Den Haag

Bijlage 3

Programma van Eisen

Vervanging en onderhoud verkeerscamerasysteem

DSB 23.181.

Den Haag

Inhoudsopgave

1 Begripsbepalingen 4
1.1 Algemene begrippen 4
1.2 Technische begrippen 10
2 Omvang en scope van de Aanbesteding 12
3 Algemene eisen 14
3.1 Eisen aan de Opdracht 14
3.2 Eisen Hardware en Software 15
3.3 Updatebeleid en back-ups 16
3.4 Eisen m.b.t. informatiebeveiliging en privacy 18
3.5 Eisen aan personeel en organisatie 22
3.6 Exit-strategie 22
3.7 Medewerkers Opdrachtgever en opleiding 23
3.8 Reserve-onderdelen 24
4 Camera's 26
4.1 Algemene eisen 26
4.2 Beveiligingseisen 27
4.3 PTZ en privacy-masking 28
5 Het videomanagementsysteem (VMS) en bijbehorende Hardware 30
5.1 Algemene eisen 30
5.2 Openheid en integratie 31
5.3 Uitkijken en bediening 31
5.4 Rechten, logging en gezondheidsinformatie 32
5.5 Redundantie 33
5.6 Beveiligingseisen aan het VMS 34
5.7 De Servers 34
5.8 De Uitkijkstations 35
5.8.1 Algemene eisen 35
5.8.2 Uitkijkstations verkeersleiding 36
5.8.3 Uitkijkstation politie Den Haag 37
5.9 Werkstation voor beheertaken 37
6 Gebruik van de netwerkinfrastructuur 39
6.1 Algemene eisen 39
6.2 Lokale switch en firewall 39

6.3 Monitoringsysteem Opdrachtnemer (optioneel) 41

7 Implementatie, oplevering en Aanpassingen 43

7.1 Realisatiefase en levering Camera's 43

7.2 Oplevering 45

7.3 Aanpassingen 46

8 Beheer en Onderhoud Cameratoezichtsysteem 48

8.1 Algemeen 48

8.2 Beschikbaarheid en Functieherstelttijden 49

8.3 Kosten 50

8.4 Storingsmanagement 51

8.5 Preventief Onderhoud en Innovatief Onderhoud 52

8.6 Correctief Onderhoud 53

8.7 Rapportage 53

8.8 Garantie 54

8.9 Documentatie 55

1 Begripsbepalingen

In dit Programma van Eisen wordt een aantal begrippen gebruikt die hieronder worden gedefinieerd. Begrippen worden in dit document met een hoofdletter geschreven. Er wordt in de begrippenlijst onderscheid gemaakt in algemene begrippen en technische begrippen.

1.1 Algemene begrippen

Zie ook Bijlage 1 bij deze Aanbesteding.

Begrip	Omschrijving
Aanbesteding	Zoals in Bijlage 1 Aanbesteding: De procedure waarbij de Aanbesteder bekend maakt dat hij een Opdracht wil laten uitvoeren en Ondernemers vraagt hiervoor een Inschrijving in te dienen.
Aanpassing	Een Aanpassing betreft een verandering van het Cameratoezichtsysteem als gevolg van een uitbreiding, wijziging, verwijdering van één of meerdere onderdelen van het Cameratoezichtsysteem. Na doorvoering van de Aanpassing dient het Cameratoezichtsysteem weer conform de eisen zoals verwoord in het Programma van Eisen te functioneren.
Acceptatie	Zoals in definitie GIBIT: De formele goedkeuring van (onderdelen van) de ICT Prestatie, afzonderlijk en in samenhang met elkaar, door middel van een succesvol uitgevoerde (integrale) Acceptatieprocedure.
Acceptatieprocedure	Zoals in definitie GIBIT: De testprocedure waarmee kan worden aangetoond dat de ICT Prestatie geen Gebrek(en) bevat.
Achtergronddocumentatie	Bijlage 13 van deze Aanbesteding. In dit document worden bepaalde aspecten voor de Inschrijver verduidelijkt.
As-builtdocumentatie	Een verzameling digitale tekeningen en documenten die door Opdrachtnemer wordt opgeleverd na voltooiing van de Realisatiefase of een Aanpassing. De documenten weer-spiegelen de staat van het Cameratoezichtsysteem in alle onderdelen die vallen onder verantwoordelijkheid van de Opdrachtnemer. Met deze documentatie moet een eventuele nieuwe leverancier zich het Cameratoezichtsysteem eigen kunnen maken en het Onderhoud hiervan op kunnen nemen en uitvoeren.

Begrip	Omschrijving
BBN	Basis BeveiligingsNiveau. Een classificatie binnen de BIO die o.a. bepaalt welke beveiligingseisen en maatregelen nodig zijn.
Bedieningsconsole	Een apparaat voor communicatie met het VMS bestaande uit een joystick en klein toetsenbord voor het snel opschakelen van Camera's via hun nummer of aansturen van presets.
Beheer	Alle activiteiten van de Opdrachtnemer die nodig zijn om gedurende de Looptijd aan de eisen uit het Programma van Eisen te voldoen en die niet onder Onderhoud vallen.
Beheer- en onderhoudsfase	De fase die direct start na afronding van de Realisatiefase. De Beheer- en onderhoudsfase richt zich op het in standhouden van het Cameratoezichtsysteem zonder Gebreken en het uitvoeren van Aanpassingen.
Beschikbaarheid	Zoals in definitie GIBIT: De mate waarin de ICT Prestatie daadwerkelijk beschikbaar is voor Opdrachtgever en gebruikt kan worden.
BIO	Baseline Informatiebeveiliging Overheid. Zie ook https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid
Camera	Dit is een Netwerkcomponent die één of meer live Videostromen uitstuurt en het betreft hier een geheel incl. behuizing, beugels en lens.
Cameratoezichtsysteem	De onderdelen van het gehele camerasysteem die onder verantwoordelijkheid van de Opdrachtnemer vallen, d.w.z. geleverd door Opdrachtnemer en/of in Beheer en Onderhoud genomen door Opdrachtnemer.
Centrale Voorzieningen	Het deel van het videomanagementsysteem (VMS), en alle hierbij behorende Hardware (zoals servers) en software op locatie bij de Opdrachtgever of politie Den haag.
Correctief Onderhoud	Zoals in definitie GIBIT: het opsporen en herstellen door Opdrachtnemer van Gebreken die Opdrachtgever hem heeft gemeld of die Opdrachtnemer anderszins bekend zijn geworden.
DAP	Dossier Afspraken en Procedures. Een aanvullend document naast de SLA waarin de procedures over samenwerking en de serviceverlening staan beschreven.

Begrip	Omschrijving
FAT	Factory Acceptance Test. Een test waarbij op locatie van Opdrachtnemer wordt aangetoond dat de ICT Prestatie aan de eisen voldoet.
Functiehersteltijd	Zoals in definitie GIBIT: de periode gelegen tussen het moment waarop een Gebrek bij Opdrachtnemer wordt gemeld en het moment waarop dit is verholpen.
Functioneel Beheer	Een groep medewerkers van Opdrachtgever die specifiek betrokken zijn bij eerstelijnsbeheer en de goede werking van het Cameratoezichtsysteem zullen controleren.
Gebrek	Zoals in definitie GIBIT: Het niet of niet volledig voldoen van de ICT Prestatie aan het Overeengekomen gebruik.
Gebruiksrecht	Zoals in definitie GIBIT: het recht op grond waarvan Opdrachtgever bevoegd is tot het gebruik van de ICT Prestatie binnen de kaders als gesteld in de Overeenkomst.
GIBIT	De Gemeentelijke inkoopvoorwaarden bij IT, zoals vastgesteld door de VNG d.d. 26 oktober 2020.
Hardware	De door Opdrachtnemer op basis van deze Overeenkomst te leveren of in Onderhoud te nemen apparatuur, inclusief bijbehorende materialen en documentatie en met inbegrip van de meest recente versie van de systeemprogram-matuur.
ICT Prestatie	Zoals in definitie GIBIT: alle door Opdrachtnemer op grond van de Overeenkomst te leveren goederen, waaronder zaken, Gebruiksrechten en diensten.
Implementatie	Zoals in definitie GIBIT: het geheel van handelingen en activiteiten dat nodig is om alle onderdelen van de ICT Prestatie, afzonderlijk en in onderlinge samenhang, in gebruik te kunnen nemen in de organisatie van Opdrachtgever, zodanig dat alle gebruikers van Opdrachtgever ermee kunnen werken overeenkomstig het Overeengekomen gebruik. Tot de Implementatie behoort tevens de Conversie, het realiseren van de voor het Overeengekomen gebruik noodzakelijke Koppelingen en het uitvoeren van de Acceptatieprocedure.
Innovatief Onderhoud	Zoals in definitie GIBIT: het beschikbaar stellen door Opdrachtnemer aan Opdrachtgever van Upgrades van de ICT Prestatie.
Inschrijver	Zoals in Bijlage 1 Aanbesteding: Een Ondernemer die een Inschrijving heeft ingediend.

Begrip	Omschrijving
Inschrijving	Zoals in Bijlage 1 Aanbesteding Een aanbieding/offerte van een Inschrijver bij de onderhavige Aanbesteding.
ITIL	Information Technology Infrastructure Library, meestal afgekort tot ITIL, is ontwikkeld als een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie.
Koppelvlak	Een koppelvlak is een punt waar infrastructuren met elkaar worden verbonden volgens een bepaalde standaard die uitwisseling van gegevens verzorgt.
KPI	Key Performance Indicator. Meetbare prestaties m.b.t. Onderhoud waar de Opdrachtnemer gedurende de looptijd van de Overeenkomst aan dient te voldoen.
Kritische Update	Een Update van een fabrikant op één of meer van zijn producten die een urgent (veiligheids)risico in het gebruik moet oplossen of mitigeren. Een fabrikant benoemt een dergelijke Update specifiek als kritisch.
Leverancier	Zie Opdrachtnemer. Deze definitie wordt in de plaats gesteld van de definitie in GIBIT.
Monitoringsysteem Opdrachtnemer	Een (optioneel) geautomatiseerd systeem van de Opdrachtnemer dat de prestaties van het Cameratoezicht-systeem monitort, alarmen van Hardware kan ontvangen en zelf een alarm genereert indien de prestaties niet meer (dreigen) te voldoen aan de door Opdrachtgever gestelde eisen.
Netwerkcomponent	Elk elektrisch apparaat met een eigen IP-adres dat onderdeel is van het Cameratoezichtsysteem.
Offerteaanvraag	Een door Opdrachtgever opgestelde aanvraag waarin hij zijn specificaties verstrekt voor het verrichten van een aanvullende Opdracht in het kader van de Overeenkomst door de Opdrachtnemer voor een Aanpassing van het Cameratoezichtsysteem.
Onbeschikbaarheid	Er is sprake van Onbeschikbaarheid indien (een deel van) het Cameratoezichtsysteem een Gebrek heeft.
Onderhoud	Het geheel van Correctief Onderhoud, Preventief Onderhoud, Innovatief Onderhoud en gebruikers-ondersteuning, een en ander zoals nader uitgewerkt in het Programma van Eisen, de DAP en de SLA. Deze definitie wordt in de plaats gesteld van de definitie in GIBIT.

Begrip	Omschrijving
Onderhoudsaannemer	De partij die voor Opdrachtgever installatie- en onderhoudswerkzaamheden uitvoert in de openbare ruimte.
Opdracht	Zoals in Bijlage 1 Aanbesteding: Al hetgeen voorwerp vormt van de overheidsopdracht zoals omschreven in de Aanbestedingsdocumenten.
Opdrachtgever	Zoals in definitie GIBIT: partij ten behoeve waarvan de Overeenkomst wordt gesloten.
Opdrachtnemer	De partij waarmee Opdrachtgever een Overeenkomst gesloten heeft.
Overeenkomst	Zoals in definitie GIBIT: de afspraken tussen Opdrachtgever en Leverancier met betrekking tot de levering van de ICT Prestatie, waarvan de GIBIT 2020 onderdeel uitmaakt.
Patchmanagement	Het proces dat ervoor zorgt dat Software en/of Hardware (firmware) van Updates worden voorzien met als doel fouten te herstellen of de security te verbeteren.
Personeel	Zoals in definitie GIBIT: de door partijen bij de uitvoering van de Overeenkomst in te schakelen personeelsleden en/of hulppersonen.
Preventief Onderhoud	Zoals in definitie GIBIT: het treffen van maatregelen door Opdrachtnemer ter voorkoming van Gebreken en andere technische problemen en andere daarmee verband houdende vormen van dienstverlening, al dan niet door het ter beschikking stellen van Updates.
Programma van Eisen (PvE)	Dit document.
Realisatiefase	Direct na inwerkingtreding van de Overeenkomst gaat de Realisatiefase in waarin Opdrachtnemer diverse werkzaamheden en leveringen afrondt die in het Programma van Eisen nader worden beschreven.
Reiskosten	Dit betreffen alle kosten die gemaakt worden voor zakelijke reizen voor afspraken met Opdrachtgever. Reiskosten mogen niet apart in rekening worden gebracht, maar zijn opgenomen in het uurtarief.
SAT	Site Acceptance Test. Dit is een test, uitgevoerd bij en onder toezicht van de Opdrachtgever, om de functionaliteiten conform het Programma van Eisen aan de hand van een door Opdrachtgever goedgekeurd SAT-protocol te verifiëren.
Server	Een voorziening die wordt gebruikt om centrale functionaliteit van bijvoorbeeld het VMS te leveren.

Begrip	Omschrijving
SLA	Zoals in definitie GIBIT: de nadere overeenkomst met betrekking tot het Onderhoud, waaronder begrepen het soort Onderhoud dat wordt verleend en de daarop toepasselijke Service Levels.
Software	Alle software noodzakelijk om de werking van het Cameratoezichtsysteem conform het PvE te garanderen.
Storing	Het niet conform het Programma van Eisen functioneren van (een deel van) het Cameratoezichtsysteem door een externe oorzaak die niet verwijtbaar is aan de Opdrachtnemer.
Storingsmanagement-systeem	Een systeem dat wordt gebruikt voor registratie en communicatie tussen Opdrachtgever en Opdrachtnemer over geconstateerde Gebreken en Storingen en de status hiervan.
Uitkijkstation	Een werkstation dat onderdeel is van het Cameratoezichtsysteem en waarmee het (o.a.) mogelijk is live Videostromen te tonen.
Update(s)	Zoals in definitie GIBIT: Een opvolgende versie van de firmware of systeemsoftware waarin Gebreken zijn hersteld en/of de werking van het betreffende onderdeel anderszins is verbeterd.
Upgrade(s)	Een opvolgende versie van de ICT Prestatie met in overwegende mate nieuwe of gewijzigde functionaliteiten, al dan niet onder een andere naam uitgebracht
Verwerkersovereenkomst	Zoals in definitie GIBIT: de bij de Overeenkomst gevoegde verwerkersovereenkomst, althans bij gebreke daarvan de ten tijde van het sluiten van de Overeenkomst door de Vereniging Nederlandse Gemeenten (VNG) tot standaard verklaarde Standaard Verwerkersovereenkomst, zoals beheerd door de Beheergroep VWO van de VNG. Bijgevoegd bij deze Aanbesteding als Bijlage 11.
Videostroom	De digitale live stroom van videobeelden die door een Camera, naar het VMS en/of een Uitkijkstation wordt gestuurd.
VMS of Videomanagement-systeem	Het videomanagementsysteem waarop de Camera's aangesloten dienen te worden. Het betreft hierbij zowel de Hardware als de Software op locatie bij Opdrachtgever.

Begrip	Omschrijving
Workaround	Een tijdelijke alternatieve oplossing om om een Gebrek heen te werken waardoor wel (grotendeels) dezelfde functionaliteit bereikt wordt.

1.2 Technische begrippen

Begrip	Omschrijving
AES-xxx bits	Advanced Encryption Standard waarbij de xxx de gebruikte blokgrootte in bits weergeeft (128, 192 en 256 zijn mogelijke waarden).
EMC	Elektromagnetische compatibiliteit.
EMI	Elektromagnetische interferentie.
Fps	Frames per seconde, het aantal beelden dat per seconde in de Videostroom wordt getoond.
Full HD	Een resolutie van 1920x1080 pixels.
Kbps	Kilobit per seconde, zie ook Mbps.
Gbps	Gigabit per seconde, zie ook Mbps.
IKxx	Onderdeel van de Europese Norm EN62262 die de bescherming van apparatuur tegen mechanische impact specificeert.
IPxy	Ingress Protection conform de internationale norm IEC60529. Deze code geeft de bescherming van elektrische apparatuur tegen stof (x) en vocht (y) aan.
Mbps	Megabit per seconde, een maat voor de hoeveelheid informatie die per tijdseenheid wordt verzonden en/of ontvangen.
NTP	Network Time Protocol (RFC 1305).
ONVIF	Open Network Video Interface Forum. Standaard om beveiligingsproducten op IP-basis met elkaar samen te laten werken. Zie ook http://www.onvif.org.
PoE	Power over Ethernet. Indien niet expliciet gespecificeerd zijn zowel PoE (IEEE 802.3af) als PoE+ (IEEE 802.3at) toegestaan.
PTZ	Afkorting voor pan (draaien), tilt (kantelen) en zoom.
PTZ-besturing	Besturing van een Camera m.b.t. pan, tilt en zoom van de camera of de lens.
PTZ-Domecamera	Een bestuurbare Camera.
Router	Hardware incl. antenne en voeding voor datatransmissie over een 4G- of 5G-netwerk van een mobiele provider.

