden en de CaDo dienen minimaal beelden van het kenteken van het passerende voertuig alsmede beelden waaruit onomstotelijk blijkt dat het voertuig de op de locatie aanwezige bebording is gepasseerd, te tonen.
- 3.2.8 De exacte posities van de Camera's voor de voetgangersgebieden en de CaDo worden na opdrachtverlening op locatie bepaald in samenspraak tussen Opdrachtgever en Opdrachtnemer.
- 3.2.9 De Opdrachtnemer dient te garanderen dat de firmware van de Camera's geupdatet blijft worden gedurende minimaal 10 jaar. Indien security-issues optreden met een CVE-score 8 of hoger, dienen deze binnen 3 maanden te worden hersteld door middel van een firmware-update.
- 3.2.10 Bij uitval van de verbinding tussen een Camera en het Managementsysteem dient de Camera de gedurende minimaal 48 uren na uitval van de verbinding gelezen kentekens met de bijbehorende data, waaronder het tijdstip en foto's van de passage, te bewaren en aan te bieden op het moment dat de verbinding is hersteld.
- 3.2.11 De Camerabehuizing dient aantoonbaar te voldoen aan IP66.
- 3.2.12 Na montage van de Camera's dienen kabels tot een hoogte van minimaal 3,50 meter afgewerkt te zijn in flexibele metalen buizen.
- 3.2.13 De masten en Camera's dienen, bij uitvoering van onderhoud conform de voorschriften van de leverancier, minimaal 10 jaar niet te corroderen.
- 3.2.14 De Camera's dienen richtinggevoelig instelbaar te zijn.
- 3.2.15 Op het beeld met de overtreding moet een tekstvak worden geplaatst waarin de onderstaande teksten duidelijk leesbaar en chronologisch moeten worden geplaatst:
- Een voor de betreffende Camera in combinatie met de locatie uniek foto ID-nummer
 - Datum en tijdstip overtreding conform de in Nederland gebruikelijke datumaanduiding, namelijk dag-maand-jaar en vervolgens het tijdstip volgens 24 uurssysteem aangeduid in seconden.
 - Locatie van overtreding conform BPS¹ en rijrichting voertuig.
 - Kenteken en land van herkomst van het voertuig.
 - Feitcodevermelding van het soort overtreding, afhankelijk van de locatie is dit:
 - o R315a voor bestuurders van motorvoertuigen bij de toegangen tot de voetgangerszones

¹ Beschrijvende Plaatsaanduiding Systematiek (zie: publicaties.minienm.nl/documenten/beschrijvende-plaatsaanduiding-systematiek-bps-1994)

- R311 voor bromfietzers bij de toegangen tot de voetgangerszones
- R309 voor snorfietzers bij de toegangen tot de voetgangerszones
- R559 voor bestuurders van motorvoertuigen bij de CaDo
- R571g voor bestuurders van vrachtauto's bij de toegangen tot de Zero-Emissiezone
- R571h voor bestuurders van bedrijfsauto's of bussen bij de toegangen tot de Zero-Emissiezone

3.3 Eisen aan Kentekenherkenning

- 3.3.1 Kentekenherkenning is van toepassing voor alle kentekenplichtige voertuigen met Nederlandse en Buitenlandse kentekens.
- 3.3.2 De Kentekenherkenning dient onder alle weersomstandigheden, uitgezonderd (natte) sneeuwval te kunnen werken en de gestelde prestatie-eisen te behalen.
- 3.3.3 De minimaal vereiste Hitrate van de Kentekenherkenning bedraagt voor voertuigen 98,5% en voor brom- en snorfietzen 95%.
- 3.3.4 Het vereiste Zekerheidspercentage van de Kentekenherkenning bedraagt: minimaal 90% voor Nederlandse kentekens, minimaal 80% voor Buitenlandse kentekens.
- 3.3.5 Het minimaal vereiste Betrouwbaarheidspercentage van de Kentekenherkenning bedraagt voor motorvoertuigen met een niet-bromfietskenteken: 98% voor Nederlandse kentekens, 95% voor Buitenlandse kentekens.
- 3.3.6 Het minimaal vereiste Betrouwbaarheidspercentage van de Kentekenherkenning bedraagt voor motorvoertuigen met een bromfietskenteken: 95% voor Nederlandse kentekens, 92% voor Buitenlandse kentekens.
- 3.3.7 Het maximaal toegestane Foutpercentage van de Kentekenherkenning bedraagt, ongeacht de voertuigcategorie: 0,15%.
- 3.3.8 Het maximaal toegestane onjuist herkende Landcodes bedraagt, ongeacht de Landcode: 2,5%.
- 3.3.9 Genoemde prestatie-eisen dienen op elk moment behaald te worden voor voertuigen met een maximumsnelheid van 100 km/uur.

3.4 Eisen aan het Managementsysteem

- 3.4.1 Het Managementsysteem dient alle aangesloten apparatuur aan te kunnen sturen en uitbreidbaar te zijn met op een later tijdstip te plaatsen Camera's.
- 3.4.2 Het Managementsysteem dient voorzien te zijn van atoomkloksynchronisatie dan wel gelijkwaardig, en de tijden van alle aangesloten apparatuur gelijk te kunnen stellen. Het Managementsysteem voorziet in aanpassingen aan zomer- en wintertijd alsmede schrikkeljaren.
- 3.4.3 Het Managementsysteem dient voor elke Camera separaat venstertijden te kunnen instellen, wijzigen en uitschakelen.

