



Gemeente Amsterdam

Bijlage 6

Programma van Eisen

Regulier cameratoezicht

Beheer en onderhoud CCTR

Contractnummer AI 2026-0113

Inhoudsopgave

Begripsbepalingen	4
1 Algemene eisen	10
1.1 Eisen aan de opdracht	10
1.2 Prijzen inschrijving en gedurende looptijd contract	11
1.3 Eisen Hardware en Software	11
1.4 Eisen m.b.t. informatiebeveiliging en privacy	14
1.5 Eisen aan personeel en organisatie	17
1.6 Spare-parts	18
1.7 Eigen mobiele systemen	19
2 Overdracht en overname	20
3 Videomanagementsysteem	21
4 Werkplekken en servers	23
4.1 Algemene eisen clients en servers	23
4.2 Uitkijkplek	23
4.3 Servers	25
5 Camera's	26
5.1 Algemene eisen	26
5.2 Beveiligingseisen aan camera's	27
5.3 Eisen bestuurbare dome-camera (PTZ-Domecamera)	27
5.4 Vernieuwing	28
6 Draadloze verbindingen	29
6.1 Algemene eisen	29
6.2 Licentievrij 5GHz	29
6.3 Licentievrij 60GHz	30
6.4 De 3.5 GHz-band	Fout! Bladwijzer niet gedefinieerd.
6.5 Point-to-point gelicenseerd	30
7 Werken in de openbare ruimte, en in en op panden	31
7.1 Algemene eisen veiligheid en vergunningen	31
7.2 230V voedingsaansluitingen	32
7.3 Tijdelijke stroomvoorzieningen	33
7.4 Cameramasten en andere voorzieningen	33
7.5 Straatkasten en junctionboxen	34
7.6 Montage	35
7.7 Ondergrondse infrastructuur	36

8	Netwerk-aspecten	37
8.1	Eisen algemeen	37
8.2	Netwerkveiligheid	37
8.3	Eisen aan switches	38
8.4	Netwerkmonitoring	39
9	Aanpassingen, implementatie en oplevering	41
9.1	Aanpassingen	41
9.2	Oplevering	42
10	Beheer en onderhoud en aanpassingen Cameratoezicht	44
10.1	Algemeen, beschikbaarheid en regelingen	44
10.2	Kosten	45
10.3	Storingsmanagement	45
10.4	Preventief onderhoud en schoonmaak Camera's	47
10.5	Correctief onderhoud	48
10.6	Rapportage	49
10.7	Garantie	51
10.8	Documentatie	51



Begripsbepalingen

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

Algemene begrippen

Aanbestedingsdocumenten	Het geheel van alle documenten die ten behoeve van deze aanbesteding zijn opgesteld, te weten de selectieleidraad met bijbehorende nota van inlichtingen, het bestek met bijbehorende nota van inlichtingen en alle bijlagen
Aanpassing	Een aanpassing betreft een verandering van het Cameratoezichtstelsel als gevolg van een uitbreiding, wijziging, verwijdering van één of meerdere onderdelen van het Cameratoezichtstelsel. Na doorvoering van de Aanpassing functioneert het Cameratoezichtstelsel weer conform de eisen zoals verwoord in het PvE
Acceptatie	Acceptatie betekent goedkeuring door Opdrachtgever op het moment dat het Cameratoezichtstelsel na de SAT-test en oplossing van alle geconstateerde restpunten, 1 maand probleemloos heeft gefunctioneerd én de as-built documentatie is opgeleverd. Alvorens tot Acceptatie over te kunnen gaan dient de acceptatietest volgens een vooraf vastgestelde acceptatieprocedure en acceptatieprotocol te worden uitgevoerd.
Beheer en Onderhoud	De werkzaamheden voor het preventief, adaptief, correctief en aanpassend onderhoud aan het te leveren systeem en bijbehorende documentatie.
Bestek	Het geheel van documenten waarin Opdrachtgever de offerteprocedure en het programma van eisen heeft verwoord en waarop de Inschrijver zijn Offerte dient te baseren.
Camera	Dit is een Netwerkkomponent die één of meer live videostreams uitstuurt en het betreft hier een geïntegreerd geheel incl. behuizing, beugels en lens.
Cameratoezichtstelsel	De onderdelen van het gehele camerasysteem die onder verantwoordelijkheid van de Leverancier vallen.
CCTR	Centrale Cameratoezichtruimte. De centrale uitkijkrimte van de gemeente(s) op politielocatie waar onder politieregie door gemeentelijk medewerkers de camerabeelden worden uitgekeken.
Contractpartner	Dit betreffen de drie organisaties die gezamenlijk de Overeenkomst met Leverancier aangaan.
Contractregisseur	De door de Opdrachtgever aangewezen persoon die de