Begrip	Omschrijving
VPN	Virtual private Network. Een VPN is een manier om een local area network (LAN) over een verbinding zoals het internet, uit te bouwen met behoud van vertrouwelijkheid.
SNMP	Simple Network Management Protocol. Een protocol voor het management van de componenten in een IP-netwerk. Via SNMP-boodschappen kunnen apparaten elkaar of een netwerk-managementsysteem op de hoogte stellen van problemen en/of veranderingen.
WDR	Wide Dynamic Range. Beeldverbetering voor situaties met een hoog dynamisch bereik. De verbetering wordt verkregen door meerdere opnames bij verschillende belichtingstijden te combineren tot één beeld.

2 Omvang en scope van de Aanbesteding

Deze Aanbesteding betreft het vervangen, aanpassen en in Beheer en Onderhoud nemen van het nieuw te realiseren Cameratoezichtsysteem. Uitbreiding van het Cameratoezichtsysteem, zoals levering van nieuwe Camera's vallen ook onder deze Aanbesteding.

Na ingangsdatum van de Overkomst gaat direct de Realisatiefase in. Opdrachtnemer dient in deze periode het bestaande systeem door het nieuwe Cameratoezichtsysteem te vervangen en te documenteren waarbij installatiewerkzaamheden van de Camera's door de Onderhoudsaannemer zullen worden uitgevoerd.

Beschrijving Cameratoezichtsysteem

Het Cameratoezichtsysteem bestaat bij ingang van de Overeenkomst uit de volgende onderdelen, en vallen dus voor Beheer en Onderhoud en Aanpassingen onder verantwoordelijkheid van de Opdrachtnemer:

1. Alle permanente camera's in eigendom van Opdrachtgever die primair gebruikt worden voor verkeerstoezicht;
2. De Centrale Voorzieningen in ieder geval bestaande uit:
    a) twee Uitkijkstations die gebruikt worden voor het tonen van zowel Videostromen maar ook voor andere verkeerskundige applicaties. Deze laatste applicaties zijn buiten de scope van Opdrachtnemer;
    b) een reserve-Uitkijkstation;
    c) een Uitkijkstation bij de politie Den Haag om mee te kunnen kijken;
    d) een werkstation voor beheertaken;
    e) de Servers waarop het Videomanagementsysteem functioneert;
    f) Optioneel: een Monitoringsysteem;
3. Lokale switch in de serverruimte in de kelder en bijbehorende mediaconverters;
4. Extenders voor doorgifte van monitors en USB over inpandige glasvezelbekabeling;
5. Lokale patchbekabeling t.b.v. de Centrale Voorzieningen;

Out-of-scope

De volgende onderdelen vallen buiten de scope van deze Aanbesteding.

1. De videoschermen in de uitkijkruimte (zowel videowall als de schermen op de werkplek zelf);
2. Het industriële netwerk van Opdrachtgever incl. 5G-Routers;
3. De internet-verbinding;
4. Inpandige vaste netwerkbekabeling (m.u.v. patchbekabeling);
5. Eventuele data-extenders bij gebruik netwerkkabel langer dan 100 meter in de buitenruimte;
6. Andere camera's van Opdrachtgever die niet primair bedoeld zijn voor verkeerstoezicht;
7. Camera's primair bedoeld voor kentekenherkenning;
8. Inpandige glasvezelbekabeling;
9. Beheer en Onderhoud van de applicaties op het Uitkijkstation die niet te maken hebben met cameratoezicht;
10. Alle installatiewerkzaamheden in de openbare ruimte;
11. Alle onderhoudswerkzaamheden in de openbare ruimte.

Realisatiefase
Hieronder staat een overzicht van de activiteiten in de Realisatiefase. Deze wordt nader gedetailleerd in paragraaf 7.1.

1. Het leveren, configureren en installeren van Uitkijkstations voor zowel cameratoezicht als andere applicaties;
2. Het leveren, configureren en installeren van Servers voor het Videomanagementsysteem;
3. Het leveren, configureren en installeren van een Uitkijkstation voor cameratoezicht zodat de politie kan meekijken;
4. Het leveren, configureren en installeren van een werkstation voor beheer voor de Functioneel beheerders van Opdrachtgever;

5. Het leveren, configureren en installeren van een lokale switch;
6. Het in stand houden van het zicht op de bestaande camera's;
7. Het leveren en configureren van 155 Camera's incl. beugels en toebehoren;
8. Het leveren en configureren van reservematerialen;
9. Het leveren van Beheer en Onderhoud op de reeds opgeleverde Camera's tot ingang van de Beheer- en onderhoudsfase;
10. Afstemming met de Opdrachtgever voor het IP-plan van de Camera's en het VMS;
11. Afstemming met de Onderhoudsaannemer voor de vervangingswerkzaamheden van de Camera's;
12. Het leveren, configureren en installeren van een optioneel Monitoringsysteem;
13. Het opstellen van de As-builtdocumentatie;
14. Het opstellen van een SLA en DAP;
15. Het verzorgen van opleidingen.

Beheer- en onderhoudsfase

Na afronding van de Realisatiefase gaat de Beheer- en onderhoudsfase in voor de rest van de duur van de Overeenkomst. De Beheer- en onderhoudsfase bestaat uit het volgende:

1. Beheer en Onderhoud van het Cameratoezichtsysteem gedurende de looptijd van de Overeenkomst. Het betreft hier alleen Beheer en Onderhoud op afstand én lokaal op de betrokken kantoorlocaties van Opdrachtgever en politie;
2. Rapportage over het uitgevoerde Beheer en Onderhoud;
3. Alle Aanpassingen van het Cameratoezichtsysteem gedurende de looptijd van de Overeenkomst, inclusief Beheer en Onderhoud hierop;
4. Samenwerking met en ondersteuning van de Onderhoudsaannemer die op locatie in de openbare ruimte de werkzaamheden verricht;
5. Coördinatieplicht bij alle Storingen die raken aan het Cameratoezichtsysteem.

3 Algemene eisen

3.1 Eisen aan de Opdracht

eis -1	Alle communicatie tussen Opdrachtnemer en Opdrachtgever geschiedt in de Nederlandse taal.
eis -2	Opdrachtnemer dient zich bij vervulling van de Opdracht te allen tijde te houden aan de vigerende wet- en regelgeving. De Opdrachtnemer houdt zich tevens aan de vigerende veiligheids- en milieuvoorschriften.
eis -3	De Opdrachtnemer mag zonder uitdrukkelijk voorafgaande schriftelijke toestemming van Opdrachtgever in publicaties, reclame-uitingen of anderszins geen gebruik maken van de naam of het logo van Opdrachtgever.
eis -4	De Opdrachtnemer dient van alle overlegvormen met Opdrachtgever uiterlijk binnen vijf (5) werkdagen zorg te dragen voor de verslaglegging en deze in digitale vorm te delen met Opdrachtgever.
eis -5	Opdrachtnemer draagt zorg voor een volledig functionerend Cameratoezichtsysteem bestaande uit alle geleverde en of in Beheer en Onderhoud genomen componenten en door Opdrachtgever geleverde voorzieningen en integratie met eventuele andere systemen (intern of van derden). De gedurende de looptijd van de Overeenkomst geleverde producten dienen naadloos met de rest van het Cameratoezichtsysteem samen te werken.
eis -6	Alle Aanpassingen gedurende de looptijd van de Overeenkomst leiden ertoe dat er sprake is en blijft van een volledig werkend Cameratoezichtsysteem conform de eisen uit dit document.
eis -7	Opdrachtnemer voldoet aan alle toepasselijke en/of verplichte normen en richtlijnen voor installatie van datanetwerken, laagspanningsinstallaties en beveiligingsnetwerken waaronder (niet limitatief): 1. laagspanningsrichtlijn 2014/35/EU; 2. EMC – richtlijn 89/336/EEG; 3. NEN 5152 Elektrotechnische symbolen, inclusief de Aanvullingen; 4. NEN 1010, Veiligheidsbepalingen voor laagspanningsinstallaties; 5. NEN 3140, Bedrijfsvoering van elektrische installaties – laagspanning.
eis -8	Alle Hardware moet geleverd worden met een geldige CE-markering. Opdrachtnemer is gedurende de looptijd van de Overeenkomst verantwoordelijk om aan alle eisen van CE te voldoen voor alles wat door hem is geleverd en/of in Beheer en Onderhoud is genomen.
eis -9	De Opdrachtnemer werkt samen met alle gemeentelijke afdelingen én leveranciers van systemen die raken aan het Cameratoezichtsysteem. Enkele voorbeelden (niet limitatief) hiervan zijn: 1. de Onderhoudsaannemer die de installatie- en/of onderhoudswerkzaamheden uitvoert; 2. de leveranciers van producten die buiten de scope van de Aanbesteding vallen; 3. het netwerkbeheer van Opdrachtgever.
eis -10	Opdrachtnemer stelt gedurende de looptijd van de Overeenkomst een functionaris aan die als primair aanspreekpunt dient. Deze functionaris neemt jaarlijks deel aan het strategisch/tactisch overleg en elk kwartaal aan het operationeel overleg. In het strategisch/tactisch overleg wordt ingegaan op komende vervangingen en projecten, nieuwe ontwikkelingen bij de klant en/of in de

	markt en de KPI's gemeten over het gehele jaar. Het operationeel overleg concentreert zich op storingsmanagement en de KPI's van het betreffende kwartaal. Het operationeel overleg kan plaatsvinden via MS Teams. Het strategisch/tactisch overleg is op locatie Opdrachtgever.
eis -11	Het gedurende de duur van de Overeenkomst niet voldoen aan contractueel overeengekomen verplichtingen leidt tot een boete voor de Opdrachtnemer. De hoogte van deze boete is in de Overeenkomst opgenomen.
eis -12	Boetes worden bepaald aan de hand van de gestelde minimale beschikbaarheidsniveaus en Functieherstelttijden. Beschikbaarheidspercentages gelden op jaarbasis. Indien een onderdeel in de loop van het afgelopen jaar is opgeleverd dan wordt gerekend naar rato van de periode na oplevering.
eis -13	De totale boete wordt na afloop van een kalenderjaar vastgesteld en in rekening gebracht. Het totaal van alle boetebedragen is per kalenderjaar gemaximeerd op de omvang kosten Beheer en Onderhoud van het betreffende jaar. Opdrachtnemer dient zelf in de jaarrapportage aan te geven wat de boete is o.b.v. de niet behaalde prestatie-eisen. Opdrachtgever heeft het recht het volledige boetebedrag te verrekenen met facturen voor Beheer en Onderhoud.

3.2 Eisen Hardware en Software

eis -14	Alle te leveren Hardware dienen geschikt te zijn voor een 24 uurs operationeel bedrijf gedurende 7 dagen per week / 365 dagen per jaar met een minimale technische levensduur van 8 jaar volcontinu bedrijf indien niet elders in dit document expliciet anders vermeld.
eis -15	Producten en installatie van te leveren Hardware dienen te voldoen aan de geldende EMI- en EMC-normen waarbij de Hardware onderling geen verstoringen veroorzaken of verstoringen veroorzaken op andere apparatuur.
eis -16	Alle te leveren Hardware dienen bij het daarvoor bestemde gebruik geen gevaar op te leveren voor gezondheid of het milieu, zowel tijdens installatie en verwijdering, bij gebruik, als bij afvalverwerking.
eis -17	Bij alle te leveren Hardware wordt gebruikgemaakt van nieuwe kwaliteitscomponenten van lopende productie van een fabrikant met een eigen serviceorganisatie. Materialen en onderdelen zijn nog ten minste 5 jaar te leveren na moment van levering of middels reserveonderdelen of vervangende onderdelen in bedrijf te houden zonder afbreuk te doen aan de systeemeisen en vormgeving. Reserve-onderdelen dienen minimaal een gelijkwaardige kwaliteit te hebben vergeleken met het origineel.
eis -18	Opdrachtnemer levert voor alle onderdelen van de ICT Prestatie alle benodigde Hardware en Software (oplossingen) inclusief alle benodigde licenties teneinde Opdrachtgever in staat te stellen het Overeengekomen gebruik te kunnen verrichten. Opdrachtnemer voert eveneens alle noodzakelijke ondersteuning op de ICT Prestatie, waaronder tenminste wordt verstaan: Beheer en Onderhoud, Updates en Upgrades gedurende de looptijd van de Overeenkomst.

	Opdrachtnemer garandeert dat in de Inschrijving alle benodigde licenties en/of abonnementskosten zijn aangeboden (en daarmee opgenomen zijn in het prijzenblad) die gedurende de looptijd van de Overeenkomst nodig zijn om de gevraagde Hardware en Software en de functionaliteit ervan in stand te houden en Opdrachtgever volledig te vrijwaren van enige aanspraak van derden op de onvolledigheid hiervan. De licenties op alle geleverde Software gelden met ingang van de datum waarop de Software op de Hardware is geïnstalleerd.
eis -19	Alle licenties en/of abonnementen dienen op naam van Opdrachtgever te worden gesteld.
eis -20	Alle Netwerkcomponenten dienen na herstel van de spanningsuitval automatisch te herstarten en operationeel te zijn binnen 15 minuten na terugkomen elektriciteitsvoorziening. Voor Camera's wordt een kortere hersteltijd gevraagd (zie eis -100).
eis -21	**Inschrijver zal** bij zijn Inschrijving een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4) indienen met specificatie van merk en type en productdocumentatie (specsheet) van de volgende producten: 1. Camera; 2. het in te zetten Videomanagementsysteem; 3. de Servers, Uitkijkstations/werkstations incl. gebruikte componenten (ten minste moederbord en CPU, werkgeheugen, opslagmedium, grafische kaart).
eis -22	De te leveren Hardware (inclusief cameraconfiguraties) dient volledig conform de bijbehorende specificaties te functioneren indien aangesloten op een elektrische installatie met de volgende eigenschappen: 1. spanning 200 – 240 Volt; 2. frequentie 47 – 53 Hertz; 3. aardlekautomaat B5A/30mA; 4. spanningsonderbreking 20 msec. maximaal
eis -23	Alle Hardware wordt door Opdrachtnemer voorzien van een sticker met een uniek identificatienummer. Bij Camera's betreft het een weer- en UV-bestendige sticker die ook na jaren vast blijft zitten en goed leesbaar blijft. Het identificatienummer dient gebruikt te worden bij beheer van de reservevoorraad en de As-builtdocumentatie. Bij afwerking in een 19"-rack wordt de sticker op een plek geplakt die altijd eenvoudig afleesbaar is.

3.3 Updatebeleid en back-ups

eis -24	Updates van elk besturingssysteem en Updates van gerelateerde applicaties (bijv. Microsoft .Net) dienen maandelijks te worden doorgevoerd. Opmerking: hypervisors zoals bijv. VMware ESXi worden ook gezien als een besturingssysteem en valt daarmee ook onder deze eis indien een dergelijke productlijn wordt aangeboden.
eis -25	Het Cameratoezichtsysteem zal nooit afhankelijk zijn van Software die end-of-life is of niet meer ondersteund wordt door de fabrikant. Software die end-of-life is of niet ondersteund wordt, dient (in overleg met Opdrachtgever) voor de ondersteuning stopt verwijderd te worden en vervangen te worden door een nog ondersteunde variant met minimaal dezelfde functionaliteit. Zie ook eis -255.

eis -26	Indien Opdrachtgever door het uitblijven van Updates gedwongen wordt niet meer ondersteunde of onveilige Hardware of Software te handhaven dan is er sprake van Onbeschikbaarheid van het betrokken deel van Cameratoezichtsysteem en is de boeteclausule van toepassing.
eis -27	Het VMS dient ten minste één keer per jaar van de meest recente Upgrade te worden voorzien.
eis -28	Updates op het VMS en andere noodzakelijke applicaties dienen ten minste één keer per drie maanden te worden doorgevoerd.
eis -29	Ten minste elke zes maanden dienen de beschikbare Updates doorgevoerd te worden op alle in Beheer en Onderhoud zijnde Hardware (bijv. Camera's) die niet onder eis -24 valt.
eis -30	Indien een fabrikant Kritische Updates uitbrengt van één van de producten die onder het Beheer en Onderhoud van de Opdrachtnemer vallen, dan dienen deze binnen één week na beschikbaar komen te worden doorgevoerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen. Indien het doorvoeren van Kritische Updates kan leiden tot verstoringen in het Cameratoezicht-systeem dan treden Opdrachtnemer en Opdrachtgever zo spoedig mogelijk met elkaar in overleg om risico's en eventuele mitigerende maatregelen te bespreken.
eis -31	Het uitvoeren van Updates en Upgrades zijn onderdeel van de rapportage over het uitgevoerde Beheer en Onderhoud (zie ook paragraaf 8.7).
eis -32	Indien het doorvoeren van Updates of Upgrades leidt tot problemen in het Cameratoezichtsysteem of andere applicaties die werken op het Uitkijkstation dan dient Opdrachtnemer op verzoek van Opdrachtgever de Update of Upgrade ongedaan te maken binnen 24 uur.
eis -33	Opdrachtnemer is verantwoordelijk voor het back-upbeleid van het Cameratoezichtsysteem. Het doel hiervan is dat bij uitval van een onderdeel (bijv. een opslagmedium) na vervanging van het betrokken onderdeel de oorspronkelijke instellingen en configuratie weer snel hersteld kunnen worden. Na elke wijziging aan de configuratie van een Netwerkcomponent die onder Beheer en Onderhoud van de Opdrachtnemer valt dient een back-up van de instellingen uitgevoerd te worden zodat bij uitval van een Netwerkcomponent deze vervangen wordt door eenzelfde product zonder langdurige installatie en configuratie. Bij een grote wijziging zoals een systeem-Upgrade dient ook vooraf een back-up te worden gemaakt. Back-ups mogen niet worden bewaard op de Netwerkcomponent waar de back-up van gemaakt is. Bij Camera's zal in afstemming tussen Opdrachtnemer en Opdrachtgever de inhoud van de back-up worden bepaald. Hierbij wordt rekening gehouden met de technische mogelijkheid van de Camera.
eis -34	De bewaartermijn van logbestanden is minimaal 12 maanden ten behoeve van onderzoek na een informatiebeveiligingsincident.
eis -35	Back-ups worden enkel terug gezet met toestemming van Opdrachtgever volgens de herstel-procedure (conform richtlijnen ISO27001).