- 3.4.4 Het Managementsysteem dient voor elk herkend kenteken het Nationaal Parkeer Register (NPR) te bevragen of dit een geldig toegangsrecht voor de betreffende locaties heeft. Deze bevraging dient direct na herkenning van het kenteken plaats te vinden en dient, indien nodig en/of gewenst door Opdrachtgever, op een vast instelbaar later tijdstip (bijvoorbeeld 23:59 uur of 24 uur na het tijdstip van herkenning) herhaald te kunnen worden. Voor de Cameralocaties van de Zero-Emissiezone geldt dat het Managementsysteem, uitsluitend voor voertuigen die behoren tot één van de geselecteerde voertuigcategorieën, van elk herkend kenteken het NPR dient te bevragen op een geldig toegangsrecht.
- 3.4.5 Pas nadat de bevraging of herhaalde bevraging (zie 3.4.4) heeft geleid tot een bevestiging dat sprake is van een geldig toegangsrecht voor de betreffende locatie, worden de beelden van een herkend kenteken verwijderd uit het Managementsysteem.
- 3.4.6 De beelden van elk voertuig waarvan het kenteken niet of met onvoldoende betrouwbaarheid wordt herkend, dienen te worden opgeslagen als een werkvoorraad ten behoeve van beoordeling door een BOA. Een geautoriseerde BOA dient van dergelijke voertuigen handmatig het kenteken in te kunnen voeren of te muteren, waarna direct een hernieuwde bevraging (zie 3.4.4) plaats dient te vinden.
- 3.4.7 Het Managementsysteem dient te beschikken over een whitelist-functionaliteit waarbij voor elk ingevoerd kenteken instelbaar is of sprake is van een toegangsrecht, centraal en indien nodig naar afzonderlijke locatie. Het invoeren van kentekens op deze whitelist-functionaliteit mag niet kunnen plaatsvinden door een BOA die beoordelingen uitvoert. Voor elk herkend kenteken dient het Managementsysteem te beoordelen of deze voorkomt op de actuele whitelist, waardoor de registratie niet meer wordt aangeboden aan de BOA ter beoordeling.
- 3.4.8 De beelden van elk voertuig waarvan het kenteken met voldoende of onvoldoende betrouwbaarheid is herkend (of dit kenteken handmatig is ingevoerd) én dit kenteken niet beschikt over een geldig toegangsrecht voor de betreffende locatie, dienen te worden opgeslagen als een werkvoorraad ten behoeve van beoordeling door een BOA.
- 3.4.9 Het Managementsysteem dient over voldoende opslagcapaciteit te beschikken om de hiervoor bedoelde beelden gedurende de wettelijke maximale toegestane 72 uur op te slaan als werkvoorraad.
- 3.4.10 Een geautoriseerde BOA dient vanaf elke werkplek binnen het ICT-netwerk van Gemeente Eindhoven de beoordelingen uit te kunnen voeren, door met behulp van een IP-protocol en 2-Factor-Authenticatie in te loggen op het Managementsysteem, zonder dat hiervoor aanvullende software of tools geïnstalleerd of gedownload behoeven te worden.
- 3.4.11 In de handhavingsfunctionaliteit dient een BOA de beoordeling “geen overtreding”, “waarschuwing” (uitsluitend indien wordt voldaan aan nader te definiëren, door de Opdrachtgever instelbare criteria) en “overtreding” te kunnen geven.
- 3.4.12 In de handhavingsfunctionaliteit dienen ten behoeve van de beoordeling door een BOA (zie 3.4.8) van elk voertuig de historische gegevens (op datum opgelegde waarschuwingen en beschikkingen) te worden getoond.
- 3.4.13 In de handhavingsfunctionaliteit dient, in geval van meerdere overtredingen van één kenteken, al dan niet bij dezelfde locatie, een overzicht van deze overtredingen te worden getoond. Een BOA dient, indien sprake is van meerdere overtredingen van één kenteken binnen een bepaald tijdsbestek, uit de lijst van overtredingen te kunnen aanvinken welke worden gesanctioneerd.

- 3.4.14 Indien de BOA beoordeelt dat sprake is van een “overtreding”, dienen de registratiegegevens door het Managementsysteem, middels een koppeling met het Kentekenregister van RDW, automatisch te worden verrijkt met de benodigde voertuiggegevens en te worden klaargezet in een voorraad ‘te verzenden’, welke periodiek wordt geëxporteerd ten behoeve van een upload naar de dienst BUBS (Bulk Upload Berichten Service) van het Centraal Justitieel Incasso Bureau. Deze export dient batchgewijs door de BOA te worden uitgevoerd aan het einde van een sessie in de handhavingsfunctionaliteit, voordat de BOA uit kan loggen uit de handhavingsfunctionaliteit. Alleen een teamleider van de BOA’s dient de exports daadwerkelijk te kunnen uploaden naar de dienst BUBS van het CJIB.
- 3.4.15 Indien de BOA beoordeelt dat sprake is van een “waarschuwing”, dienen de registratiegegevens door het Managementsysteem, middels een koppeling met het Kentekenregister van RDW, automatisch te worden verrijkt met de benodigde voertuig- en houdergegevens en te worden klaargezet voor een export ten behoeve van de verzending van een waarschuwingsbrief, indien het Managementsysteem deze functionaliteit niet biedt.
- 3.4.16 In de handhavingsfunctionaliteit dient de mogelijkheid te zijn opgenomen om per Camera bepaalde voertuigcategorieën te filteren (bijvoorbeeld op basis van de samenstelling van het kenteken of de onderscheiden voertuigcategorieën van het RDW) en niet op te nemen in de werkvoorraad ten behoeve van beoordeling door een BOA.
- 3.4.17 De beelden van elk voertuig waarvan door de BOA wordt beoordeeld dat sprake is van een “overtreding” dienen gedurende minimaal 5 jaar te worden opgeslagen.
- 3.4.18 Het Managementsysteem dient op basis van de invoer van een kenteken alle overtredingen op datum te tonen en van elk van deze overtredingen één document te kunnen samenstellen die voorziet in alle door CVOM benodigde informatie voor de afhandeling van bezwaarschriften, waarbij ten minste een goed leesbare uitsnede van het kenteken als kader is opgenomen.
- 3.4.19 Het Managementsysteem dient te beschikken over een telssystematiek waarmee per afzonderlijke Cameralocatie de tijdstippen van passages worden vastgelegd (indien mogelijk op basis van voertuigcategorie), inclusief de beoordeling of dit een “geldige” of “ongeldige” passage betreft.
- 3.4.20 Het Managementsysteem dient te beschikken over een telssystematiek waarmee per afzonderlijke Cameralocatie de tijdstippen van passages worden vastgelegd, inclusief de beoordeling of dit een passage van een “herkend” of “niet herkend” kenteken betreft. Met “niet herkend” wordt in dit kader bedoeld die voertuigen waarvan het kenteken met onvoldoende betrouwbaarheid is herkend. Deze voertuigen dienen tevens in de werkvoorraad te worden geplaatst t.b.v. handmatige invoer (lees: correctie herkende tekens) van het kenteken.
- 3.4.21 Het Managementsysteem dient te beschikken over een functionaliteit welke per afzonderlijke Cameralocatie alle gebeurtenissen, voorzien van een eenduidig tijdsstempel, worden geregistreerd. Deze gebeurtenissen dienen minimaal 1 jaar te worden bewaard.
- 3.4.22 Het Managementsysteem dient te beschikken over een recidive-functie. Deze functie houdt in dat kentekens met een eerste overtreding binnen een door Opdrachtgever vrij instelbare periode een waarschuwing ontvangen en pas bij een tweede overtreding binnen deze periode een beschikking, dan wel binnen een vrij instelbare periode een 2e, 3e, etc. beschikking.
- 3.4.23 Het Managementsysteem dient voor alle aangesloten apparatuur een storingsmelding te kunnen genereren en deze als ‘push-melding’ actief te verzenden naar nader op te geven e-mailadressen en/of mobiele telefoonnummers van de 1^e lijns beheerder(s).
- 3.4.24 Het Managementsysteem dient een goede performance te bieden. Onder een goede performance wordt in ieder geval verstaan:
- Opstarten applicatie: maximaal 10 seconden