3.4 Eisen m.b.t. informatiebeveiliging en privacy

In deze Aanbesteding worden de richtlijnen van de Informatiebeveiligingsdienst voor gemeenten (IBD, https://www.ibdgemeenten.nl/) gehanteerd. In deze paragraaf worden relevante eisen omtrent deze richtlijnen gesteld.

eis -36	Gedurende de looptijd van de Overeenkomst dient de Opdrachtnemer zich te houden aan de geldende wet- en regelgeving op het gebied van privacy, de Algemene Verordening Gegevensbescherming (AVG). Ten aanzien van het beschermen van de privacy en/of het verwerken van persoonsgegevens worden nadere afspraken vastgelegd in een Verwerkersovereenkomst en de Overeenkomst.
eis -37	Het verwerken van alle data van Opdrachtgever dient plaats te vinden binnen de Europese economische ruimte.
eis -38	De ICT Prestatie dient te vallen onder het managementsysteem voor informatiebeveiliging waarover de Opdrachtnemer dient te beschikken.
eis -39	De ICT Prestatie dient te voldoen aan de volgende standaarden en controles: 1. Het systeem dient beveiligd te worden op basis van actuele standaarden zoals te herleiden uit de OWASP guidelines (owasp.org); 2. Ontwikkeling dient aantoonbaar volgens een secure software development framework plaats te vinden; 3. Een auditlog rond toegang en verwerking van persoonsgegevens dient voor de wettelijke maximale periode beschikbaar te blijven voor analyse in geval van een vermeend datalek.
eis -40	Gedurende de looptijd van de Overeenkomst dient de Opdrachtnemer te beschikken over een geldig ISO27001-certificaat (of gelijkwaardig) dat van toepassing is op alle verwerkingen die door Opdrachtnemer voor Opdrachtgever worden uitgevoerd. Het niet langer beschikken over een geldig ISO27001-certificaat (of gelijkwaardig) is reden tot onmiddellijke ontbinding van de Overeenkomst zonder recht op schadevergoeding voor Opdrachtnemer. Bij inzet van een eventuele onderaannemer door de Opdrachtnemer dient de Opdrachtnemer een onderaannemer te selecteren die minimaal en aantoonbaar voldoet aan dezelfde eisen – inclusief beveiligingseisen – waar de Opdrachtnemer aan dient te voldoen.
eis -41	Bij start Overeenkomst en daarna jaarlijks gedurende de looptijd van de Overeenkomst stelt de Opdrachtnemer voor zichzelf en eventuele onderaannemers die subverwerker zijn een Third Party Mededeling (TPM-verklaring) beschikbaar aan Opdrachtgever. De jaarlijkse TPM-verklaring moet tenminste inzicht geven in hoeverre in de ISO 27001 en BIO beschreven procedures worden toegepast, op basis van opzet, bestaan en werking.
eis -42	Opdrachtgever is en blijft te allen tijde eigenaar van alle data die door het te leveren Cameratoezichtsysteem wordt verzameld. De Opdrachtnemer mag deze data niet zelf gebruiken voor andere doeleinden dan bedoeld in deze Overeenkomst zonder uitdrukkelijke en schriftelijke toestemming van de Opdrachtgever.
eis -43	Opdrachtnemer beschikt over een actuele autorisatiematrix van al het Personeel dat rechten heeft om gegevens van het Cameratoezichtsysteem in te zien, te verwijderen of aan te passen. Op verzoek van Opdrachtgever wordt deze autorisatiematrix per direct beschikbaar gesteld.

eis -44	Gedurende de looptijd van de Overeenkomst dient de Opdrachtnemer, incl. de door hem geleverde producten, te voldoen aan de richtlijnen zoals gesteld in de BIO niveau BBN2. Eventuele afwijkingen zijn alleen toegestaan na schriftelijke instemming van Opdrachtgever. De volgende afwijkingen zijn bij voorbaat en bij uitzondering al toegestaan: 9.4.3.1 Hierbij wordt niet geëist dat een account door een Camera of het VMS wordt geblokkeerd na een aantal foutieve inlogpogingen; 9.4.3.3. Camera's hoeven geen eisen af te dwingen m.b.t. wachtwoordsterkte. Dit dient organisatorisch te worden opgelost; 9.4.3.4 Camera's en VMS hoeven geen maximale geldigheidsduur aan een initieel wachtwoord toe te kennen. Camera's hoeven niet af te dwingen dat een wachtwoord direct wordt gewijzigd bij eerste gebruik. Dit dient organisatorisch te worden opgelost; 9.4.3.5. Camera's hoeven niet een maximale geldigheidsduur van wachtwoorden af te dwingen. Dit dient organisatorisch te worden opgelost; 11.2.9.2 Een videowall of de werkplek van de verkeersleiding of politie mag niet worden voorzien van een screensaver na 15 minuten inactiviteit; 12.1.4.1 Het Cameratoezichtsysteem is niet voorzien van een test-omgeving; 12.4.1.1 Logregels in Camera's dienen herleidbaar te zijn tot een account en niet per se een natuurlijk persoon. Het is hiermee toegestaan dat Camera's zijn voorzien van een enkel bedrijfsaccount voor Opdrachtnemer. Indien de Camera wel in staat is tot één of meer van bovenstaande uitzonderingen dan komt de betreffende uitzondering te vervallen.
eis -45	Niet-essentiële softwareapplicaties, services, poorten e.d. moeten worden verwijderd of gedeactiveerd.
eis -46	Opdrachtnemer dient actief de kwetsbaarheden te volgen die gepubliceerd worden door zowel fabrikanten als organisaties die databases met bekende kwetsbaarheden beheren. Opdrachtnemer meldt kwetsbaarheden in alle onderdelen van de ICT Prestatie aan Opdrachtgever binnen een week nadat deze ontdekt zijn en adviseert over mitigerende maatregelen.
eis -47	Opdrachtnemer heeft Patchmanagement ingericht, zodat alle onderdelen van het Cameratoezichtsysteem worden voorzien van de meest recente Updates. Hiervoor is een aantoonbaar Patchmanagementproces van toepassing. Kritische Updates vallen onder eis -30.
eis -48	De Opdrachtnemer levert alleen Netwerkcomponenten die niet End-of-life of End-of-sales zijn verklaard en waarvan de fabrikant tot ten minste 5 jaar na End-of-life verklaring van het product garandeert dat er (firmware-)Updates worden uitgebracht bij constatering van beveiligingsrisico's. Indien binnen deze termijn de fabrikant niet binnen drie maanden na constatering van het beveiligingsrisico met een firmware-Update komt die het probleem volledig oplost dan is Opdrachtnemer verplicht de door hem geleverde Netwerkcomponenten die hierdoor geraakt worden te vervangen op eigen kosten voor minimaal gelijkwaardige producten die wel aan de gestelde eisen voldoen. Zie ook eis -299.

eis -49	Door de Opdrachtnemer te leveren of in te zetten producten mogen de netwerkveiligheid van het Cameratoezichtsysteem niet in gevaar brengen.
eis -50	De toegang tot alle Netwerkcomponenten verloopt via een systeem met accounts en wachtwoorden. Bij installatie dienen wachtwoorden te zijn ingesteld. Het is niet toegestaan om fabriekswachtwoorden te handhaven.
eis -51	Ten minste de volgende subeisen gelden m.b.t. wachtwoorden: 1. Er worden geen wachtwoorden gebruikt die voor meerdere klanten gelden. 2. Wachtwoorden zijn niet triviaal en ten minste 16 karakters lang en bestaan uit ten minste vier karaktersoorten (hoofdletters, kleine letters, cijfers, leestekens); 3. Wachtwoorden dienen willekeurig gegenereerd te zijn; 4. Voor administrator- en beheeraccounts geldt dat wachtwoorden anders zijn dan het wachtwoord van het gebruikersaccount; 5. Er worden geen wachtwoorden hergebruikt. Het is nadrukkelijk niet toegestaan dat meerdere Camera's hetzelfde wachtwoord gebruiken; 6. De geldigheidsduur van alle wachtwoorden is beperkt tot één jaar en Opdrachtnemer zal jaarlijks alle wachtwoorden herzien. Vervanging is onderdeel van de rapportage. Kosten hiervoor zijn onderdeel van het reguliere Beheer en Onderhoud; 7. Waar instellingen van Hardware en Software dit mogelijk maken worden eisen aan de wachtwoordsterkte en wachtwoordduur automatisch afgedwongen. 8. Wachtwoorden dienen in een specifiek en volgens industriestandaards versleuteld systeem, zoals een wachtwoordkluis, beheerd te worden.
eis -52	Opdrachtnemer heeft een adequaat beveiligingsbeleid voor gevoelige klantinformatie zoals As-builtdocumentatie, logging-bestanden en persoonsgegevens. De volgende subeisen gelden: 1. Alle gegevensdragers (memorysticks, laptops, etc.) met klantgevoelige informatie die buiten de vestiging van Opdrachtnemer komen, worden volledig versleuteld. Bij laptops en tablets wordt gebruikgemaakt van versleuteling van de volledige harde schijf (bijv. Microsoft Bitlocker, McAfee Drive Encryption, VeraCrypt); 2. De kantooromgeving van de Opdrachtnemer is adequaat beveiligd tegen digitale én fysieke inbraak; 3. Communicatie van gevoelige gegevens, via internet of externe dragers als memory-sticks of remote beheer, is altijd additioneel versleuteld met ten minste AES-256 bits of gelijkwaardig gebruikmakend van een sleutel die voldoet aan de eisen gesteld aan een administrator-account.
eis -53	Bij gebruik van cloud-diensten door Opdrachtnemer (bijv. voor opslag van projectinformatie, logging-bestanden of As-builtgegevens) geldt: 1. Er is een contract tussen Opdrachtnemer en de provider; 2. Opslag van alle gegevens dient contractueel vastgelegd binnen de EU plaats te vinden; 3. Toegang tot de dienst of gegevens is o.b.v. 2-factor authentication; 4. Het gebruik van deze dienst valt onder alle toepasselijke Europese regelgeving en wetgeving; 5. De opgeslagen gegevens betreffen geen persoonsgegevens; 6. De cloud-provider dient ISO27001 of gelijkwaardig gecertificeerd te zijn; 7. Het gebruik van deze dienst zal voldoen aan de eisen zoals gesteld in de Baseline Informatiebeveiliging Overheid (BIO, niveau BBN2).

eis -54	Uitwisseling van informatie over internet via een website dient altijd versleuteld te zijn via HTTPS (geen self-signed certificaat) gebruikmakend van TLS 1.2 of hoger. Opdrachtnemer dient protocollen en ciphers te gebruiken die minimaal “voldoende” zijn volgens de “ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.1” van het NCSC. Zie ook https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
eis -55	Opdrachtnemer verleent alle medewerking bij het uitvoeren van audits door derde partijen in het kader van privacy en beveiliging. De Opdrachtgever heeft het recht door een derde partij een zgn. pen en hacktest uit laten voeren. Kritische Gebreken die hieruit voortkomen dienen binnen één week te zijn opgelost, anders is in het kader van het boeteregime sprake van Onbeschikbaarheid van de Centrale Voorzieningen. Kosten voor de hertest na geconstateerde Gebreken zijn voor Opdrachtnemer met uitzondering van de allereerste hertest gedurende looptijd Overeenkomst. Een hertest zal zich beperken tot de geconstateerde Gebreken. Kosten voor het verlenen van medewerking zijn o.b.v. nacalculatie. Kosten voor het oplossen van geconstateerde problemen zijn voor Opdrachtnemer indien de problemen voortkomen uit fouten of niet uitgevoerde werkzaamheden.
eis -56	De Opdrachtnemer werkt, op verzoek van Opdrachtgever, mee aan de uitvoering van een Data Protection Impact Assessment (DPIA). Kosten hiervoor zijn verrekenbaar op nacalculatie.
eis -57	Bij afvoer van (Hardware met) datadragers ziet Opdrachtnemer toe op gespecialiseerde commerciële vernietiging van alle datadragers (‘shredding’). Vernietiging van de datadragers wordt met een certificaat van vernietiging aangetoond aan Opdrachtgever.
eis -58	Detectie van (pogingen tot) oneigenlijk gebruik, toegang tot, oneigenlijk wijzigen van het Cameratoezichtsysteem incl. loggegevens, worden zo snel mogelijk, maar uiterlijk binnen 24 uur, gemeld als beveiligingsincident aan de contractbeheerder van Opdrachtgever.
eis -59	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. Opdrachtnemer dient alle relevante logging veilig te stellen op een separate opslag en over te dragen aan Opdrachtgever.
eis -60	Om eventuele kwetsbaarheden van een website in een zo vroeg mogelijk stadium te detecteren maakt de gemeente Den Haag naast een meldingsproces gebruik van een detectieportaal. Het detectieportaal hanteert een Digital Risk Protection platform en detecteert automatisch alle online kwetsbaarheden van bekende, ‘verborgen’, en valse online toegangspunten. Zij brengen het online aanvalsvlak in beeld en geven advies over mogelijke maatregelen. De gemeente Den Haag zal de Opdrachtnemer om instemming vragen om de website op te nemen in het detectieportaal waarna er bij het ontdekken van kwetsbaarheden bevindingen doorgegeven zullen worden en na een redelijke termijn opgelost moeten worden. **Inschrijver dient** in een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4) aan te geven of deze medewerking wil verlenen aan het opnemen van de website(s) in een detectieportaal.
eis -61	De gemeente Den Haag organiseert periodiek een Hackevent: Hâck the Hague. Tijdens dit event krijgt een groot aantal ethische hackers de mogelijkheid om de door de gemeente Den Haag gebruikte applicaties en systemen die bereikbaar zijn vanaf het internet te onderwerpen aan een test. De bevindingen worden gedeeld met de leveranciers die daarna de bevinding(en) kan

	oplossen. Medewerking van de Opdrachtnemer (beschikbaar stellen test- of productieomgeving en oplossen van de kwetsbaarheden tijdens het event) wordt zeer op prijs gesteld. Er zal geen vergoeding tegenover staan maar is te bezien als een meervoudige en goedkope pentest. Echter, de Opdrachtnemer heeft geen enkele zekerheid dat haar applicatie daadwerkelijk door ethisch hackers wordt geselecteerd voor grondige tests. Uiteraard zijn de deelnemende ethische hackers gebonden aan de voorwaarden van de gemeente Den Haag en haar leveranciers. Ook buiten dit evenement om stimuleert de gemeente Den Haag ethische hackers kwetsbaarheden te melden via het CVD proces. Deelname aan het hackevent is niet verplicht, Inschrijver dient wel aan te geven of er wel/geen medewerking zal worden verleend. **Inschrijver dient** in een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4) aan te geven of deze wil deelnemen aan het periodieke evenement Hâck the Hague en daarvoor de ICT Prestatie beschikbaar stelt voor penetratietesten tijdens het evenement en zorg zal dragen voor opvolging van gevonden kwetsbaarheden tijdens of (direct) na het evenement.

3.5 Eisen aan personeel en organisatie

eis -62	Opdrachtnemer garandeert dat het door hem Personeel die vaardigheden en eigenschappen bezit die nodig zijn voor de adequate uitvoering van de Overeenkomst.
eis -63	De bij de uitvoering van de Opdracht betrokken Personeel die direct contact hebben met medewerkers van Opdrachtgever dienen de Nederlandse taal te beheersen in woord en geschrift.
eis -64	Alle medewerkers van Opdrachtnemer of onderaannemers die (remote) toegang hebben tot het Cameratoezichtsysteem of werkzaamheden verrichten op gemeente- of politielocaties worden gescreend o.b.v. een Verklaring Omtrent Gedrag (VOG) met ten minste screeningsprofielen 11, 12, 13 en 41. Opdrachtnemer is verantwoordelijk voor tijdige vervanging van medewerkers waarvoor geen VOG wordt afgegeven. Opdrachtnemer is verantwoordelijk voor het tijdig (opnieuw) aanvragen van de VOG voor alle betrokken medewerkers. Een VOG mag maximaal drie jaar oud zijn. Medewerkers dienen bij het betreden van het pand een geldige VOG en geldig identiteitsbewijs te kunnen overleggen.
eis -65	Voor het verlopen van de termijn van drie jaar van de VOG dient deze door Opdrachtnemer opnieuw te worden aangevraagd, ten minste drie maanden voor einddatum.