- Wisseling gegevensveld: maximaal 1,0 seconden
 - Schermwisseling: maximaal 2,0 seconden
- 3.4.25 Het Managementsysteem dient op enig moment zonder meerkosten geschikt te maken te zijn voor handhaving op andere dan de initieel uitgevraagde toegangsbeperkingen (bijvoorbeeld: lengtebeperking, milieuzonering), voor zover deze beperkingen kentekengebonden zijn en opvraagbaar uit een externe database (bijvoorbeeld: NPR of Kentekenregister).

3.5 Eisen aan communicatie en rapportage

- 3.5.1 De data uit het Managementsysteem dient vrij toegankelijk te zijn voor de Opdrachtgever. Dat betekent dat het mogelijk moet zijn om, los van de rapportages vanuit het Managementsysteem, alle data te exporteren naar een rapportagevorm die de Opdrachtgever wenst. De leverancier dient dit mogelijk te maken door toepassing van open data communicatie.
- 3.5.2 Gedurende de technische levensduur van het systeem dient de open data communicatie kosteloos ondersteund te worden. Eventuele updates van de software hebben geen invloed op de koppeling met de data en indien dat wel het geval is, dient Opdrachtnemer deze koppeling kosteloos te herstellen.
- 3.5.3 Het gebruik van de gegevens uit de database dient zonder additionele kosten en zonder additionele licenties gedurende de gehele technische levensduur van het systeem mogelijk te zijn voor Opdrachtgever.
- 3.5.4 Binnen het Managementsysteem dienen standaard query's aanwezig te zijn waarmee in een beperkt aantal stappen een standaardrapportage gegenereerd kan worden. Tenminste de volgende rapportages dienen door middel van een eenvoudige handeling opgeroepen kunnen worden binnen het Managementsysteem:
- Aantal passages per locatie binnen een vrij instelbare periode.
 - Aantal passages van niet-ontheffing houders per locatie binnen een vrij instelbare periode.
 - Aantal ten behoeve van een upload naar de Transactiemodule van CJIB geëxporteerde overtredingen per locatie binnen een vrij instelbare periode.
 - Aantal handmatig gewiste beelden van passages (inclusief geregistreerde login-/gebruikersnaam waaronder is gewist en eventuele meegegeven toelichting)
 - Overzicht van de storingen in het Managementsysteem binnen een vrij instelbare periode.
 - Beschikbaarheid van de Camera en Kentekenherkenning per locatie binnen een vrij instelbare periode.
 - De Hitrate per locatie binnen een vrij instelbare periode.
 - Het Foutpercentage per locatie binnen een vrij instelbare periode.
 - Een SLA-rapportage inzake de performance van elke afzonderlijke camera en het ANPR-camerasysteem.
- 3.5.5 De Opdrachtnemer dient elk kwartaal via Teams operationeel overleg te voeren met de Opdrachtgever inzake het dagdagelijks systeembeheer.
- 3.5.6 Ieder kwartaal wordt de gang van zaken met betrekking tot de Overeenkomst en de kwaliteit van de geleverde dienstverlening geëvalueerd ten kantore van de Opdrachtgever. De gespreksonderwerpen worden in overleg tussen de Opdrachtgever en de Opdrachtnemer vastgesteld en nader bepaald.
- 3.5.7 Gedurende het 1e jaar na implementatie kan op initiatief van de Opdrachtgever een hogere overlegfrequentie dan elk kwartaal worden aangehouden.

- 3.5.8 In geval van calamiteiten of wanneer de Opdrachtgever en/of de Opdrachtnemer aanleiding ziet om in extra overleg te treden, dienen beide partijen hier hun medewerking aan te verlenen.
- 3.5.9 De Opdrachtnemer dient ieder kwartaal een rapportage aan te leveren, waarin ten minste is opgenomen:
- systeemprestaties,
 - systeemstoringen en oplostijden,
 - beschikbaarheid per maand per camera en van het Managementsysteem,
 - mutaties,
 - uitgevoerd onderhoud,
 - security incidenten

3.6 Eisen aan de FAT, uitvoering en SAT

- 3.6.1 Indien het systeem fabrieksklaar is en de complete levering voor installatie gereed is, wordt een FAT (Factory Acceptance Test) bij de Opdrachtnemer uitgevoerd. Indien tijdens deze FAT wordt geconstateerd dat de installatie niet volledig voldoet aan het voorliggende PvE en/of bepaalde zaken niet gebruiksklaar zijn voor installatie, wordt het volledige systeem niet afgenomen. In overleg wordt dan een termijn voor herstel bepaald, waarna een hernieuwde FAT wordt afgenomen. De hieruit voortvloeiende kosten zijn volledig voor rekening van Opdrachtnemer.
- 3.6.2 Onderdeel van de SAT is het verkrijgen van goedkeuring van het CVOM voor het fotomateriaal en brondocument van een overtredenswaardige passage. Dit fotomateriaal en brondocument dient uiterlijk twee weken na livegang door de Opdrachtnemer te worden samengesteld en aangeleverd aan de Opdrachtgever.
- 3.6.3 Voor zover onderdelen van het systeem “buiten” gerealiseerd worden, dient deze realisatie uitgevoerd te worden door bedrijven en medewerkers welke VCA gecertificeerd zijn.
- 3.6.4 Voor zover de werkzaamheden “buiten” dit vereisen, dient bij de uitvoering gewerkt te worden conform CROW-publicatie 96b.
- 3.6.5 Nadat de installatie op locatie is voltooid en de Opdrachtnemer het systeem heeft getest vindt de SAT-test (Site Acceptance Test) plaats. Binnen deze test worden alle apparaten en verbindingen getest onder gebruikers-omstandigheden, en vinden functionele en gebruikersacceptatietesten plaats. De Opdrachtnemer levert minimaal 2 weken voorafgaand aan de SAT een testplan en checklisten ter goedkeuring aan de Opdrachtgever. In dit plan dient de omvang van steekproeven gemotiveerd onderbouwd te worden, rekening houdend met een statistische bias.
- 3.6.6 Wanneer de SAT met goed gevolg wordt doorlopen, wordt het systeem formeel opgeleverd en in bedrijf gesteld. Ontbrekende punten die in bedrijfstelling niet in de weg staan worden opgenomen in een opleveringsprotocol. Als deze punten zijn opgelost vindt de eindoplevering en afrekening van de laatste betaaltermijn plaats. De garantie gaat in nadat alle punten zijn opgeleverd.