3.6 Exit-strategie

Bij beëindiging van de Overeenkomst (zowel bij einde contractduur als bij tussentijdse beëindiging) treedt de exit-strategie in werking. De eisen in deze paragraaf zijn in aanvulling op de GIBIT.

eis -66	De Opdrachtnemer doet al het mogelijke om de verlangde exit mogelijk te maken, voor zover dit redelijkerwijs van de Opdrachtnemer verwacht mag worden.

eis -67	De Opdrachtnemer levert aan Opdrachtgever of een door haar gekozen nieuwe leverancier alle informatie die benodigd is (incl. wachtwoorden van het Cameratoezichtsysteem) voor het uitvoeren van de transitie en zal beschikbaar zijn voor het geven van toelichting op de informatie.
eis -68	De Opdrachtnemer verleent ook tijdens de transitie toegang tot de informatie, data en systemen die Opdrachtgever nodig heeft.
eis -69	De Opdrachtnemer voldoet ook tijdens de transitieperiode aan de voorschriften op het gebied van geheimhouding en beveiliging.
eis -70	Gedurende de transitieperiode blijven alle relevante bepalingen van de Overeenkomst van kracht.
eis -71	Opdrachtnemer zal een exit-plan uitwerken en aan Opdrachtgever ter goedkeuring voorleggen. Het exit-plan wordt een aparte bijlage bij de Overeenkomst. Het goedgekeurde exit-plan dient gereed te zijn bij afronding van de Realisatiefase. Het exit-plan dient expliciet in te gaan op de verschillende soorten gegevens van Opdrachtgever.
eis -72	Voor afgaand aan de vernietiging van data wordt de vernietigingslijst opgesteld. Hierin wordt duidelijk omschreven welke gegevens wanneer zullen worden vernietigd. De lijst dient vooraf door Opdrachtgever te worden goedgekeurd.
eis -73	Na beëindiging van de Overeenkomst (zowel tussentijds als bij beëindiging na de maximale looptijd) dient de Opdrachtnemer binnen één maand alle persoonsgegevens en andere gevoelige gegevens zoals As-builtdocumentatie in haar bezit actief te vernietigen (zodat herstel onmogelijk is) en dit schriftelijk te bevestigen.
eis -74	De Opdrachtnemer zal een up-to-date versie van de As-builtdocumentatie, en een kopie van logbestanden en alle andere gegevens overdragen aan Opdrachtgever voor tot vernietiging van de gegevens over wordt gegaan. Hij dient in dit geval volledige medewerking te verlenen aan en ondersteuning te bieden bij het opstellen en het uitvoeren van een plan voor migratie van de gegevens.

3.7 Medewerkers Opdrachtgever en opleiding

eis -75	Voor een beperkte groep medewerkers van Opdrachtgever maakt Opdrachtnemer accounts aan (of zal deze in standhouden) met administrator-rechten op alle Hardware en Software. Het betreft hierbij als functioneel beheerder opgeleide medewerkers die de goede werking van het Cameratoezichtsysteem niet in gevaar brengen waardoor er Gebreken of Storingen kunnen ontstaan.
eis -76	Opdrachtnemer verzorgt twee opleidingen voor de uitkijkers van Opdrachtgever. Hierbij dient Opdrachtnemer uit te gaan van vier cursisten tegelijk. De volgende onderdelen dienen in deze opleiding aan bod te komen: 1. Het opschakelen en sturen van Camera's, zowel via scherm, toetsenbord/muis, als Bedieningsconsole; 2. Het instellen en gebruik van presets o.a. via de Bedieningsconsole; 3. Het aanpassen van de indeling en configuratie op de videowall; 4. Het gebruik van de kaart; 5. Het opschakelen van een Camera op een ander Uitkijkstation.

	Een beknopte digitale handleiding in het Nederlands is onderdeel van de opleiding. Na deze opleiding zijn de cursisten in staat effectief uit te kijken met het Cameratoezichtsysteem. Basis van de opleiding is dat cursisten zelf door alle relevante handelingen gaan. De duur van de opleiding is een dagdeel.
eis -77	Opdrachtnemer verzorgt twee opleidingen voor de functioneel beheerders van Opdrachtgever. Hierbij dient Opdrachtnemer uit te gaan van vier cursisten tegelijk. De opleiding gaat in op het gebruik van de aangeboden Camera's, VMS en Uitkijkstation. De volgende onderdelen dienen in deze opleiding aan bod te komen: 1. Basale uitkijkvaardigheden conform de opleiding uitkijkers. 2. Onderscheid kunnen maken tussen fouten van de gebruikers en werkelijke problemen. 3. Welke aanpassingen Functioneel beheerders wel kunnen doen en welke niet. 4. Eenvoudige beheertaken uit te voeren zoals het aanmaken accounts, aanpassen gebruiksrechten, basale foutdiagnose. 5. Toelichting op de rechtenstructuur; 6. Aanpassen en maken van schermindelingen, zowel qua lay-out als inhoud. 7. Veranderen relevante instellingen in de Camera (bijv. voorbereiden netwerkinstellingen voor plaatsing op straat, tijd tot automatische terugkeer naar home-preset in geval van PTZ, privacy-masking). Een beknopte digitale handleiding in het Nederlands is onderdeel van de opleiding. Na deze opleiding zijn de cursisten in staat functioneel beheer effectief uit te voeren. Basis van de opleiding is dat cursisten zelf door alle relevante handelingen gaan. De duur van de opleiding is één dag.
eis -78	Op verzoek van Opdrachtgever wordt deze opleiding herhaald, bijv. bij nieuwe functioneel beheerders van Opdrachtgever.
eis -79	De opleidingen dienen verzorgd te worden op locatie van Opdrachtgever.

3.8 Reserve-onderdelen

eis -80	Opdrachtnemer is er gedurende de looptijd van de Overeenkomst verantwoordelijk voor dat de reservevoorraad voldoende is uitgerust om aan alle contractuele verplichtingen te voldoen. Opdrachtnemer dient ervoor te zorgen dat de omvang van de reservevoorraad gelijk blijft en dus tijdig wordt aangevuld bij gebruik. Zie ook eis -261.
eis -81	Indien door veranderingen aan het Cameratoezichtsysteem, bijv. operationele inzet of de levering van een nieuw type product, het noodzakelijk is de reservevoorraad aan te passen dient Opdrachtnemer hiertoe tijdig een voorstel bij Opdrachtgever in. Minimaal elk halfjaar komt de Opdrachtnemer met een voorstel. Indien geen aanpassing nodig is dan wordt dit ook expliciet vermeld.
eis -82	Onderdeel van de Opdracht is levering van het volgende die op voorraad wordt gehouden bij Opdrachtgever:

	1. 10 Camera's; 2. 1 paar Video-extenders; 3. 1 USB-extender; 4. 1 Bedieningsconsole. Indien Opdrachtnemer meer reserve-onderdelen nodig heeft om aan de eisen gesteld aan het Beheer en Onderhoud te voldoen dan dienen deze onderdelen te worden opgevoerd in het prijzenblad.

4 Camera’s

Het betreft hier eisen aan door Opdrachtnemer te leveren Camera’s gedurende de looptijd van de Overeenkomst.

4.1 Algemene eisen

De eisen in deze paragraaf gelden voor alle te leveren Camera’s gedurende de looptijd van de Overeenkomst.

eis -83	De Camera moet geschikt zijn voor gebruik in alle Nederlandse buitenomstandigheden en de doelstelling om goed verkeerstoezicht mogelijk te maken in de openbare ruimte.
eis -84	De Camera wordt geleverd met behuizing in RAL-kleur 7032. De RAL-kleur is onderdeel van de prijs in het prijzenblad.
eis -85	Onderdeel van het bevestigingsmateriaal van een Camera en daarmee van de prijs in het prijzenblad zijn beugels in RAL-kleur, klembanden, bescherming tegen metaal-metaalcontact). Opdrachtgever zal per Camera specificeren of de beugels bedoeld zijn voor mastmontage of pendelmontage op een zweepmast. Bescherming tegen metaal-metaalcontact dient te gebeuren o.b.v. weer- en UV-bestendig materiaal, bijv. neopreen. Tape is niet toegestaan.
eis -86	Onderdeel van een Camera en daarmee de prijs in het prijzenblad is configuratie en toevoegen aan het VMS incl. eventuele eenmalige kosten van het VMS.
eis -87	De Camera dient gevoed te kunnen worden via zowel 230V als PoE. Bij voeding over 230V dient de transformator geplaatst te kunnen worden in de camerabehuizing of beugels. Eventuele aanvullende onderdelen dienen geleverd te worden in RAL-kleur en zijn daarmee onderdeel van de prijs in het prijzenblad.
eis -88	De Camera is geschikt voor een omgevingstemperatuur van -20 tot 50 graden Celsius.
eis -89	De Camera is digitaal en in staat om gelijktijdig minimaal twee vrij configureerbare streams uitsturen van zowel type H.264 als H.265, beide in ten minste Full-HD resolutie.
eis -90	Alle te leveren Camera’s hebben zowel een dag als een nachtstand. In de nachtstand wordt het IR-filter weg geklapt en is de Camera gevoelig voor infrarood-licht. Het lichtniveau waarbij dit gebeurt dient instelbaar te zijn en/of uitschakelbaar te zijn.
eis -91	De resolutie van een Camera is ten minste Full HD, d.w.z. 1920x1080 pixels.
eis -92	De Camera is minimaal genormeerd op IP66 en IK10.
eis -93	De Camera is uitgerust met automatische witbalans, auto-iris en autofocus.
eis -94	De Camera is voorzien van een username en password. Standaard- of fabriekswachtwoorden worden direct na installatie aangepast. Opdrachtgever krijgt per camera een eigen account met rechten tot aanpassing van instellingen zoals privacymasks.
eis -95	De Camera ondersteunt een beeldfrequentie van zowel 15, 25 als 30 fps.

eis -96	De (eventuele) koepel van de Camera veroorzaakt geen zichtbare vervorming/verstoring in het beeld.
eis -97	De Camera is specifiek geschikt voor omstandigheden met gelijktijdig zowel onderbelichting als overbelichting. Dit wordt bereikt via echte WDR, d.w.z. door het combineren van meerdere opnames met verschillende belichtingstijden, resulterend in een dynamisch bereik van ten minste 120 dB.
eis -98	De Camera ondersteunt HTTPS, TLS1.2 of hoger, NTP, SNMPv3, Syslog.
eis -99	De Camera incl. recente firmware-versies is gecertificeerd voor ONVIF Profile S en Profile T, te verifiëren op de ONVIF-website.
eis -100	Na spanningstuitval dient de Camera automatisch te herstarten met behoud van de gehele configuratie, logging en binnen twee minuten weer werkend te zijn.
eis -101	De Camera wordt via haar eigen interface / SDK (d.w.z. niet ONVIF) expliciet zonder voorbehoud of aanvullende voorwaarden ondersteund door ten minste vier verschillende VMS-fabricaten. **Inschrijver toont dit aan in** een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4).
eis -102	Indien de Camera in staat is tot opname of doorgifte van geluid dient dit expliciet en controleerbaar uitgeschakeld te kunnen worden.
eis -103	De Camera ondersteunt een resolutie van zowel Full-HD (1920x1080) als HD (1280x720).
eis -104	De Camera (in combinatie met het VMS) biedt voldoende mogelijkheden om de bitrate terug te brengen om zo, indien nodig, de databelasting te beperken.
eis -105	De Camera wordt expliciet en zonder voorbehoud of aanvullende voorwaarden ondersteund door het aangeboden VMS.

4.2 Beveiligingseisen

eis -106	Toegang tot de Camera vindt plaats via een veilig protocol (bijv. HTTPS, SFTP, SSH). De Camera vereist geen onveilige of onversleutelde protocollen (bijv. telnet of ftp) voor Beheer en Onderhoud. Onveilige protocollen als telnet en ftp dienen uitgeschakeld te worden (of te ontbreken).
eis -107	Opdrachtnemer zal aantoonbaar via een checklist de hardeningsrichtlijnen van de fabrikant volgen. Daar waar dit niet mogelijk of ongewenst is zal Opdrachtnemer in overleg treden met Opdrachtgever. Opdrachtgever zal hierin de definitieve keuze maken.
eis -108	De Camera ondersteunt het IEEE 802.1x toegangsprotocol o.b.v. EAP-TLS. Dit protocol wordt niet gebruikt bij ingang Overeenkomst, maar Opdrachtgever wenst de optie naar de toekomst open te houden.
eis -109	Elke Camera wordt zo opgeleverd dat de live Camerastream via de webserver niet zonder authenticatie kan worden bekeken.
eis -110	De Camera beschikt over een voorziening waardoor alleen door de fabrikant gewaarmerkte firmware op de Camera geïnstalleerd en uitgevoerd kan worden.

eis -111	De Camera is in staat tot het intern loggen van gebeurtenissen (conform BIO) gedurende 90 dagen. De volgende informatie zal gelogd worden: 1. De gebeurtenis. Het betreft hier ten minste configuratiewijzigingen en het inloggen op de Camera; 2. Accountnaam; 3. Het gebruikte apparaat; 4. Het resultaat van de handeling; 5. Een datum en tijdstip van de gebeurtenis incl. de gebruikte tijdzone. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. De gegenereerde logbestanden worden beschermd tegen onbevoegde toegang. Op basis van een expliciete risicoafweging wordt de bewaarperiode van de logging bepaald. Gegevens in de logging zijn persistent en verdwijnen niet na stroomuitval of reboot.
eis -112	De fabrikant van de Camera heeft aantoonbaar als standaard beleid voor al haar camera's dat ten minste 5 jaar na einde verkoop (end-of-life verklaring) van een bepaald type camera deze security Updates op de camera blijft uitgeven. Dit standaard beleid dient zonder inlog verifieerbaar te zijn via een algemeen vindbaar deel van de internationale website van de fabrikant. **Inschrijver toont dit aan** in een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4).
eis -113	De fabrikant van de Camera heeft aantoonbaar als standaard beleid voor al haar camera's die sinds 2018 zijn uitgebracht dat ten minste 5 jaar na einde levensduur (end-of-life verklaring) van een bepaald type camera de laatste firmware downloadbaar is via de website van de fabrikant. Hierbij is geen inlog vereist of is het triviaal mogelijk om een account hiervoor te verkrijgen, bijvoorbeeld door alleen een naam en e-mailadres op te geven. **Inschrijver toont dit aan** in een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4)
eis -114	De Camera biedt in combinatie met het aangeboden VMS de mogelijkheid tot end-to-end-encryptie. **Let op:** deze functionaliteit is geen onderdeel van de initiële uitvraag maar Opdrachtgever wenst deze optie naar de toekomst toe open te houden. Zie ook eis -162.

4.3 PTZ en privacy-masking

eis -115	Het zoombereik van de Camera is minimaal 20x.
eis -116	Installatie en oplevering van een Camera is incl. configuratie van privacy-maskering en presets. Het is niet mogelijk om zelfs maar oppervlakkig in woningen te kijken vanaf de 1e verdieping of hoger. Privacymasks dienen pas te verschijnen bij een zoomniveau net voordat privacy-schending mogelijk is. Het is ongewenst dat privacymasks continu zichtbaar zijn in een min of meer uitgezoomde staat indien niet strikt noodzakelijk.
eis -117	De Camera behoudt de positionering van de privacymasks en presets. Verloop van de positionering is ongewenst omdat dit tot het opnieuw instellen van privacy-zones en presets leidt. Indien in de praktijk Camera's het nulpunt verliezen waardoor privacymasks verplaatsen telt dit als een Gebrek en Onbeschikbaarheid van de Camera. De Opdrachtnemer dient vervolgens de privacymasks en presets in de oude staat te herstellen. De Onbeschikbaarheid van een Camera door verlopen van de privacymasks telt mee in de bepaling van een eventuele boete door Onbeschikbaarheid van Camera's.

eis -118	De Camera beschikt over ten minste 20 instelbare privacymasks die hun positie behouden bij PTZ-sturing. Privacymasking mag niet meer dan 0.1 sec. ‘na-ijlen’ bij door besturing veranderende camerabeelden.
eis -119	De kleur van de privacymasks is instelbaar. Ten minste grijs of een blur is mogelijk. De vorm is ten minste een vrij instelbaar (convex of concaaf) polygoon met ten minste vier hoeken. Alleen de rechthoek als polygonvorm is niet toegestaan.
eis -120	De minimale PTZ-dome eigenschappen van de Camera zijn: 1. Pan snelheid: Variabel 0.1 – minimaal 200 °/s; 2. Tilt snelheid: Variabel 0.1 – minimaal 100 °/s; 3. Pan bereik 360 graden continu; 4. Tilt bereik ten minste -90 tot +90 graden bij volledige zoom waarbij 0 graden verticaal naar beneden is gericht. Bij horizontaal kijken i.c.m. volledige zoom en montage op 4,5m hoogte mag de horizon niet hoger dan halverwege het beeld zijn; 5. Aantal presets is ten minste 30.

5 Het videomanagementsysteem (VMS) en bijbehorende Hardware

Zie ook Achtergronddocumentatie voor een nadere toelichting.