- 3.6.7 Na inbedrijfstelling van het Managementsysteem en de betreffende camera's dient voor de Zero Emissiezone gedurende 4 maanden te worden gewaarschuwd in plaats van gehandhaafd, waarbij elke 3 weken één waarschuwingsbrief worden verstuurd aan de houder van één of meerdere Nederlandse kentekens waarvoor in die periode ten minste één passage als waarschuwing is beoordeeld. Voor de voetgangerszones en de CaDo is deze waarschuwingstermijn 4 weken vanaf de inbedrijfstelling van de betreffende camera's, waarbij wekelijks één waarschuwingsbrief dient te worden verzonden aan de houder van één of meerdere Nederlandse kentekens waarvoor in die periode ten minste één passage als waarschuwing is beoordeeld.
- 3.6.8 De kosten voor de waarschuwingsbrieven gedurende de 4 maanden na de initiële inbedrijfstelling van het Managementsysteem en de camera's voor de Zero Emissiezone alsmede de 4 weken na de inbedrijfstelling van de camera's voor de voetgangerszones en de CaDo komen voor rekening van Opdrachtnemer.

3.7 Eisen aan documentatie

- 3.7.1 Bij de oplevering dient ten minste de volgende documentatie te worden geleverd:
- Gebruikersdocumentatie
 - Systeemdokumentatie
 - Architectuur
 - Overzichtstekening met locaties van hardware
 - Hardwarecomponenten
 - Naam
 - Merk-type
 - IP-nummer-subnet-gateway
 - MAC-adres
 - Firmware
 - Relevante setting
 - Verbinding
 - Installatiedatum +foto
 - GPS-coördinaten
 - Specifieke opmerkingen
 - Interface-specificaties
 - Specifieke projectdocumentatie
 - Een releaseplanning van de software (jaarlijks geupdatete planning aan te leveren aan Opdrachtgever).
- 3.7.2 De Opdrachtnemer houdt, naast de verplichte documentatie die in Artikel 6 en 14 in de GIBIT worden gesteld, actuele overzichten, documentatie en handleidingen bij en stelt deze beschikbaar aan de Opdrachtgever met minimaal de volgende eigenschappen voor SaaS applicaties:
- Handleiding tbv het vervangen van certificaten/secret keys gebruikt door de ICT Prestatie bij Azure application tbv SSO/SCIM
 - Een overzicht van de parametrisering van de ICT Prestatie
 - Gebruikte http-requestmethoden (GET, POST)
 - Informatie in de http-headers die voor het functioneren van belang zijn
 - Poorten en protocollen van en naar de Programmatuur zijn vastgelegd, dit mag in de vorm van een overzicht of netwerktekening

- 3.7.3 De Opdrachtnemer beschikt over en verstrekt (geanonimiseerd) aan de Opdrachtgever de Incident Response procedure welke minimaal voldoet aan de ISO 27001 template.
- 3.7.4 De Opdrachtnemer beschikt over en verstrekt aan de Opdrachtgever de Coordinated Vulnerability Disclosure procedure, dit mag via een publiek beschikbare security.txt file. Deze moet voldoen aan de richtlijnen van NCSC.
- 3.7.5 Het ANPR-Camerasysteem dient een audit trail te loggen van alle transacties en wijzigingen waarbij de logging minimaal het volgende bevat (indien van toepassing):
- Een tot een natuurlijke persoon herleidbare gebruikersnaam of ID;
 - De gebeurtenis;
 - Waar mogelijk de identiteit van het werkstation;
 - Host naam;
 - Naam van de toepassing;
 - IP-adres(sen);
 - Het object waarop de handeling werd uitgevoerd;
 - Het resultaat van de handeling;
 - De datum en het tijdstip van de gebeurtenis.

De logging wordt minimaal 1 jaar bewaard en bij het voorkomen van een incident wordt de logging omtrent het incident 3 jaar bewaard.

3.8 Eisen aan beheer en onderhoud

- 3.8.1 De Opdrachtnemer dient aan te geven op het prijzenblad welke garantieperiode hij voor het totale systeem afgeeft, met een minimum van 3 jaar voor de camera's en masten en 1 jaar voor de overige onderdelen van het systeem. Gedurende de looptijd van de overeenkomst worden alle technische storingen, met uitzondering van storingen als gevolg van aanrijdingen, blikseminslag of vandalisme, door de Opdrachtnemer kosteloos op werkdagen binnen 24 uur na melding opgelost. Voorrijkosten en kosten voor (het verzenden van) onderdelen dienen hierbij te zijn inbegrepen en kunnen niet in rekening worden gebracht.
- 3.8.2 Het systeem bestaat uit hardware-, software- en netwerkcomponenten die van afstand worden bewaakt en beheerd en remote worden onderhouden.
- 3.8.3 Opdrachtgever dient het eenzijdige recht te hebben de te sluiten onderhoudsovereenkomst / SLA jaarlijks te verlengen tot een maximale periode van 10 jaren, waarbij de kosten vanaf 1 januari 2026 jaarlijks maximaal kunnen worden geïndexeerd met de jaarmutatie per september van het voorafgaande jaar van de CPS-index alle huishoudens (2015=100, of het meest recente basisjaar indien dit wijzigt gedurende de looptijd van de onderhoudsovereenkomst): <http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=82838NED&D1=3,10&D2=0&D3=13&D4=a&D5=a&HDR=T,G1,G3&STB=G2,G4&VW=T>
- 3.8.4 Voorstellen voor een prijswijziging dienen door Opdrachtnemer minimaal 1 maand voor toepassing schriftelijk bekend te worden gemaakt aan de Opdrachtgever. De Opdrachtnemer dient het voorstel, voorzien van nieuwe prijslijsten, gespecificeerd en met referte aan de overeenkomst in te dienen.
- 3.8.5 Voor het indienen, monitoren en bewerken van calls en het reageren op ingediende calls dient de Opdrachtnemer 24/7 een digitale omgeving beschikbaar te stellen.
- 3.8.6 Opdrachtnemer beschikt gedurende de gehele looptijd van de overeenkomst over een telefonische helpdesk die op werkdagen minimaal tussen 08.00 en 17.00 uur bereikbaar is, alsmede een te allen tijde telefonisch bereikbare piketdienst.
- 3.8.7 Bij de telefonische helpdesk en overige ondersteuning dient Nederlands de voertaal te zijn.