5.1 Algemene eisen

eis -121	Het VMS dient aan de eisen in dit PvE te voldoen zonder de noodzaak van maatwerk of klant-specifieke aanpassingen.
eis -122	Het VMS dient op locatie van Opdrachtgever gehost te worden.
eis -123	Bij oplevering van de Realisatiefase heeft het VMS (Software en Hardware) voldoende verwerkingscapaciteit om ten minste 200 Camera's te koppelen waarvan er tegelijk 30 getoond kunnen worden op de Uitkijkplek, 8 op het Uitkijkstation politie, 8 op de werkplek voor beheertaken en 12 via de webserver (zie ook eis -128). Bij volle belasting is er nog minimaal 30% overcapaciteit. Het gaat hierbij om Full-HD H.265 Videostromen tot mogelijk 6 Mbps. Eventuele cameralicenties mogen bij de Realisatiefase beperkt te zijn tot 155.
eis -124	Het VMS is eenvoudig schaalbaar tot ten minste 300 Camera's. Indien het aantal gelijktijdig uit te kijken Camera's niet toeneemt t.o.v. de uitgangssituatie dienen hiervoor alleen extra cameralicenties te worden aangeschaft en is geen uitbreiding van één of meer Servers nodig. **Opmerking:** Inschrijver mag ervan uitgaan dat de Videostromen van de Camera's niet worden opgenomen.
eis -125	Het VMS dient bij oplevering geen Videostromen op te slaan. Er dient alleen live uitgekeken te kunnen worden.
eis -126	Een Camera die nergens wordt uitgekeken en niet wordt opgeslagen dient geen significante datastroom te genereren. Een zgn. 'heart beat' van enkele tientallen Kbps tussen Camera en VMS is toegestaan. Verkeer ten behoeve van monitoring valt hier buiten.
eis -127	Het VMS dient alle Camera's op een vast instelbaar tijdstip in de nacht naar de home-preset te sturen. Deze functionaliteit dient eenvoudig per Camera aan- en uitgezet te kunnen worden.
eis -128	Het VMS wordt opgeleverd met een webserver waardoor het mogelijk is dat ten minste tien gebruikers die hiertoe gemachtigd zijn gelijktijdig live Videostromen kunnen bekijken en Camera's kunnen besturen via internet. De volgende aanvullende eisen zijn van toepassing: 1. De communicatie tussen client en de server is versleuteld via HTTPS met een geldig certificaat (zie ook eis -55); 2. Er is Multi Factor Authenticatie ingericht op de toegangsverlening o.b.v. de mobiele telefoon van de gebruiker; 3. Ondersteuning van gangbare moderne browsers (Chrome, Edge, Firefox). Alle gebruikers samen zullen niet meer dan twaalf Videostromen tegelijk opschakelen.
eis -129	De ontvangst van geluid komende met de Videostroom vanuit de Camera dient expliciet in het VMS uitgezet te kunnen worden.
eis -130	Het VMS ondersteunt ONVIF Profile S en T.

eis -131	Het VMS is geschikt om te werken in een gevirtualiseerde omgeving van een recente versie van zowel VMware als Microsoft Hyper-V. Opmerking: dit is een globale eis aan het VMS. Of in de praktijk wordt gekozen voor virtualisatie is aan Opdrachtnemer maar naar de toekomst die wil Opdrachtgever deze optie openhouden.
eis -132	Indien een Camera meerdere Videostromen beschikbaar stelt van verschillende resolutie dan dient het VMS de juiste Videostroom te kiezen op basis van de gekozen afbeeldingsgrootte op het scherm.
eis -133	Alle kosten voor Updates en Upgrades, abonnementskosten en alle verlenging van licenties zijn onderdeel van de jaarlijkse kosten voor Beheer en Onderhoud.

5.2 Openheid en integratie

Opdrachtgever wenst een aantoonbaar open VMS om te voorkomen ooit in een situatie van zgn. ‘vendor lock-in’ te komen.

eis -134	Het VMS ondersteunt op basis van algemeen verkrijgbare informatie van de fabrikant aantoonbaar een zeer breed aanbod van producten. Het ondersteunt de Videostromen van ten minste 100 verschillende merken IP-camera’s en ten minste 3000 verschillende cameratypes op basis van directe (native) integratie (d.w.z. niet o.b.v. ONVIF o.i.d.). **Inschrijver toont dit aan** in een bijlage (zie inschrijvingsleidraad, paragraaf 3.4.2.4)
eis -135	Het VMS biedt de mogelijkheid tot integratie van producten van derden via een SDK en is aantoonbaar in staat tot ten minste 20 verschillende fabrikanten die een dergelijke koppeling hebben gemaakt. Hierbij mag worden uitgegaan van informatie van de website van de fabrikant van het VMS of de fabrikanten zelf. **Inschrijver levert** in een bijlage een beschrijving van de SDK of SDK’s en een lijst van fabrikanten die reeds een integratie hebben gemaakt (zie inschrijvingsleidraad, paragraaf 3.4.2.4).

5.3 Uitkijken en bediening

eis -136	De uitkijkapplicatie van het VMS kan ten minste zowel op één als op alle schermen van het Uitkijkstation getoond worden.
eis -137	De uitkijkapplicatie van het VMS maakt het mogelijk om in hetzelfde window/scherm eenvoudig tussen verschillende taken te wisselen. Voorbeelden van taken zijn spotmonitor, kaart, of aanpassen indeling videowall.
eis -138	De selectie en bediening van de Camera’s is zowel mogelijk via een Qwerty-toetsenbord en een muis als Bedieningsconsole. De toetsenbord, muis en Bedieningsconsole is onderdeel van de levering.
eis -139	De Bedieningsconsole maakt het mogelijk om presets bij een Camera te selecteren.
eis -140	De uitkijkapplicatie van het VMS moet voorzien in de mogelijkheid om een kaart te tonen op basis van up-to-date Open Street Maps (max. 1 maand oud) waarin de locatie van alle Camera’s wordt getoond. Het moet eenvoudig mogelijk zijn op de kaart in of uit te zoomen en de kaart te verschuiven.

	Daarnaast dient live de kijkrichting en mate van zoom van elke Camera te worden getoond.
eis -141	Bij het aanklikken van een Camera op de kaart is het mogelijk deze eenvoudig op te schakelen.
eis -142	Het dient mogelijk te zijn om macro's (of vergelijkbaar) te definiëren om eenvoudig en snel groepen van camera's op te kunnen schakelen op een willekeurig Uitkijkstation. Opdrachtnemer is ervoor verantwoordelijk om de eerste benodigde salvo's en macro's te programmeren.
eis -143	Het dient mogelijk te zijn om met een enkele handeling een willekeurige Camera op te schakelen op een zelf gekozen plek op een ander willekeurig Uitkijkstation.
eis -144	Het dient mogelijk te zijn om met een enkele handeling een andere schermindeling te kiezen op een ander willekeurig Uitkijkstation.

5.4 Rechten, logging en gezondheidsinformatie

eis -145	Het VMS dient het gebruik van gebruikers- en groepsprofielen te ondersteunen. Het aantal aan te maken accounts is in principe onbeperkt. Het aantal accounts mag geen consequenties hebben voor licenties, kosten, etc.
eis -146	Per gebruikers- of groepsprofiel is het mogelijk om een prioriteitsniveau in te stellen die bepaalt wie prioriteit krijgt indien meerdere gebruikers dezelfde camera tegelijk besturen. Een gebruiker met hogere prioriteit moet te allen tijde de besturing van een gebruiker met lagere prioriteit over kunnen nemen.
eis -147	Uitsluitend een daarvoor expliciet geautoriseerde gebruiker of rol kan machtigingen van gebruikers of services aanmaken of wijzigen.
eis -148	Opdrachtnemer dient tijdens de realisatie van het Cameratoezichtsysteem de initiële gebruikers en bijbehorende gebruikersrechten af te stemmen met Opdrachtgever. Opdrachtnemer maakt deze gebruikers met de bijbehorende gebruiksrechten aan voor het eerste gebruik door Opdrachtgever. Opdrachtnemer draagt de bijbehorende authenticatiegegevens over aan Opdrachtgever.
eis -149	De rechten zijn per gebruiker of gebruikersgroep gedetailleerd in te stellen. Het betreft hierbij ten minste de volgende aspecten: 1. Per camera (groep) het recht om deze uit te kijken; 2. Per camera (groep) het recht om hiervan beelden terug te kijken; 3. Het recht om videomateriaal te exporteren; 4. Het recht om schermafdrukken op te slaan; 5. Het recht om gebruik te maken van de webserver (zie eis -128); 6. Het recht om gebruik te maken van een app op de telefoon om camera's uit te kijken; 7. Het recht om logging-gegevens op te vragen; 8. Het recht om instellingen aan te passen van Camera's; 9. Het recht om instellingen aan te passen van het systeem.
eis -150	Gedurende de looptijd van de Overeenkomst zal het VMS gebeurtenissen loggen conform de richtlijnen van de BIO. Het volgende wordt gelogd: 1. De gebeurtenis. Ten minste de volgende gebeurtenissen worden gelogd: a. Export beeldmateriaal (niet van toepassing bij oplevering maar dient in principe wel mogelijk te zijn);

	b. Terugkijken beeldmateriaal (niet van toepassing bij oplevering maar dient in principe wel mogelijk te zijn); c. Configuratiewijzigingen; d. Inlog/uitlog; e. Aanpassen wachtwoord; f. Aanpassingen aan rechten/rollen; g. Opschakelen Camera; h. Sturen van een Camera. 2. Het gebruikte apparaat; 3. Het betrokken account; 4. Informatie waar het resultaat van de handeling uit af kan worden geleid; 5. Een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. Loggegevens dienen gedurende 12 maanden bewaard te worden. De gegenereerde logbestanden zijn beschermd tegen onbevoegde toegang en dienen niet gewijzigd te kunnen worden.
eis -151	De loggegevens dienen veiliggesteld te kunnen worden in een gangbaar formaat als Comma Separated Values (csv) of Microsoft Excel.
eis -152	Het VMS detecteert en waarschuwt de Opdrachtnemer in geval van mogelijk falen bij het vastleggen van gelogde informatie.
eis -153	Het VMS genereert foutberichten met voldoende informatie voor de beheerder voor het verhelpen van storingen. Foutberichten mogen niet meer informatie bevatten dan strikt noodzakelijk voor het verhelpen van storingen om zo misbruik te voorkomen.
eis -154	Het VMS is voorzien van een voorziening die de gezondheidsstatus van het gehele Cameratoezichtsysteem monitort en via een dashboard een overzicht kan geven. Deze voorziening moet alarmen kunnen genereren en overzichten kunnen tonen wanneer (op de seconde nauwkeurig) en welk gezondheidsincident heeft voorgedaan. Het gaat hierbij ten minste om problemen in de verbinding met individuele Camera's (verlies van de verbinding, packet loss, vertraging), problemen in de server-omgeving.
eis -155	Het VMS is voorzien van een voorziening die laat zien dat Camera's verouderde firmware gebruiken of dat het VMS zelf verouderd is.
eis -156	Het VMS voorziet in een mechanisme dat bij geconstateerde gezondheidsproblemen er voorgeprogrammeerde acties kunnen worden uitgevoerd. Specifiek: indien een probleem optreedt met een Camera dan is het mogelijk een actie in te stellen waarbij de Camera automatisch wordt gereboot.

5.5 Redundantie

eis -157	Het VMS is bij oplevering zo ingericht dat bij uitval, tijdens het uitvoeren van Updates of Upgrades, of het niet functioneren van onderdelen van het VMS er een failover-mechanisme in werking treedt die de functie overneemt waarbij de eindgebruiker effectief geen verschil merkt t.o.v. de oorspronkelijke situatie.

	Dit dient te zijn ingericht voor elk onderdeel van het centrale VMS die noodzakelijk is voor het tonen van Videostromen op de Uitkijkclients en/of de webserver.
eis -158	Het failover-mechanisme dient binnen twee minuten na uitval de betreffende taak of taken overgenomen te hebben.

5.6 Beveiligingseisen aan het VMS

eis -159	Wachtwoorden van zowel gebruikers, Camera's en andere delen van het VMS zoals databases worden nooit onversleuteld opgeslagen of uitgewisseld.
eis -160	Wachtwoorden in de applicatie kunnen een instelbare en beperkte geldigheidsduur te hebben, waarna de gebruiker automatisch wordt gevraagd het wachtwoord te wijzigen. Tevens dient het mogelijk te zijn dat de gebruiker verplicht wordt het wachtwoord te wijzigen bij de eerste keer inloggen.
eis -161	Het VMS biedt een bescherming tegen brute-force aanvallen om wachtwoorden te achterhalen.
eis -162	Het VMS biedt in combinatie met de aangeboden Camera de mogelijkheid tot end-to-end-encryptie tussen Camera's en Servers en/of Uitkijkstations van alle uitgewisselde informatie incl. de Videostroom. **Let op:** deze functionaliteit is geen onderdeel van de initiële uitvraag maar Opdrachtgever wenst deze optie naar de toekomst toe open te houden. Zie ook eis -114.
eis -163	Het is mogelijk om voor gebruikerswachtwoorden eisen aan de wachtwoordsterkte af te dwingen, d.w.z. het minimum aantal karakters, en welke karaktersoorten gebruikt dienen te worden.
eis -164	Indien bij het inloggen in het VMS een ongeldige gebruikersnaam wordt ingevoerd geeft de applicatie eenzelfde reactie als bij een ongeldig wachtwoord met een geldige gebruikersnaam zodat het niet mogelijk is om zo te herleiden wat bestaande en niet bestaande gebruikersnamen zijn.
eis -165	Opdrachtnemer zal aantoonbaar via een checklist de hardeningsrichtlijnen van de fabrikant volgen. Daar waar dit niet mogelijk of ongewenst is zal Opdrachtnemer in overleg treden met Opdrachtgever. Opdrachtgever zal hierin de definitieve keuze maken.
eis -166	De broncode of configuratiebestanden van het VMS mogen geen gevoelige informatie hard-coded bevatten.

5.7 De Servers

eis -167	Elke Server en alle componenten zijn geschikt voor volcontinu gebruik en hoge prestaties. Dit betekent dat gekozen dient te worden voor professionele productlijnen.
eis -168	Elke Server betreft een 19"-rackmodel.
eis -169	Elke Server is uitgerust met een dubbele voeding zodat bij aansluiting op twee verschillende groepen, één stroomvoorziening of voeding uit kan vallen zonder enig effect op het functioneren. De status van de voedingen dient gemonitord te kunnen worden via het Monitoringsysteem.

eis -170	Elke Server is voorzien van de mogelijkheid om op afstand Beheer en Onderhoud uit te voeren, zelfs als bijvoorbeeld het besturingssysteem niet meer functioneert of het werkstation is gecrasht. Het gaat hierbij bijv. om Dell iDRAC, HP ILO, etc.
eis -171	Elke Server is voorzien van het meest recente 64-bits (Windows) besturingssysteem dat wordt ondersteund door het VMS en dat specifiek toegerust is voor server-toepassingen.
eis -172	Het besturingssysteem van elke Server dient geïnstalleerd te zijn op twee opslagmediums van type NVMe-drive van ten minste 500GB in RAID-1 (mirroring). Deze worden ook gebruikt voor de bijbehorende VMS-applicatie.
eis -173	Elke Server wordt voorzien van een professionele virusscanner die dagelijks wordt geüpdatet. Kosten incl. Updates zijn onderdeel van de kosten van Beheer en Onderhoud. Opmerking: aangetroffen virussen / malware zijn onderdeel van de rapportage over informatiebeveiligings-incidenten.
eis -174	De Servers zijn voorzien van 64GB intern RDIMM geheugen, verdeeld over ten minste twee modules.

5.8 De Uitkijkstations

Opdrachtnemer dient vier Uitkijkstations te leveren en in Beheer en Onderhoud te nemen. Twee Uitkijkstations voor de verkeersleiding, een reserve-Uitkijkstation, en een Uitkijkstation bij de Politie Den Haag. Zie ook de Achtergronddocumentatie voor een nadere toelichting. Eerst wordt ingegaan op de algemene eisen die gelden voor alle Uitkijkstations. Vervolgens worden voor de Uitkijkstations van resp. verkeersleiding en politie nadere eisen gesteld.

5.8.1 Algemene eisen

De eisen in deze paragraaf gelden voor alle vier de Uitkijkstations.

eis -175	Elk Uitkijkstation en alle componenten zijn geschikt voor volcontinu gebruik en hoge prestaties. Dit betekent dat gekozen dient te worden voor professionele productlijnen en niet voor consumentenproducten / gaming.
eis -176	Elk Uitkijkstation betreft een 19”-rackmodel.
eis -177	Opdrachtgever heeft admin-rechten op alle Uitkijkstations.
eis -178	Elk Uitkijkstation is uitgerust met een dubbele voeding zodat één stroomvoorziening of voeding uit kan vallen zonder enig effect op het functioneren. De status van de voedingen dient gemonitord te kunnen worden via het Monitoringsysteem.
eis -179	Elk Uitkijkstation is voorzien van de mogelijkheid om op afstand Beheer en Onderhoud uit te voeren, zelfs als bijvoorbeeld het besturingssysteem niet meer functioneert of het werkstation is gecrasht. Het gaat hierbij bijv. om Dell iDRAC, HP ILO, etc.
eis -180	Elk Uitkijkstation is voorzien van het meest recente 64-bits Windows besturingssysteem dat wordt ondersteund door het VMS.
eis -181	Elk Uitkijkstation is voorzien van de VMS-applicatie.

eis -182	Het besturingssysteem van elk Uitkijkstation dient geïnstalleerd te zijn op een opslagmedium van type NVMe-drive van ten minste 500GB. Deze wordt ook gebruikt voor de bijbehorende VMS-applicatie.
eis -183	De Uitkijkstations beschikken over ten minste 32GB intern DDR5 geheugen, verdeeld over ten minste twee geheugenmodules.
eis -184	Elk Uitkijkstation wordt voorzien van een professionele virusscanner die dagelijks wordt geüpdatet. Kosten incl. Updates zijn onderdeel van de kosten van Beheer en Onderhoud. Opmerking: aangetroffen virussen / malware zijn onderdeel van de rapportage over informatiebeveiligings-incidenten.