- 3.8.8 De reactietijd voor het opnemen van telefoontjes bedraagt maximaal 20 seconden.
- 3.8.9 Het minimale service-window van de Opdrachtnemer voor het oplossen van aangemelde problemen is maandag tot en met vrijdag, van 08.00 tot 17.00 uur.
Onderhoudswerkzaamheden die de werking van (delen van) het ANPR-Camerasysteem verstoren, dienen in overleg met de Opdrachtgever te worden ingepland.
- 3.8.10 Meldingen dienen geprioriteerd te worden met een verwijzing naar reactietijden en oplostijden
- 3.8.11 Een Escalatie matrix is in kaart gebracht voor het geval dat de afgesproken servicelevels niet worden nageleefd
- 3.8.12 Opdrachtnemer beschikt in Nederland over tenminste 10 monteurs die aantoonbaar gekwalificeerd zijn voor het uitvoeren van onderhoudswerkzaamheden aan het systeem.
- 3.8.13 Opdrachtnemer verzorgt 1 keer per jaar een preventieve onderhoudsronde, inclusief schoonmaak, van de camera's, inclusief verslaglegging van de bevindingen en ondernomen acties/werkzaamheden alsmede advisering ten aanzien van te ondernemen acties/werkzaamheden.
- 3.8.14 Opdrachtnemer doet minimaal 2 weken van tevoren aan Opdrachtgever een voorstel voor de aanvangsdatum en doorloopplanning van een preventieve onderhoudsronde van de camera's. Eerst na schriftelijk akkoord van de Opdrachtgever kan een preventieve onderhoudsronde plaatsvinden.
- 3.8.15 Een monteur van Opdrachtnemer meldt zich bij aankomst op locatie aan en bij vertrek af bij de beheerder van of namens Opdrachtgever.
- 3.8.16 Alle monteurs van Opdrachtnemer die werkzaamheden buiten op straat uitvoeren aan het systeem zijn minimaal VCA gecertificeerd.
- 3.8.17 Een monteur van Opdrachtnemer dient te allen tijde een opdracht bon in te vullen, waarop minimaal is aangegeven de aankomst- en vertrektijd, de naam van de monteur, constatering met betrekking tot de storing, de uitgevoerde testen en werkzaamheden en de verbruikte materialen en/of onderdelen voor werkzaamheden die niet vanaf achter het bureau uitgevoerd kunnen worden.
- 3.8.18 Bij facturering van werkzaamheden met betrekking tot storingen die niet binnen de reikwijdte van het onderhoudscontract vallen, dient Opdrachtnemer de kopie opdrachtbon met de factuur mee te zenden.
- 3.8.19 De ANPR-camera's dienen minimaal 99,5% van de tijd functioneel werkzaam te zijn, voor het Managementsysteem is deze eis minimaal 99% van de tijd. De werkelijk gerealiseerde beschikbaarheid wordt maandelijks bepaald.
- 3.8.20 De Opdrachtnemer dient over een duidelijk plan / beleid te beschikken voor wat betreft het vervangen van defecte hardware (m.b.t. spares, voorraadbeheer en on-site support).
- 3.8.21 Clouddiensten/applicaties dienen gemonitored te worden met een statuspagina of healthcheck (endpoint monitoring)

3.9 Eisen privacy en informatiebeveiliging

- 3.9.1 Opdrachtnemer dient ISO27001, dan wel aantoonbaar gelijkwaardig, gecertificeerd te zijn. Dit geldt tevens voor eventuele onderaannemers van Opdrachtnemer.
- 3.9.2 Het volledige ANPR-Camerasysteem inclusief bijbehorende koppelingen dienen te voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

- 3.9.3 Opdrachtnemer dient actief bij te dragen aan het doorlopen van het gemeentelijke DPIA-proces en daaruit voortvloeiende noodzakelijke aanpassingen aan de software en/of koppelingen door te voeren.
- 3.9.4 Het volledige ANPR-Camerasysteem inclusief bijbehorende koppelingen dienen te zijn ontwikkeld conform de principes van Security- en Privacy-by-Design alsmede Security- en Privacy-by-Default.
- 3.9.5 Het volledige ANPR-Camerasysteem dient de functionele en technische mogelijkheden te hebben, zodat de Opdrachtgever kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO).
- 3.9.6 Opdrachtnemer dient te beschikken over een interne procedure met betrekking tot 'Responsible Disclosure'. Onder Responsible Disclosure wordt verstaan dat wanneer een persoon die beroepsmatig of bij toeval een kwetsbaarheid tegen komt in een applicatie en dit meldt bij Opdrachtnemer, deze de kwetsbaarheid adequaat oplost voordat deze bekend wordt.
- 3.9.7 Metadata of gegevens ten behoeve van authenticatie (iets wat je hebt, bent of weet of mogelijk metadata tbv tijd en plaats) dienen uitgewisseld te kunnen worden met informatiesystemen. Bijvoorbeeld Identity & Access Management (IDM) of Azure ten behoeve van Single-Sign-On (SSO).
- 3.9.8 De hosting van het ANPR-Camerasysteem dient plaats te vinden bij een provider die niet onder de US Patriot Act valt en op servers die zijn gevestigd binnen de Europese Economische Ruimte.Fwaar
- 3.9.9 Opdrachtnemer dient medewerking te verlenen aan audits en pentesten op verzoek van Opdrachtgever ('right to audit').
- 3.9.10 Voor zover (delen van) de applicatie als een clouddienst wordt aangeboden, dient hiervoor periodiek, minimaal 1 keer per jaar, een Grey box pentest, uit te voeren door een onafhankelijke gecertificeerde partij, te worden doorlopen. De resultaten van deze pentest, de opvolging van de testresultaten en de oplossing, inclusief oplossingstermijn, van 'high risk' bevindingen dienen te worden gerapporteerd aan Opdrachtgever.
- 3.9.11 Alle dataverbindingen tussen onderdelen van het ANPR-Camerasysteem dienen beveiligd te zijn.
- 3.9.12 Opdrachtgever is eigenaar van alle data die met behulp van het ANPR-Camerasysteem wordt vergaard door gebruikers van Opdrachtgever. Opdrachtnemer mag deze data gebruiken voor zover dit noodzakelijk is voor de uitvoering van de dienstverlening.
- 3.9.13 Het kopiëren, muteren of verwijderen van data is niet toegestaan zonder expliciete schriftelijke toestemming van Opdrachtgever.
- 3.9.14 Voor zover (delen van) het ANPR-Camerasysteem toegankelijk dienen te zijn voor geautoriseerde medewerkers van Opdrachtgever, dienen deze gebruikt te kunnen worden met de laatste 3 versies van de browser Micorsoft Chromium Edge. Daarbij is het niet toegestaan dat lokaal plug-ins of andersoortige (installatie)bestanden opgeslagen dienen te worden.
- 3.9.15 Geautoriseerde medewerkers van Opdrachtgever of Opdrachtnemer dienen uitsluitend toegang te kunnen verkrijgen tot (delen van) het ANPR-Camerasysteem middels een persoonsgebonden login en 2-factor authenticatie.
- 3.9.16 Geautoriseerde medewerkers van Opdrachtgever dienen toegang te kunnen verkrijgen tot (delen van) de applicatie middels Single-Sign-On (SSO).
- 3.9.17 Session time-out instellingen (Idle, Absolute, Renewal) voor het webbased gedeelte van de Totale ICT prestatie zijn zo ingesteld dat de navolgende maximale tijden niet worden overschreden.

Time-out voor inactiviteit (Idle):

- Max 15 minuten voor toepassingen met hoog risico of na handmatig beëindigen van de sessie

Absolute time-out:

- Max 4 uur of na handmatig beëindigen van de sessie

Verlenging Time-out (Renewal):

- Maximaal iedere uur midden in de gebruikerssessie, en onafhankelijk van de sessieactiviteit en dus van de time-out voor inactiviteit, dient er automatisch een nieuw sessie ID te worden gegenereerd welke, met een veiligheidsinterval van max 10 minuten, automatisch overgang verzorgt van het oude naar het nieuwe sessie ID en hiermee het voorgaande sessie ID ongeldig maakt.

- 3.9.18 Software libraries mogen niet EOL(End-of-life) zijn. Update mag N-1 zijn.
- 3.9.19 Authenticatie loopt via (Seamless) Single Sign On. Hierbij worden de door Microsoft Azure Active Directory protocollen ondersteund en wordt als identity provider de Entra ID omgeving van de opdrachtgever gebruikt.
- 3.9.20 (Seamless) Single Sign on gebeurt op basis van least privilege. De Leverancier dient aan te tonen en te onderbouwen welke premissies, attributen en/of claims nodig zijn om de koppeling op te zetten. (SSO, SCIM en SP(N))
- 3.9.21 Bij gebruik van een subdomein of domein dat door de Opdrachtgever wordt beheerd dan gebruikt Leverancier alleen certificaten welke zijn verstrekt door de Opdrachtgever.
- 3.9.22 De Leverancier is verantwoordelijk voor de aankoop van certificaten. Tenzij het gaat om de door Opdrachtgever beheerde domeinnamen.
- 3.9.23 Alle protocollen die worden gebruikt in de ICT Prestatie staan in de verplichte of aanbevolen standaarden van Forum Standaardisatie en voldoen aan de vereiste versie of hoger.
- 3.9.24 De ICT Prestatie voldoet en blijft voldoen aan de meest actuele NCSC richtlijnen voor wat betreft de ICT-beveiligingsrichtlijnen voor webapplicaties, TLS, Mobile apps en HTTPS.
- 3.9.25 De SSL Cipher Suites volgorde is zo ingesteld dat deze als eerst gebruikt maakt van het sterkste Cipher en zo aflopend. Hierbij gebruikt de Leverancier enkel ciphers met de status goed en/of voldoende van het NCSC.
- 3.9.26 Encryptie & hashing algoritmes voldoen aan de FIPS standaard N-1 (meest recente definitieve versie of 1 versie lager).
- 3.9.27 Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als dit noodzakelijk is.
- 3.9.28 Onprem to SaaS, SaaS to Onprem en SaaS to SaaS koppelingen verlopen altijd via de door de Opdrachtgever aangeboden Enterprise Service Bus (ESB), API Gateway of SFTP oplossing. Tenzij het gaat om openbaar raad te plegen data, deze data mag rechtstreeks bij de aanbieder van de data worden geraadpleegd en/of opgehaald of als het gaat om koppelingen onderling tussen leveranciers welke vallen onder de wettelijke grondslag welke is gesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties of als data van de onprem omgeving van de Opdrachtgever via een priveverbinding gaat naar de Azure Tenant van de Opdrachtgever.
- 3.9.29 Enterprise Service Bus (ESB) verbindingen verlopen via een 2-way SSL handshake met een Signed Named SSL certificaat (geen self signed en/of wildcard certificaten)
- 3.9.30 Enterprise Service Bus (ESB), API Gateway of SFTP koppelingen dienen via een statisch IP adres te worden opgezet.
- 3.9.31 SFTP koppeling authenticatie is op basis van certificaten, dit mogen geen wildcard certificaten zijn. De SFTP server (indien van toepassing) aan de kant van leverancier ondersteunt IP Whitelisting.