5.8.2 Uitkijkstations verkeersleiding

Conform de Achtergronddocumentatie dient de werkplek van de wegverkeersleiders te bestaan uit twee Uitkijkstations en één reserve-Uitkijkstation. Het eerste Uitkijkstation voor drie schermen op de videowall en het tweede Uitkijkstation voor de andere 7 tot 8 schermen. Waar in deze paragraaf Uitkijkstation wordt gebruikt zonder aan te geven of het het eerste, tweede of reserve Uitkijkstation betreft geldt deze eis voor alle drie de Uitkijkstations.

eis -185	Het eerste Uitkijkstation is in staat om vier 4K beeldschermen aan te sturen via HDMI 2.0 of DP1.4. Bij oplevering betreft dit de drie bovenste schermen van de videowall die uitsluitend worden gebruikt voor het tonen van Videostromen van Camera's.
eis -186	Het eerste Uitkijkstation is in staat om zonder haperingen 27 H.265 Full-HD beelden te tonen bij 6 Mbps, 25 fps per Videostroom.
eis -187	Het tweede Uitkijkstation is in staat om acht 4K beeldschermen aan te sturen via HDMI 2.0 of DP1.4. Tevens dient het Uitkijkstation te kunnen werken met ultra wide schermen (3440x1440 pixels). Bij oplevering betreft het de onderste drie schermen van de videowall en de vier dan wel vijf schermen op de desk zelf.
eis -188	Het tweede Uitkijkstation zal de VMS-applicatie tonen op één willekeurig te kiezen scherm van de desk. Alle andere schermen zijn beschikbaar voor andere applicaties en deze dienen geen hinder te ondervinden van de VMS-applicatie.
eis -189	De Uitkijkstations beschikken over een CPU met ten minste 16 cores en een Passmark score van ten minste 40.000. Zie ook https://www.cpubenchmark.net/
eis -190	De Uitkijkstations beschikken over ten minste 32GB intern DDR5 geheugen, verdeeld over ten minste twee geheugenmodules.
eis -191	De Uitkijkstations beschikken over hetzelfde type grafische kaart.
eis -192	Levering van het tweede Uitkijkstation is inclusief een Bedieningsconsole voor PTZ-besturing, en het selecteren van camera-presets. De Bedieningsconsole dient geschikt te zijn voor USB 1.1 of 2.0.
eis -193	Onderdeel van de levering is een reserve-Uitkijkstation dat bij storing in het eerste of tweede Uitkijkstation in zeer korte tijd op als eerste of als tweede Uitkijkstation ingezet kan worden met daarmee minimale uitval. Dit dient mogelijk te zijn zonder componenten toe te voegen.

	Het Uitkijkstation dient mee te lopen in alle van toepassing zijnde Updates en Upgrades en kan gebruikt worden voor test-, opleidings- of acceptatiedoeleinden.
eis -194	De communicatie tussen beeldschermen, keyboard, muis en Bedieningsconsole in de uitkijkruimte van de verkeersleiding en het Uitkijkstation dient door middel van zgn. extenders gerealiseerd te worden. Hiervoor gelden de volgende subeisen: 1. De Inschrijver biedt extenders geschikt voor singlemode-glasvezelbekabeling o.b.v. ST-connectoren; 2. Per monitorsignaal dient een aparte extender te worden gebruikt. De extender is in staat ten minste een HDMI of DisplayPort signaal zonder kwaliteitsverlies over ten minste 75 meter te transporteren over één of twee enkele vezels; 3. De extender ondersteunt zowel 4K (3840x2160 pixels) als ultra wide (3440x1440 pixels); 4. De extender dient zelf de Extended Display Identification Data te detecteren en de resolutie hieraan aan te passen; 5. Het USB-signaal (voor muis, toetsenbord én Bedieningsconsole) verloopt over een aparte extender. De extender biedt ten minste 4 USB-aansluitingen van type USB 2.0 of beter en is in staat het signaal over een afstand van 75 meter te transporteren over twee glasvezels.
eis -195	De extenders voor een monitorsignaal en een USB-signaal zijn geschikt om te functioneren in een omgevingstemperatuur van 0°C tot +40°C.
eis -196	Opdrachtnemer is verantwoordelijk voor levering en montage van alle lokale (patch)-bekabeling om monitors en USB te verbinden met de Uitkijkstations.
eis -197	De extenders dienen aan beide zijdes professioneel gemonteerd te worden, bijv. op legborden in het 19”-rack in de kelder-SER (zie ook de Achtergronddocumentatie). Het is niet toegestaan extenders op te hangen aan de eigen bekabeling.

5.8.3 Uitkijkstation politie Den Haag

eis -198	Het Uitkijkstation voor de politie is in staat om twee 4K-schermen aan te sturen via HDMI 2.0 of DP1.4.
eis -199	Het Uitkijkstation is in staat om zonder haperingen 8 H.265 Full-HD beelden te tonen bij 6 Mbps, 25 fps per Videostroom.
eis -200	Het Uitkijkstation beschikt over ten minste 16GB intern DDR5 geheugen.

5.9 Werkstation voor beheertaken

Voor beheerdoeleinden van het Functioneel beheer door Opdrachtgever dient een client geleverd te worden. Opdrachtgever is verantwoordelijk voor patching.

eis -201	Het werkstation is geschikt voor plaatsing in een kantooromgeving en betreft daarom geen 19”-rackmodel.
eis -202	Opdrachtgever heeft admin-rechten op het werkstation.
eis -203	Het werkstation is voorzien van het meest recente Windows besturingssysteem dat wordt ondersteund door het VMS.
eis -204	Het werkstation is voorzien van de VMS-applicatie (uitkijk én beheer).

eis -205	Het besturingssysteem van het werkstation dient geïnstalleerd te zijn op een opslagmedium van type NVMe-drive van ten minste 500GB. Deze wordt ook gebruikt voor de bijbehorende VMS-applicatie.
eis -206	Het werkstation wordt voorzien van een professionele virusscanner die dagelijks wordt geüpdatet. Kosten incl. Updates zijn onderdeel van de kosten van Beheer en Onderhoud. Opmerking: aangetroffen virussen / malware zijn onderdeel van de rapportage over informatiebeveiligings-incidenten.
eis -207	Het werkstation is in staat om twee 4K-schermen aan te sturen via HDMI 2.0 of DP1.4.
eis -208	Het werkstation is in staat om zonder haperingen 8 H.265 Full-HD beelden te tonen bij 6 Mbps, 25 fps per Videostroom.
eis -209	Het werkstation beschikt over ten minste 16GB intern DDR5 geheugen.
eis -210	Het werkstation wordt geleverd met mediaconverter voor koppeling op de lokale switch via het inpandige glas. Zie ook de Achtergronddocumentatie, paragraaf 7.1.

6 Gebruik van de netwerkinfrastructuur

6.1 Algemene eisen

eis -211	Opdrachtnemer maakt gebruik van de netwerkinfrastructuur van Opdrachtgever en werkt samen met het netwerkbeheer van Opdrachtgever en dient instructies hiervan op te volgen. Zie ook de Achtergronddocumentatie voor aanvullende informatie m.b.t. gebruik van de netwerkinfrastructuur.
eis -212	Opdrachtnemer krijgt van Opdrachtgever een IP-range en eventueel bijbehorende netwerkinstellingen toegewezen voor de in Beheer en Onderhoud te nemen en gedurende de looptijd van deze Overeenkomst te leveren voorzieningen.
eis -213	Opdrachtnemer heeft continue remote toegang tot het netwerk. Opdrachtnemer mag uitgaan van een functionele internetverbinding (100 Mbps symmetrisch en gegarandeerd) en een koppelpunt op het netwerk van Opdrachtgever. Ten minste 50 Mbps is continu beschikbaar voor Opdrachtnemer t.b.v. monitoring en/of beheer op afstand. Opdrachtgever behoudt echter het recht dat als de integriteit van het netwerk in gevaar komt door deze remote verbinding, per direct de verbinding af te (laten) breken en/of Opdrachtnemer remote toegang tot het netwerk te ontzeggen. Zie ook de Achtergronddocumentatie voor meer details over remote-toegang.
eis -214	De door Opdrachtgever beschikbaar gestelde remote-accessvoorziening kan niet gebruikt worden voor het structureel uitwisselen van applicatiedata, zoals monitoring. Hiertoe dient een separate VPN-tunnel te worden gebruikt. Kosten voor configuratie zijn onderdeel van de Inschrijving.
eis -215	Alle Netwerkcomponenten dienen hun systeemtijd te synchroniseren met de NTP-server van de Nationaal Dataportaal Wegverkeer (NDW) die beschikbaar is vanuit het netwerk van Opdrachtgever.
eis -216	Installatie van elk Netwerkcomponent geleverd door de Opdrachtnemer is incl. volledige configuratie van dit component, het toevoegen aan het VMS en/of optionele monitoring, het koppelen aan de NTP-server, en het instellen van accounts en wachtwoorden.

6.2 Lokale switch en firewall

De huidige switch in de serverruimte dient vervangen te worden en in Beheer en Onderhoud genomen te worden. Zie de Achtergronddocumentatie, paragraaf 7.1.

eis -217	De te leveren switch dient voldoende switchcapaciteit te hebben voor de beoogde inzet waarbij er ten minste nog 60% overcapaciteit (bandbreedte en CPU) is bij momenten van piekbelasting.
eis -218	De switch dient een managed laag 2 switch te zijn.
eis -219	Indien de switch en/of firewall geen rack-mounted model zijn dan is levering en montage incl. legbord.
eis -220	De switch dient voorzien te zijn van een dubbele voeding.

eis -221	De switch dient geleverd te worden incl. alle benodigde support en updates van de fabrikant. Kosten hiervoor zijn onderdeel van het Beheer en Onderhoud van de switch.
eis -222	De switch beschikt over ten minste: 1. 12x 10/1001000 Mbps RJ45 netwerkpoort; 2. 2x SFP-poort 1 Gbps; 3. Geschikt voor een omgevingstemperatuur van 40°C; 4. MTBF > 40 jaar.
eis -223	De switch ondersteunt SNMPv3.
eis -224	De switch is voorzien van een 1 Gbps transceiver voor koppeling van het werkstation voor functioneel beheer (paragraaf 5.9).
eis -225	Opdrachtnemer zorgt voor een adequate netwerksegmentatie. Hiervoor gelden de volgende aanvullende eisen: 1. Segmentatie vindt plaats op laag 2 van het OSI-model; 2. Hosts worden vooraf geclassificeerd, bijv. CIA-triad (Confidentiality, Integrity, Availability). Alleen hosts met dezelfde classificatie worden bij elkaar in een segment geplaatst; 3. Hosts die bereikbaar zijn via het internet worden in een DMZ geplaatst; 4. Uitkijkclients hebben een eigen netwerksegment; 5. Switches hebben een eigen netwerksegment; 6. Servers hebben een eigen netwerksegment; 7. Verschillende soorten verkeer worden van elkaar gescheiden, bijv. management-verkeer, VPN-verkeer t.b.v. remote Beheer en Onderhoud en Videostromen; 8. Camera’s mogen alleen communiceren met Servers en het werkstation voor beheertaken; 9. Voor elke wijziging in een netwerksegment dient er beoordeeld te worden of de wijziging aanvullende risico’s teweegbrengt en of er daardoor aanvullende maatregelen benodigd zijn. Indien aanvullende risico’s worden gevonden treedt Opdrachtnemer in overleg met Opdrachtgever.
eis -226	Onderdeel van de levering is een interne firewall die het netwerkverkeer filtert o.b.v. de volgende eisen: 1. Alleen protocollen die nodig zijn voor werking of beheer en onderhoud worden toegestaan. Al het andere verkeer wordt geblokkeerd; 2. Al het verkeer tussen LAN en WAN wordt gefilterd o.b.v. white-listing; 3. Clients en centrale servers hebben geen directe toegang tot internet, met uitzondering van: • Een voorziening voor het verkrijgen van actuele kaarten van Open Street Maps (zie eis -140);

	• Een voorziening voor het geven van waarschuwingen bij achterlopende firmware en software (zie eis -152); • Het tweede Uitkijkstation heeft diverse verkeerskundige applicaties die toegang tot internet vereisen; 4. Al het verkeer tussen de verschillende netwerksegmenten wordt gefilterd; 5. Filtering van dataverkeer is strikt, d.w.z. geen verkeer tenzij expliciet toegestaan. Filtering gebeurt o.b.v. source en destination adres/poortnummers en protocol; 6. Servers die met het internet of andere netwerken communiceren worden in een DMZ geplaatst; 7. Ondersteuning SNMPv3, d.w.z. monitoring van de firewall zelf; 8. De firewall heeft een filtercapaciteit van ten minste 1 Gbps.

6.3 Monitoringsysteem Opdrachtnemer (optioneel)

Opdrachtgever wil optioneel de mogelijkheid af te nemen tot monitoring van het Cameratoezichtsysteem. Deze optie dient separaat beprijsd te worden in het prijzenblad. Onderstaande eisen gelden enkel als deze optie daadwerkelijk wordt afgenomen.

eis -227	Het Monitoringsysteem dient te functioneren bij Opdrachtgever.
eis -228	Voor monitoringdoeleinden mogen alleen versleutelde protocolversies worden gebruikt. Het gebruik van SNMPv1 of SNMPv2c is daarmee niet toegestaan. Er dient minimaal SNMP-v3 gebruikt te worden of gelijkwaardig. Het is toegestaan om op een Uitkijkstation of Hardware met een eigen besturingssysteem specifieke monitoringsoftware (een ‘agent’) van het Monitoringsysteem te plaatsen mits deze de gegevens adequaat versleuteld ten minste gelijkwaardig aan SNMPv3.
eis -229	Het Monitoringsysteem dient ten minste elke vijf minuten elke Netwerkcomponent te controleren. Indien (potentiële) problemen worden geconstateerd wordt dit gemeld aan Opdrachtnemer. Deze dient hierop vervolgens adequaat actie te ondernemen.
eis -230	Het Monitoringsysteem zal alle problemen die Netwerkcomponenten zelf melden afvangen en aan Opdrachtnemer doorgeven. Deze dient hierop vervolgens adequaat actie te ondernemen.
eis -231	De volgende overige gebeurtenissen dienen ten minste door het Monitoringsysteem te worden waargenomen en gemeld: 1. Het wegvallen van de verbinding naar een Netwerkcomponent; 2. Storing of overschrijden van ingestelde grenswaardes in een Netwerkcomponent die via SNMP achterhaald kan worden; 3. Storing in de opslag (bijv. het uitvallen of foutmelding van één of meer harde schijven, het vollopen van het opslagmedium); 4. Continue hoge belasting van componenten zoals geheugen, CPU, grafische kaart; 5. Problemen met het besturingssysteem op de Netwerkcomponent;

	6. Voedingsproblemen.
eis -232	Elke Netwerkcomponent dient te worden opgenomen in het Monitoringsysteem incl. het instellen van drempelwaardes bij de via SNMP te ontvangen informatie. Kosten hiervoor zijn onderdeel van de installatieprijs en/of kosten voor Beheer en Onderhoud.