- 3.9.32 Machine to machine (G1) certificaten voor de Enterprise Service Bus (ESB) of API koppeling, die worden gebruikt voor het uitwisselen van gegevens onderling tussen machines, die door de Leverancier worden aangeschaft en gebruikt, krijgen per koppeling een certificaat en dit mag geen wilcard certificaat zijn.
- 3.9.33 De ICT Prestatie voorziet in validatiecontroles in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken. Er zijn door Leverancier beheersmaatregelen geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
- 3.9.34 De ICT Prestatie moet voorzien zijn van strikte input- en output-validatiemechanismen. Voor de input houdt dit in dat alle ontvangen gegevens, of deze nu van gebruikers, andere systemen of bestanden afkomstig zijn, gecontroleerd en gevalideerd worden op veiligheid en correctheid voordat ze worden verwerkt. Dit is essentieel om beveiligingsrisico's zoals SQL-injectie, cross-site scripting en andere potentiële aanvallen te voorkomen. Wat betreft de output, moeten alle gegevens die naar externe bestemmingen worden verzonden, zorgvuldig worden gecontroleerd en gevalideerd om te waarborgen dat er geen gevoelige informatie wordt gelekt en dat de gegevens correct worden weergegeven. De implementatie en werking van deze validatiemechanismen dienen in lijn te zijn met de richtlijnen zoals beschreven in NORA online met betrekking tot input-/output-validatie.
- 3.9.35 De ICT Prestatie gaat om met diakrieten
- 3.9.36 De ICT Prestatie is benaderbaar zowel IPv4 als IPv6
- 3.9.37 Voor het installeren van extensies in de Edge Browser dient de Opdrachtnemer het ID en de URL van de Edge-browserextensie aan te leveren. Een extensie op een andere manier installeren wordt niet ondersteund door de Opdrachtgever.
- 3.9.38 De ICT Prestatie gebruikt minimaal de onderstaande Security Headers, conform best practices van het OWASP <https://owasp.org/www-project-secure-headers>.
- Strict-Transport-Security (HSTS)
 - Content-Security-Policy (CSP)
 - X-Content-Type-Options
 - Referrer-policy
 - X-Frame-Options
 - Permissions-Policy
- 3.9.39 Voor SaaS-applicaties en producten is de Opdrachtnemer verantwoordelijk voor de beveiliging en updates van de ICT-prestatie. Kwetsbaarheden worden conform de SLA-oplostijden opgelost. De Opdrachtnemer is vereist een WAF (Web Application Firewall) en antivirus te gebruiken. De ICT-prestatie moet worden ingericht volgens best practices, huidige technologische standaarden en het Zero Trust-principe. Daarnaast dient de Opdrachtnemer te voldoen aan de volgende eisen:
- Periodieke Beveiligingsaudits: De Opdrachtnemer moet periodieke beveiligingsaudits uitvoeren, inclusief penetratietesten, om de beveiligingsmaatregelen te evalueren en te verbeteren.
 - Encryptie: Alle gegevens, zowel in transit als in rust, moeten worden versleuteld met encryptiealgoritmes conform eis SECA08.
 - Toegangsbeheer: Er moet een robuust toegangsbeheerbeleid zijn, inclusief SSO (of multi-factor authenticatie (MFA)), voor alle beheerders en personen met toegang vanuit de leverancier.

- Data Back-up en Herstel: Back-ups van alle gegevens moeten worden uitgevoerd conform RTO en RPO. Er moet een gedetailleerd disaster recovery plan zijn om snelle herstelmaatregelen te garanderen in geval van gegevensverlies. RTO en RPO worden elders in de uitvraag gedefinieerd. De backup moet op een andere locatie zijn dan de locatie van het live systeem.
 - Monitoring en Logging: Continue monitoring en logging van alle activiteiten binnen de applicatie om verdachte activiteiten snel te detecteren en hierop te reageren conform eis LOG01/02.
 - Datacenter: Tier 2 of hoger
- 3.9.40 Indien er sprake is van gedeelde (beheers) verantwoordelijken tussen Opdrachtgever en Opdrachtnemer dient een RACI (Responsible, Accountable, Consulted, Informed) model opgenomen te worden in een DAP (Dossier Afspraken en Procedures). Eventueel verantwoordelijkheden/ afhankelijkheden met 3de partijen dienen ook opgenomen te worden
- 3.9.41 Opdrachtnemer heeft een releasestrategie voor het (versie)beheer van software, firmware en licenties. Daarin wordt duidelijk aangegeven welk proces wordt gevolgd bij het invoeren van updates en welke rapportages worden gedeeld over de versies die in gebruik en beheer zijn
- 3.9.42 Lifecycle management/EOL (End-Of-Life status) van hardware dient door de Opdrachtnemer gemonitord en gerapporteerd te worden
- 3.9.43 Changes dienen uitgevoerd te worden volgens een duidelijk IPC (Incident Management, Problem Management en Change Management of "Change Enablement/ITIL) proces
- 3.9.44 De Opdrachtnemer heeft een backupstrategie voor het terughalen en herstellen van data (inclusief jaarlijks backup restore tests). Daarin wordt duidelijk aangegeven welke RTO (Recovery Time Objective) en RPO (Recovery Point Objective) van toepassing is
- 3.9.45 Informatie m.b.t. logging en monitoring kan (periodiek) opgevraagd worden door de Opdrachtgever t.b.v. audit trails
- 3.9.46 Vulnerability scanning op software wordt (periodiek) uitgevoerd door de Opdrachtnemer.
- 3.9.47 Security incidenten en datalekken dienen gemeld te worden bij de Opdrachtgever binnen 48 uur. Security issues dienen opgelost te worden op basis van CVSS score:
- Kritiek – Oplossen binnen 1 dag
 - High – Oplossen binnen 1 week
 - Medium – Oplossen binnen 2 maanden
 - Low – Oplossen in overleg
- 3.9.48 In aanvulling op Staatsblad 2019, 457 (<https://zoek.officielebekendmakingen.nl/stb-2019-457.html>) stelt Opdrachtgever de Leverancier verplicht geen gebruik te maken van producten of diensten van een partij waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft een product of -dienst te misbruiken of uit te laten vallen, of nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld onder met deze intentie, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

3.10 Eisen netwerk

De navolgende eisen zijn uitsluitend van toepassing indien en voor zover het ANPR-Camerasysteem voor de communicatie gebruik maakt van het VRI-netwerk.

- 3.10.1 Network Client ondersteunt minimaal 1 gbit/sec auto-negotiate.
- 3.10.2 Network Client ondersteunt DHCP.

- 3.10.3 Netwerk Client ondersteunt DNS.
- 3.10.4 Netwerk Client ondersteunt DDNS obv DHCP optie 81. Bonjour en mdns worden niet ondersteund door de Opdrachtgever.
- 3.10.5 Netwerk client maakt geen gebruik van layer 2 flooding (geen broadcast, geen Link local multicast en geen Arp flooding) (default behaviour DNA SDA Fabric).
- 3.10.6 Netwerk client consumeert maximaal 30 watt POE.
- 3.10.7 Client ondersteunt 802.1x EAP-TLS.
- 3.10.8 LAN/Wireless clients 802.1x certificaten kunnen remote worden vervangen door de Opdrachtgever.
- 3.10.9 Netwerk architectuur van de ICT prestatie wordt gedocumenteerd t.b.v. zero trust.
- 3.10.10 De ICT Prestatie ondersteunt zowel IPv4 als IPv6.

3.11 Eisen functioneel beheer

- 3.11.1 De functioneel beheerders van de Opdrachtgever kunnen zelf een gebruiker toevoegen, wijzigen of beëindigen aan de ICT prestatie.
- 3.11.2 Standaard autorisatieprofielen worden door de functioneel beheerders van de Opdrachtgever zelf gedefinieerd. Deze profielen worden toegewezen aan individuele gebruikers op basis van hun rol (Role Based Access - RBAC)
- 3.11.3 Autorisaties worden toegekend op functionaliteit met toegang tot die modules die de gebruiker nodig heeft voor zijn of haar werkprocessen.
- 3.11.4 Autorisaties worden toegekend op inhoud (data). Niet alle gebruikers die dezelfde functionaliteit hebben zien dezelfde data.
- 3.11.5 De ICT prestatie heeft de mogelijkheid om verschillende beheerders / keyusers een verschillend niveau van rechten als beheerder toe te wijzen met behulp van RBAC.
- 3.11.6 De standaardrapportages over de ingerichte autorisatiematrix en de manier waarop gebruikers gekoppeld werden aan de autorisatiematrix, zijn beschikbaar vanuit de Programmatuur voor Functioneel beheer van de Opdrachtgever.
- 3.11.7 De gebruiker moet inloggen in de applicatie volgens de door de Opdrachtgever gestelde technische en security eisen.
- 3.11.8 De functioneel beheerder van de Opdrachtgever moet een secundair inlogkanaal hebben om te garanderen dat hij of zij altijd toegang heeft tot de ICT prestatie
- 3.11.9 De functioneel beheerder van de Opdrachtgever kan onjuiste acties van gebruikers herstellen, hiervoor is een beheershandleiding beschikbaar.
- 3.11.10 De functioneel beheerder van de Opdrachtgever kan wisselen naar wat een gebruiker in een andere rol kan en ziet ten behoeve van gerichte ondersteuning.
- 3.11.11 De functioneel beheerder van de Opdrachtgever heeft invloed op de inrichting van invoervelden binnen de ICT prestatie, waaronder het verplicht kunnen stellen van specifieke invoervelden.
- 3.11.12 De rapportages en selecties in de ICT prestatie dienen beschikbaar te zijn op het niveau van strategisch, tactisch en operationeel.
- 3.11.13 De selecties waarop rapportages in de ICT prestatie zijn gebaseerd, zijn door de Opdrachtgever aanpasbaar zonder tussenkomst van de Opdrachtnemer.
- 3.11.14 Door een gebruiker opgevraagde rapportages en selecties tonen alleen waartoe die gebruiker in de ICT prestatie geautoriseerd is.

- 3.11.15 Wanneer functioneel beheer of een gebruiker ten behoeve van een rapportage een selectie van gegevens maakt, wordt deze selectie geautoriseerd toegankelijk en gedeeld met anderen, conform RBAC / profiel van de gebruiker.
- 3.11.16 Gegevens uit de ICT prestatie zijn beschikbaar voor gebruik in het Datawarehouse / Datavault / BI-omgeving van de Opdrachtgever ten behoeve van management rapportages.
- 3.11.17 De ICT prestatie koppelt met het MIM / Azure systeem van de Opdrachtgever zodat gegevens van gebruikers / personeel op één centrale plaats beheerd worden.
- 3.11.18 Alle handelingen in de ICT prestatie (bv. toevoegen, raadplegen, bewerken, goedkeuren, verwijderen, kopiëren, exporteren) op informatieobjecten en hun kenmerken zijn vastgelegd in een audit trail. De opgenomen gegevens in de audit trail kunnen niet gewijzigd worden.
- 3.11.19 De logging opgenomen in de audit trail moet gefilterd kunnen worden.
- 3.11.20 In importkoppelingen wordt op Veld niveau aangegeven wat met de informatie gedaan moet worden in welke situatie: overschrijven - altijd of alleen indien leeg, toevoegen, wanneer een veld in bron of doel is gevuld met afwijkende gegevens.
- 3.11.21 De Opdrachtnemer biedt inzicht in de samenhang tussen de verschillende entiteiten voor functioneel beheer van de Opdrachtgever, door het beschikbaar stellen van het datamodel (ERD).
- 3.11.22 Gegevens uit de ICT prestatie moeten geëxporteerd kunnen worden naar gangbare bestandstypen, minimaal naar PDF, Excel en/of naar csv, ook voor 1 op n relaties ten behoeve van verwerking buiten de ICT prestatie.
- 3.11.23 De ICT prestatie registreert alle beheersactiviteiten. Er wordt minimaal bijgehouden wie wat wanneer gedaan heeft in de beheerdersrol.
- 3.11.24 De functioneel beheerders van de Opdrachtgever hebben de mogelijkheid om functionele parameters, stuurgegevens en meldingen aan te passen/onderhouden.
- 3.11.25 Implementeren van de ontwikkeling, test en acceptatie (OTA) omgeving naar productie wordt zonder overtypen uitgevoerd.
- 3.11.26 Aanpassingen in de inrichting / processen / workflows worden zonder consultancy en met hulp van de helpdesk van de Leverancier gedaan.
- 3.11.27 Invoerschermen kunnen door functioneel beheer van de Opdrachtgever worden aangepast op lay-out en aantal en soort velden.
- 3.11.28 Bij nieuwe releases van de ICT prestatie blijven bestaande data in de applicatie toegankelijk zonder verandering van inhoud en structuur en verlies van functionaliteit. Oorspronkelijke metadata blijven behouden.
- 3.11.29 Wanneer gebruik gemaakt wordt van certificaten is voor de Functioneel Beheerder van de Opdrachtgever inzichtelijk welke certificaten gebruikt worden, wat de looptijd is en wie verantwoordelijk is voor tijdige signalering en verlenging.