7 Implementatie, oplevering en Aanpassingen

7.1 Realisatiefase en levering Camera's

De eisen in deze paragraaf hebben betrekking op de werkzaamheden m.b.t. de vervanging van het Cameratoezichtsysteem in de Realisatiefase die direct aanvangt na de ingangsdatum van de Overeenkomst. De Realisatiefase beperkt zich tot de eerste 30 Camera's. De resterende 125 camera's en sparevoorraad worden vervangen in de Beheer- en onderhoudsfase die daarna in gaat.

eis -233	Gedurende de Realisatiefase zal er ten minste elke twee weken, of zo vaak als nodig, overleg plaatsvinden tussen Opdrachtgever en Opdrachtnemer op een locatie in Den Haag, of op aangeven van Opdrachtgever, via MS-Teams.
eis -234	Na ingangsdatum van de Overeenkomst stelt Opdrachtnemer binnen twee weken een Implementatieplan op inclusief planning. Pas na goedkeuring door Opdrachtgever vangen de werkzaamheden aan. Een Implementatieplan dient ten minste in te gaan op de volgende aspecten: 1. Scope, omvang en buiten scope; 2. Detail-planning incl. levertijden; 3. Gevolgen (en minimalisatie hiervan) voor de bedrijfsvoering van Opdrachtgever; 4. Aandachtspunten en relevante details van de installatie; 5. Het lokale netwerk; 6. Risico's en mitigerende maatregelen; 7. Verantwoordelijkheden Opdrachtnemer en Opdrachtgever; 8. Inzet derden / onderaannemers en taakomschrijving van deze partijen; 9. Koppeling van het VMS aan de bestaande Active Directory van Opdrachtgever; 10. FAT-protocol; 11. SAT-protocol.
eis -235	De werkzaamheden (zoals beschreven in eis -238) in de Realisatiefase dienen uiterlijk binnen 13 weken na ingangsdatum van de Overeenkomst gerealiseerd te zijn en worden afgesloten met een eindrapport van alle uitgevoerde werkzaamheden en bevindingen. De rest van de Realisatiefase bestaat uit: 1. Het leveren en configureren van Camera's; 2. Na installatie door de Onderhoudsaannemer, het direct toevoegen van de Camera's aan het VMS; 3. Bijwerken van de As-builtdocumentatie.
eis -236	Binnen 10 weken na ingangsdatum van de Overeenkomst dienen de eerste 30 Camera's geleverd en geconfigureerd te zijn. Vervolgens dienen de resterende Camera's incl. 10 reserve-exemplaren te worden geleverd met ten minste 20 per week.

eis -237	Bij installatie van een Camera door de Onderhoudsaannemer en controle van connectie via het netwerk, dient Opdrachtnemer ter plekke de Camera toe te voegen aan het VMS en de goede werking hiervan te verifiëren. Bij goede werking wordt dit doorgegeven aan de Onderhoudsaannemer en dient de rest van de configuratie te worden afgerond.
eis -238	Onderdeel van de Realisatiefase zijn de volgende activiteiten die hieronder (indien nodig) nader worden gedetailleerd. 1. Het uitvoeren van een FAT op eis-niveau; 2. Het leveren, configureren en installeren van de Uitkijkstations voor de wegverkeersleiders incl. extenders en patchbekabeling; 3. Het leveren, configureren en installeren van een werkstation voor de Functioneel beheerders van Opdrachtgever; 4. Het leveren, configureren en installeren van een lokale switch en firewall en optioneel Monitoringsysteem; 5. Het creëren van een overgangssituatie voor de periode dat nog niet alle oude camera's vervangen zijn. Zie ook de Achtergronddocumentatie; 6. Het leveren, configureren en installeren van een Uitkijkstation voor de politie (locatie hoofdbureau); 7. Het opleveren van het VMS; 8. Implementatie van de hardening-richtlijnen van de fabrikant (VMS en Camera's); 9. Het opstellen van de As-builtdocumentatie conform de eisen in paragraaf 8.9; 10. Het leveren, configureren en toevoegen aan het VMS van de Camera's; 11. Het leveren van de reserve-onderdelen conform eis -82; 12. Opleiding van de medewerkers Opdrachtgever; 13. Het doorlopen van het SAT-protocol; 14. Het opstellen van een SLA en DAP conform eis -254; 15. Het opstellen van een Exit-plan conform eis -71.
eis -239	Gedurende de gehele periode dat de bestaande camera's vervangen worden door nieuwe Camera's, dient de verkeersleiding zicht op de oude camera's te blijven houden. Zie ook de Achtergronddocumentatie, paragraaf 3.3.
eis -240	Voordat tot implementatie bij Opdrachtgever wordt overgegaan dient Opdrachtnemer een FAT uit te voeren conform een FAT-protocol. Hiervoor gelden de volgende subeisen: 1. Opdrachtnemer toont op eigen locatie aan dat de combinatie van de te leveren Hardware, Software aan een aantal eisen uit dit PvE voldoen. Het gaat hierbij om alle eisen die vooraf verifieerbaar zijn. De FAT betreft ten minste vijf aangesloten en werkende Camera's. 2. Opdrachtnemer voert eerst zelfstandig deze test uit (de pre-FAT) en stuurt, bij succesvolle FAT, een ondertekend FAT-rapport aan Opdrachtgever;

	3. Vervolgens wordt op korte termijn na deze pre-FAT de FAT herhaald onder toezicht van Opdrachtgever. Bij succesvolle herhaling geeft Opdrachtgever akkoord voor de daadwerkelijke implementatie op locatie Opdrachtgever.
eis -241	Bij oplevering van het VMS en koppeling hiermee van 30 Camera's zal voor dit deel de SAT conform SAT-protocol worden uitgevoerd. Bij oplevering van de resterende Camera's zullen deze in batches van 10 stuks conform het SAT-protocol worden afgenomen. In het SAT-protocol worden in principe alle eisen uit de FAT herhaald met uitzondering van eisen die naar mening van Opdrachtgever slechts één keer aangetoond hoeven te worden.
eis -242	Na toevoegen van een Camera aan het VMS wordt deze ook beheerd en onderhouden conform de eisen in dit PvE. De kosten hiervoor vallen onder de kosten voor de Realisatiefase.
eis -243	Na afronding van de Realisatiefase incl. levering van alle Camera's en Acceptatie door Opdrachtgever conform het Acceptatieprotocol start de Beheer- en onderhoudsfase.

7.2 Oplevering

eis -244	Opdrachtgever gaat tot Acceptatie over op het moment dat het Cameratoezichtsysteem of het opgeleverde deel hiervan) na de Acceptatieprocedure en oplossing van alle geconstateerde restpunten, 1 maand probleemloos heeft gefunctioneerd én de As-builtdocumentatie is geaccepteerd.
eis -245	Voor een succesvolle Acceptatieprocedure dienen de volgende onderdelen te zijn behaald: 1. Succesvolle FAT; 2. Akkoord Opdrachtgever op Implementatieplan; 3. Ontvangst geleverde Hardware incl. reserve-onderdelen; 4. Succesvolle SAT VMS en 30 Camera's; 5. Succesvolle SAT alle resterende Camera's; 6. Afronding opleiding medewerkers; 7. Akkoord Opdrachtgever op As-built; 8. Akkoord Opdrachtgever op SLA, DAP en Exit-plan.
eis -246	Bij elke projectoplevering, incl. oplevering van de Realisatiefase, dient Opdrachtnemer een door Opdrachtgever vooraf goed te keuren, SAT-protocol te leveren waarin de volgende punten minimaal doorlopen dienen te worden: 1. Controle configuratie (zie ook eis -248); 2. Functionele inspectie van correcte werking binnen het VMS met uitkijkers van gemeente Den Haag met aandacht voor de beeldkwaliteit en bediening van de Camera's; 3. Bijgewerkte As-builtdocumentatie en beschikbaarheid handleidingen.
eis -247	De SAT van het VMS incl. Hardware wordt uitgevoerd met specifieke aandacht voor de volgende punten: 1. Rechtenstructuur en accounts voor alle medewerkers Opdrachtgever; 2. Hardening-richtlijnen van de fabrikant zijn geïmplementeerd; 3. Logging is aangezet voor de relevante onderdelen en geëiste duur; 4. De Hardware wordt gemonitord door het Monitoringsysteem (optioneel);

	5. Belasting van het systeem met ten minste 46 Camera's die een Full-HD H.265 stream uitsturen.
eis -248	De SAT van een Camera wordt uitgevoerd met specifieke aandacht voor de volgende punten: 1. Juiste en meest recente firmware-versie; 2. Aanpassen van wachtwoorden conform het beleid in eis -51; 3. Aanmaken beheerdersaccount voor Opdrachtgever; 4. Instellingen van de parameters van de Videostroom; 5. Logging is aangezet voor inloggen, reboot, Updates en configuratiewijzigingen; 6. Camera is gekoppeld aan de NTP-server; 7. Hardening-richtlijnen van de Camerafabrikant zijn geïmplementeerd; 8. Privacymasking is ingesteld conform eis -116; 9. Camera wordt gemonitord door het Monitoringsysteem (optioneel); 10. Indien van toepassing het expliciet uitzetten van geluidsopname (zie ook eis -102 en eis -129).
eis -249	Elke projectoplevering wordt na afronding als geheel getest en geaccepteerd in combinatie met de rest van het Cameratoezichtsysteem. De acceptatie door Opdrachtgever vindt plaats na goedkeuring uitkomsten van de Acceptatieprocedure en oplossing van alle geconstateerde restpunten, twee weken probleemloos functioneren én oplevering As-builtdocumentatie. LET OP: zonder volledige en goedgekeurde Acceptatieprocedure inclusief As-builtdocumentatie wordt de oplevering niet geaccepteerd en vindt er geen betaling plaats.

7.3 Aanpassingen

eis -250	Aanpassingen aan het Cameratoezichtsysteem worden als offerte aangeboden en als project uitgevoerd (waar mogelijk) conform de posten en prijzen uit de Inschrijving.
eis -251	Voor elk project stelt Opdrachtnemer een projectmanager aan die als direct aanspreekpunt voor Opdrachtgever functioneert.
eis -252	Werkzaamheden voor uitbreiding, vervanging of nieuwe projecten worden marktconform aangeboden. De volgende subeisen zijn van toepassing: 1. De offerte wordt door de Opdrachtnemer volledig en open gespecificeerd. Het betreft hierbij ten minste merk en type van te leveren Hardware en detaillering en uitsplitsing van de uitvoering; 2. De offerte hanteert waar mogelijk de posten en prijzen zoals gespecificeerd in het prijzenblad van deze Aanbesteding; 3. Posten hoger dan € 1.000 moeten onderbouwd worden; 4. Opvolgers van in deze Aanbesteding aangeboden Hardware (die op dat moment wordt uitgefaseerd of niet meer wordt geleverd) en/of nieuwe technologie wordt aangeboden in dezelfde verhouding tussen aangeboden prijs en list price (door de fabrikant gesuggereerde prijs) als het geval is in de offerte voor de Aanbesteding met een vergelijkbare categorie van Hardware;

	5. Indien er voor bepaalde leveringen of diensten geen prijzen in het prijzenblad bekend zijn dient de Opdrachtnemer marktconforme tarieven in rekening te brengen. Indien Opdrachtgever van mening is dat de tarieven niet marktconform zijn, dan kan dit reden zijn om de offerte, of delen hiervan, elders onder te brengen, of onderdelen als directielevering aan Opdrachtnemer beschikbaar te stellen.
eis -253	Opdrachtnemer heeft de verplichting om een eenduidige en consistente technische infrastructuur van het Cameratoezichtsysteem in stand te houden.

8 Beheer en Onderhoud Cameratoezichtsysteem

Dit hoofdstuk beschrijft de eisen gesteld aan het Beheer en Onderhoud door Opdrachtnemer.

8.1 Algemeen

eis -254	Opdrachtnemer sluit een SLA en een DAP af met Opdrachtgever conform de aanbestedings-documenten, waaronder dit PVE, en deze naleven. Opdrachtnemer biedt deze documenten als concept en ter goedkeuring aan gedurende de Realisatiefase.
eis -255	De Opdrachtnemer is gedurende de gehele looptijd van de Overeenkomst verantwoordelijk voor het Beheer en Onderhoud voor alle onderdelen van het Cameratoezichtsysteem (de ICT-prestatie).
eis -256	Verbindingen derden en elektriciteitsvoorzieningen vallen buiten de verantwoordelijkheid van de Opdrachtnemer. Wel heeft de Opdrachtnemer hier een coördinatieplicht bij Storingen die impact hebben op het Cameratoezichtsysteem en waar nodig ondersteuning te verlenen bij het oplossen van de Storing dan wel te controleren of de Storing is opgelost.
eis -257	Het resultaat van Beheer en Onderhoud moet zijn dat er zo min mogelijk sprake is van Onbeschikbaarheid van het Cameratoezichtsysteem en dit beschikbaar is en blijft voor het uitkijken van Camera's.
eis -258	Opdrachtnemer beschikt over een eigen Nederlandstalige serviceorganisatie die is gebaseerd op ITIL-principes en die alle dagen van het jaar en 24 uur per dag in staat is om Gebreken op te lossen.
eis -259	Onderdeel van de dienstverlening is het melden van alle beveiligingsincidenten en (vermoedelijke) inbreuken op persoonsgegevens (zie ook de Verwerkersovereenkomst en eis -58). De Verwerkersovereenkomst detailleert de contactgegevens bij inbreuken op persoonsgegevens. In het DAP zullen de contactgegevens worden opgenomen voor het melden van beveiligings-incidenten.
eis -260	Bij een Gebrek aan een Camera die niet door Opdrachtgever op afstand opgelost kan worden zal een monteur van de Onderhoudsaannemer ter plekke een onderzoek uitvoeren. Indien voeding, verbinding en bekabeling correct werken zal worden overgegaan tot een vervangingsactie van de Camera voor een exemplaar uit de reservevoorraad. De Onderhoudsaannemer is hierbij verantwoordelijk voor: 1. Het voorzien van de Camera van de juiste netwerkinstellingen; 2. Het voorzien van de Camera van een default wachtwoord; 3. Het ophangen en aansluiten van de Camera conform de instructies van de fabrikant; 4. Het bij Opdrachtgever op locatie beschikbaar stellen van de defecte Camera zodat deze opgehaald kan worden voor reparatie door Opdrachtnemer. 5. Het aangeven welke Camera's zijn verwisseld t.b.v. beheer van de reservevoorraad door Opdrachtnemer. Opdrachtnemer is hierbij verantwoordelijk voor: 1. Afstemming met de verkeersleiding Opdrachtgever, dan wel Functioneel beheer;

	2. Afstemming met de monteur Onderhoudsaannemer op locatie om te controleren op bereikbaarheid van de nieuwe Camera; 3. Zorgen voor werkende oplevering Camera binnen het VMS; 4. Instellen van de privacymasks en presets in overleg met de wegverkeersleiders; 5. Indien binnen de garantie: het in ontvangst nemen van de defecte Camera en aanvullen van de reservevoorraad met eenzelfde model binnen één maand na ontvangst; 6. Indien buiten de garantie: het offreren van een nieuwe Camera.
eis -261	Opdrachtnemer mag wachten tot er 5 defecte Camera's zijn alvorens deze op te halen en om te wisselen.

8.2 Beschikbaarheid en Functieherstelttijden

eis -262	Het VMS dient een gegarandeerde Beschikbaarheid te hebben van 99,6% gedurende de werktijden van de wegverkeersleider.
eis -263	Het Uitkijkstation van de wegverkeersleiders dient een Beschikbaarheid te hebben van 99,6% gedurende de werktijden van de wegverkeersleider. Het Uitkijkstation van de politie dient een Beschikbaarheid te hebben van 99,0%. Het werkstation voor beheertaken dient een Beschikbaarheid te hebben van 99,0%.
eis -264	De lokale switch dient een Beschikbaarheid te hebben van 99,6% gedurende de werktijden van de wegverkeersleider.
eis -265	De Onbeschikbaarheid van het Cameratoezichtsysteem ten gevolge van niet verwijtbare stroomuitval of uitval verbindingen derden wordt niet meegerekend bij de bepaling van Onbeschikbaarheid die de Opdrachtnemer zijn toe te rekenen.
eis -266	Het moment van Onbeschikbaarheid gaat in bij de melding van een Storing door Opdrachtgever of uitkijkers van gemeente Den Haag of dat de Onbeschikbaarheid op andere wijze blijkt aan de Opdrachtnemer.
eis -267	De Functieherstelttijd en daarmee Onbeschikbaarheid eindigt op het moment dat de Opdrachtnemer het Gebrek heeft verholpen c.q. functieherstel heeft gerealiseerd en hiervan een schriftelijke melding is gedaan bij Opdrachtgever door de Opdrachtnemer.
eis -268	Indien een Gebrek niet correct is afgehandeld, gegeven een tweede vergelijkbare storingsmelding binnen twee kalenderdagen aan hetzelfde onderdeel van het Cameratoezichtsysteem, wordt de eerste melding als niet-afgehandeld beschouwd.
eis -269	De Onbeschikbaarheid van het Cameratoezichtsysteem ten gevolge van Storingen of schades door aanrijdingen, natuurgeweld, vandalisme, sabotage of ondeskundig handelen van Opdrachtgever worden niet meegerekend bij de bepaling van de Onbeschikbaarheid die de Opdrachtnemer is toe te rekenen. Opdrachtnemer dient duidelijk te maken waarom een dergelijke Onbeschikbaarheid hem niet is toe te rekenen. Tevens geldt voor Opdrachtnemer een inspanningsverplichting om te doen wat in zijn macht ligt om de Storing zo snel mogelijk op te lossen.
eis -270	Bij de eisen aan de Functieherstelttijden wordt onderscheid gemaakt tussen uren met prioriteit en uren zonder prioriteit. Uren met prioriteit betreffen de uren dat de verkeersleiders werken (zie

<table>
<tr><td></td><td>Achtergronddocumentatie). Indien een Gebrek niet is hersteld bij het einde van de dienst van de verkeersleiders dan loopt de Functiehersteltijd niet door en loopt weer verder bij start van de eerst volgende dienst van de wegverkeersleiding.

Bij de Functiehersteltijden wordt tevens onderscheid gemaakt tussen ernstige hinder en lichte hinder. In het geval van lichte hinder is het nog mogelijk dezelfde functionaliteit te bereiken met een Workaround. Het is aan de verkeersleider te bepalen of de aangeboden Workaround acceptabel is. Ernstige hinder is elk Gebrek dat geen lichte hinder is.</td></tr>
<tr><td>eis -271</td><td>De volgende eisen worden gesteld aan de Functiehersteltijden:

<table>
<tr><th>Onderdeel dat wordt geraakt</th><th>Ernstige hinder</th><th>Lichte hinder</th></tr>
<tr><td>VMS</td><td>4 uur</td><td>2 werkdagen van de verkeersleider</td></tr>
<tr><td>Uitkijkstation(s) verkeersleiding en lokale switch</td><td>4 uur</td><td>2 werkdagen van de verkeersleider</td></tr>
<tr><td>Uitkijkstation politie Den Haag en het werkstation voor beheertaken</td><td>1 werkdag van de verkeersleider</td><td>5 kalenderdagen</td></tr>
<tr><td>Enkele Camera</td><td>6 uur</td><td>1 werkdag van de verkeersleider</td></tr>
</table>
</td></tr>
</table>

8.3 Kosten

<table>
<tr><td>eis -272</td><td>Alle kosten voor Beheer en Onderhoud zijn onderdeel van het aangeboden Beheer en Onderhoud. Het betreft hierbij ten minste arbeid, voorrijkosten, transportkosten, materialen. Ook kosten voor vervanging van componenten binnen de garantietermijn zijn onderdeel van de kosten voor Beheer en Onderhoud.

Het volgende valt niet onder deze kosten:

1. Aanpassingen aan het Cameratoezichtsysteem m.b.t. het realiseren van nieuwe functionaliteit of het verwijderen van bestaande functionaliteit;
2. Aanschafkosten bij vervanging van componenten na afloop van de garantietermijn;
3. Correctief Onderhoud ten gevolge van Storingen of schade door aanrijdingen, natuurgeweld, vandalisme of sabotage en ondeskundig handelen van Opdrachtgever;
4. Aanvulling van de voorraad reservematerialen (tenzij van producten binnen de garantietermijn).</td></tr>
<tr><td>eis -273</td><td>Voorrijkosten wordt alleen in rekening gebracht voor uitvoerend technisch Personeel voor werkzaamheden buiten de SLA. Andere reiskosten dienen onderdeel te zijn van de jaarlijkse kosten voor Beheer en Onderhoud.</td></tr>
<tr><td>eis -274</td><td>Kosten voor het aanvullen en transporteren van de voorraad reservematerialen van onderdelen binnen de garantietermijn zijn onderdeel van het aangeboden Onderhoud.</td></tr>
</table>

8.4 Storingsmanagement

eis -275	Onder storingsmanagement wordt in het kader van deze Aanbesteding verstaan de taak om waar mogelijk Storingen of Gebreken te voorkomen of vroegtijdig op te sporen en bij optreden van een Storing of Gebrek deze in behandeling te nemen en binnen de Functieherstelttijden te verhelpen, dan wel coördinatie te voeren met derden om de Storing of Gebrek te laten verhelpen. Tot het takenpakket storingsmanagement behoren verschillende activiteiten. De Opdrachtnemer garandeert dat ten minste de volgende activiteiten behoren tot het storingsmanagement: 1. Het in behandeling nemen van Storingen of Gebreken, zowel telefonisch, e-mail als via een webapplicatie; 2. Afstemming met de beheerder van het VMS en/of afdeling ICT Den Haag; 3. Het leveren van eerste- en tweedelijns-ondersteuning bij vragen en Gebreken; 4. De registratie van de Storing of het Gebrek en alle statuswijzigingen hiervan in het Storingsmanagementsysteem; 5. De bevestiging van de Storing of het Gebrek (via e-mail), met vermelding van de datum en het tijdstip van de eerste melding en een uniek storingsnummer; 6. Melding aan relevante onderdelen van de organisatie van Opdrachtgever zoals netwerkbeheer en/of servicedesk; 7. Onmiddellijk informeren Opdrachtgever indien zich onvoorziene ontwikkelingen voordoen bij het verhelpen van de Storing of het Gebrek; 8. Het informeren Opdrachtgever tijdens en na het verhelpen van de Storing of het Gebrek; 9. Het tijdig uitvoeren van Preventief en Correctief Onderhoud; 10. De coördinatie met servicediensten (van derden zoals stroomvoorziening en datacommunicatie) en de voortgangsbewaking van de storingsafhandeling; 11. De storingsrapportage, waaronder Storingen van servicediensten van derden, met een formele herstelmelding van de servicedesk van de Opdrachtnemer aan de servicedesk van de Opdrachtgever (zie ook paragraaf 8.6); 12. Het leveren van correcte overzichtsrapportages zoals beschikbaarheidspercentages voor een bepaalde periode (zie ook paragraaf 8.7).
eis -276	Opdrachtnemer stelt aan Opdrachtgever een Storingsmanagementsysteem beschikbaar waarmee de Opdrachtgever in staat wordt gesteld Storingen of Gebreken te melden, de status van de storingsoplossing te volgen, en Storingen en Gebreken uit het verleden in te zien. Het Storingsmanagementsysteem is de plek waarin alle informatie over de Storingen of Gebreken wordt bijgehouden.
eis -277	Het Storingsmanagementsysteem is beschikbaar als beveiligde webapplicatie (authenticatie en versleuteling van de verbinding via HTTPS met geldig certificaat).
eis -278	Opdrachtnemer heeft de plicht om Storingen (in domeinen van derden of van Opdrachtgever) zo spoedig mogelijk te melden aan de relevante storingsorganisaties en waar nodig ondersteuning te verlenen bij het oplossen van de Storing dan wel te controleren of de Storing is opgelost.
eis -279	De Opdrachtnemer is verantwoordelijk voor het aanhouden, opslaan en beheren van alle benodigde reservematerialen, Personeel en materieel om aan de eisen met betrekking tot de Beschikbaarheid te kunnen voldoen. Het niet op voorraad hebben van een onderdeel is dus geen valide reden voor overschrijding van Functieherstelttijden of minimale beschikbaarheids-percentages.

8.5 Preventief Onderhoud en Innovatief Onderhoud

eis -280	Preventief Onderhoud en Innovatief Onderhoud dient uitgevoerd te worden volgens afspraken in de op te stellen DAP.
eis -281	Minimaal één keer per jaar zal de Opdrachtnemer Preventief Onderhoud uitvoeren op het Cameratoezichtsysteem dat in Onderhoud is. Opdrachtnemer dient alle betrokken installaties, Hardware na te lopen en de correcte functionaliteit vast te stellen. Onderdeel hiervan is de inspectie van logbestanden van het VMS die op problemen waaronder beveiligingsincidenten kunnen wijzen. In het geval van Camera's betreft het hier alleen werkzaamheden die op afstand uitgevoerd kunnen worden. Hardware op locatie bij Opdrachtgever of politie dient wel fysiek geïnspecteerd te worden.
eis -282	Opdrachtnemer is verantwoordelijk voor het tijdig verlengen en doorvoeren van alle (onderhouds)licenties en/of betalen van abonnementskosten van het Cameratoezichtsysteem.
eis -283	Tijdens het Preventief Onderhoud en/of Innovatief Onderhoud dient het Cameratoezichtsysteem zoveel mogelijk te blijven functioneren. Indien door het Preventief Onderhoud en/of Innovatief Onderhoud uitval van (onderdelen van) het Cameratoezichtsysteem niet te vermijden is dient Opdrachtgever hiervoor eerst akkoord te geven. Afspraken hierover worden nader gedetailleerd in het DAP.
eis -284	Onderdeel van het Preventief Onderhoud is het uitvoeren van Updates en back-ups conform de eisen in paragraaf 3.3.
eis -285	Het reserve-Uitkijkstation voor de wegverkeersleiders dient als eerste van Updates en/of Upgrades te worden voorzien en dient daarmee voor test- en acceptatiedoeleinden te worden gebruikt voordat tot Updates en/of Upgrades van de andere Uitkijkstations over wordt gegaan. Eén van de reserve-camera's zal in een beschermde kantooromgeving worden geplaatst en ontsloten via een door Opdrachtgever ter beschikking te stellen 5G-router. Deze camera dient gebruikt te worden voor testdoeleinden bij firmware-Updates.
eis -286	Preventief Onderhoud en Innovatief Onderhoud dient buiten de belangrijkste of drukste uitkijkuren te worden gerealiseerd.
eis -287	Minimaal één keer per jaar dient Innovatief Onderhoud uit te worden gevoerd op de Software van het VMS en bijbehorende Uitkijkstations.
eis -288	Preventief Onderhoud en Innovatief Onderhoud wordt pas uitgevoerd na overlegging aan en goedkeuring door Opdrachtgever van een onderhoudsplan. Dit plan dient ten minste in te gaan op: 1. Toelichting en algemene omschrijving werkzaamheden; 2. Planning incl. go/no go momenten; 3. Risico's en mitigerende maatregelen; 4. Impact op de bedrijfsvoering; 5. Roll-back scenario's.

8.6 Correctief Onderhoud

eis -289	Correctief Onderhoud dient te worden uitgevoerd op het Cameratoezichtsysteem, d.w.z. alle voorzieningen, Hardware incl. firmware die onder verantwoordelijkheid van Opdrachtnemer vallen. Onder Correctief Onderhoud wordt verstaan: het opsporen en herstellen van onvolkomenheden en Gebreken, nadat deze door de Opdrachtgever zijn gemeld of als deze op andere wijze zijn gebleken. In het geval van Camera's betreft het hier alleen werkzaamheden die op afstand uitgevoerd kunnen worden.
eis -290	Schade of Storingen die zijn veroorzaakt als gevolg van overmacht en die niet vanuit het ontwerp, toegepaste materialen en installatie voortkomen, worden per geval tussen de Opdrachtgever en Opdrachtnemer besproken en van acties voorzien. De Onbeschikbaarheid van het Cameratoezichtsysteem als gevolg van deze schade of defecten wordt dan niet meegerekend in de Onbeschikbaarheid toe te rekenen aan de Opdrachtnemer. Wel heeft de Opdrachtnemer een inspanningsverplichting deze Storingen zo snel mogelijk op te lossen.
eis -291	Correctief Onderhoud dient te worden uitgevoerd op alle door Opdrachtnemer geleverde en/of in Onderhoud genomen installaties.
eis -292	In geval van een Storing of Gebrek stelt de Opdrachtnemer onmiddellijk de herstelprocedure in werking. De herstelprocedure voorziet onder meer in: 1. Analyse van de Storing of het Gebrek, incl. inschatting van impact en omvang; 2. Diagnose van de oorzaak van de Storing of het Gebrek binnen de overeengekomen tijd incl. de planning van de uitvoering van de herstelwerkzaamheden, en eventuele maatregelen die getroffen moet worden om de gevolgen van de Storing of het Gebrek te beheersen; 3. Functieherstel; 4. Registratie in het Storingsmanagementsysteem of aanlevering van alle relevante gegevens t.b.v. Storingsmanagement.
eis -293	Indien van een Camera op afstand geen herstel mogelijk is dan zal de Onderhoudsaannemer van Opdrachtgever een swap & replace uitvoeren van de defecte Camera met een Camera uit de reservevoorraad. Het ondersteunen van de Onderhoudsaannemer en configuratie van het VMS om de Camera uit de reservevoorraad werkend te krijgen is onderdeel van het standaard Beheer en Onderhoud.
eis -294	Het ophalen van het defecte exemplaar en deze vervangen door een werkend exemplaar is onderdeel van de kosten voor Onderhoud (mits binnen de garantietermijn).

8.7 Rapportage

eis -295	Per kwartaal dient Opdrachtnemer een overzicht te overleggen van alle verrichte werkzaamheden in het kader van Beheer en Onderhoud. Deze rapportage wordt geleverd binnen één maand na afloop van de betreffende maand. In dit overzicht dient in ieder geval opgenomen te zijn:

	1. Overzicht van gemelde Storingen en Gebreken en het hierbij horende Correctief Onderhoud; 2. Onderscheid naar Gebreken binnen SLA en Gebreken/Storingen buiten de SLA; 3. Overzicht percentage Beschikbaarheid per component over de betreffende tijdsperiode van de rapportage, uitgesplitst naar binnen en buiten SLA; 4. Overzicht van gerealiseerde Functiehersteltijd per Gebrek waarbij Gebreken worden gemarkeerd die buiten de afgesproken Functiehersteltijd vallen; 5. Uitgevoerde werkzaamheden ten behoeve van Preventief Onderhoud waaronder Updates op firmware; 6. Uitgevoerde werkzaamheden ten behoeve van Innovatief Onderhoud waaronder Upgrades; 7. Uitgevoerde werkzaamheden én eventuele incidenten in het kader van informatiebeveiliging of privacy. Het vervangen van wachtwoorden en/of certificaten is onderdeel van de rapportage; 8. Overzicht van nieuw geïnstalleerde Hardware; 9. Reservematerialen die zijn gebruikt en voor welke Storing/project en de omvang van de reservevoorraad incl. identificatienummers per onderdeel; 10. Personele wijzigingen van personeel dat toegang heeft tot het systeem of gegevens van Opdrachtgever; 11. Actuele lijst van reservematerialen.
eis -296	Binnen twee maanden na afloop van het kalenderjaar wordt tevens een jaarrapportage opgeleverd. De jaarrapportage geeft zelfde informatie als de kwartaalrapportages maar voor de periode van het kalenderjaar. Onderdeel van de jaarrapportage is een eventueel boetebedrag o.b.v. de niet-behaalde prestatie-eisen.

8.8 Garantie

eis -297	De garantie op Hardware gaat in op het moment van werkend opleveren, dan wel toevoegen aan de reservevoorraad.
eis -298	De fabrieksgarantie op Camera's is minimaal 3 jaar. **Inschrijver toont dit aan** in een bijlage bij Inschrijving (zie inschrijvingsleidraad, paragraaf 3.4.2.4).
eis -299	De garantie op alle Hardware is minimaal acht jaar. Opdrachtgever realiseert zich dat het zeer waarschijnlijk niet mogelijk is om met de initieel aangeboden en geleverde Hardware gedurende deze periode aan alle eisen te voldoen, bijv. eisen m.b.t. Beschikbaarheid, Updates en Upgrades. Inschrijver dient daarom in zijn Inschrijving hiermee rekening te houden door bij ingang van het (optionele) zesde jaar ten minste alle werkstations, Uitkijkstations en Servers te vervangen. De kosten hiervoor dienen verwerkt te worden in de kosten voor Beheer en Onderhoud van jaar 6 in het prijzenblad.

	Camera's hoeven in principe niet vervangen te worden gedurende de looptijd van de Overeenkomst, tenzij deze een onherstelbaar Gebrek vertonen. Wel dient Inschrijver zich te realiseren dat als de aangeboden Camera niet meer ondersteund wordt door de fabrikant gedurende de potentiële looptijd van acht jaar, en er treedt een security-probleem op, alle Camera's op kosten van de Opdrachtnemer vervangen moeten worden voor een vergelijkbaar model.
eis -300	Garantietermijnen langer dan de fabrieksgarantie vervallen bij beëindiging van de Overeenkomst. De fabrieksgarantie vervalt niet bij beëindiging van de Overeenkomst. Bij beëindiging van de Overeenkomst wordt informatie overgedragen zodat het mogelijk is voor een nieuwe leverancier om de fabrieksgarantie te kunnen claimen.
eis -301	Gedurende de garantietermijn zijn alle kosten waaronder diagnose-, transport-, reparatie- en/of vervangingskosten incl. uren en voorrijkosten etc. voor rekening van de Opdrachtnemer. De kosten van de Onderhoudsaannemer zijn niet voor Opdrachtnemer.
eis -302	Opdrachtnemer dient een duidelijke administratie up-to-date te houden waarbij voor elke Camera eenvoudig is te herleiden wanneer de garantie is ingegaan.

8.9 Documentatie

eis -303	De As-builtdocumentatie van het Cameratoezichtsysteem dient actueel te zijn en na elke wijziging moet de As-builtdocumentatie binnen één maand aangepast worden en beschikbaar worden gesteld aan de Opdrachtgever. Indien blijkt dat de As-builtdocumentatie niet actueel is, is de boeteclausule van toepassing tot aan het moment dat de Opdrachtnemer de up-to-date documentatie oplevert. Het bijwerken van As-builtdocumentatie n.a.v. een Aanpassing is een standaard verplichting van de Opdrachtnemer.
eis -304	De As-builtdocumentatie wordt digitaal beschikbaar gesteld en is zo georganiseerd dat informatie en gerelateerde informatie snel kan worden gevonden en kan worden uitgebreid met aanvullende documenten van bijv. Opdrachtgever. De As-builtdocumentatie dient lokaal bij Opdrachtgever beschikbaar te zijn. Na elke Aanpassing wordt een volledige up-to-date versie van de As-builtdocumentatie beschikbaar gesteld.
eis -305	Onderdeel van de As-builtdocumentatie is documentatie van het netwerk: IP-plan, gebruikte VLANs, segmentering van het netwerk, en alle andere relevante informatie nodig om Beheer en Onderhoud hierop uit te kunnen voeren.
eis -306	Onderdeel van de As-builtdocumentatie zijn foto's en schematische tekeningen van de door de Opdrachtnemer geïnstalleerde installatie, waaronder: 1. Overzichtstekeningen en logische schema's die tonen welke componenten in het systeem zitten, hoe deze met elkaar zijn verbonden en hoe informatie wordt verwerkt; 2. Een kaart (kmz-bestand) met daarop de locaties van de Camera's; 3. Foto's van de gehele installatie excl. Camera's.
eis -307	Van elke elektrische component wordt in de As-builtdocumentatie in een MS Excel bestand de volgende informatie gespecificeerd:

	1. Identificatienummer dat ook op de sticker wordt aangebracht; 2. Naam; 3. IP-adres en MAC-adres (bij een Netwerkcomponent); 4. Merk en type; 5. Datum installatie; 6. Locatie gespecificeerd als kruispuntnummer (bij een Camera); 7. Adres (benadering) of ruimtenummer; Dit overzicht wordt bij elke Aanpassing geactualiseerd binnen één maand.
eis -308	Van elk type geleverde Hardware-component wordt de fabrieksdocumentatie aan de As-builtdocumentatie toegevoegd (handleiding en specsheet).
eis -309	De gebruikershandleidingen worden in de Nederlandse taal aangeleverd. Technische documentatie dient in de Engelse of Nederlandse taal gesteld zijn.