	Overeenkomst centraal beheert.
DAP	Dossier Afspraken en Procedures. Een aanvullend document naast de SLA waarin de procedures over samenwerking en de serviceverlening staan beschreven.
Diagnosetijd	De tijd waarbinnen na melding van een storing een diagnose over de oorzaak van de storing is gesteld.
Gebrek	Het niet of niet volledig voldoen aan de overeengekomen eisen, specificaties of eigenschappen.
Hardware	De door Leverancier op basis van deze Overeenkomst te leveren of in beheer te nemen apparatuur, inclusief bijbehorende materialen en documentatie en met inbegrip van de meest recente versie van de systeemprogrammatuur.
Inschrijver	Een rechtspersoon (of een combinatie van rechtspersonen) die naar aanleiding van dit Bestek een Offerte heeft ingediend.
Koppelvlak	Een koppelvlak is een punt waar infrastructuren met elkaar worden verbonden volgens een bepaalde standaard die uitwisseling van gegevens verzorgt.
Leverancier	De rechtspersoon (of een combinatie van rechtspersonen) aan wie op basis van dit Bestek de Opdracht is gegund.
Nota van Inlichtingen	Een document dat dient als aanvulling of wijziging op dit Bestek. De verstrekte Nota van Inlichtingen maakt deel uit van dit Bestek.
Offerte	Een aanbieding van Leverancier uitgebracht aan Opdrachtgever gebaseerd op de eisen en wensen van Opdrachtgever zoals beschreven in dit Bestek.
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 Leverancier voor een Aanpassing van het Cameratoezichtstelsysteem.
Opdracht	Het geheel aan werkzaamheden dat wordt opgedragen door Opdrachtgever om een Aanpassing op het Cameratoezichtstelsysteem door te voeren.
Opdrachtgever	De Contractpartner van de Leverancier die opdracht voor een Aanpassing geeft. Dit kan zijn: Gemeente Amsterdam, Gemeente Amstelveen of Politie Eenheid Amsterdam.
Oplostijd	De tijd waar binnen na melding van een storing volledig functieherstel heeft plaatsgevonden.
Overdrachtsdatum	Het moment waarop het huidige contract wordt beëindigd en het nieuwe contract ingaat.
Overdrachtsperiode	Een periode van twee maanden direct voorafgaand aan de Overdrachtsdatum. In deze periode wordt de nieuwe Leverancier in staat gesteld het over te nemen systeem te onderzoeken en te



	leren kennen.
Overeenkomst	Overeenkomst tussen Contractpartner en Leverancier betreffende de voorwaarden die gelden voor de Opdracht.
Penvoerder aanbesteding	Ingenieursbureau Gemeente Amsterdam.
Programma van Eisen	De functionele omschrijvingen van de levering en dienstverlening waarin eisen zijn gesteld.
Reiskosten	Dit betreffen alle kosten die gemaakt worden voor zakelijke reizen voor afspraken met Opdrachtgever, niet zijnde woon-werkverkeer en niet zijnde voorrijkosten. Reiskosten mogen niet apart in rekening worden gebracht, maar zijn opgenomen in het uurtarief.
Responstijd	De tijd waar binnen na melding van een storing deze door Leverancier in behandeling is genomen, incl. terugkoppeling hiervan aan Opdrachtgever.
SLA	Service Level Agreement, een schriftelijke overeenkomst tussen Opdrachtgever en Leverancier waarin de te leveren diensten en het overeengekomen kwaliteitsniveau hiervan worden beschreven.
SMA	Onderhoudscontract op aangeschafte software die recht geeft op ondersteuning, foutoplossing, updates en upgrades.
Software	Het geheel van alle software noodzakelijk voor dit project, waaronder het VMS en de aanvullende software om de goede werking van het Cameratoezichtstelsel te garanderen.
Storingsmanagement-systeem	Een systeem dat wordt gebruikt voor registratie en communicatie tussen Opdrachtgever en Leverancier over geconstateerde verstoringen en de status hiervan.
Supervisor-plek	Een voorziening waarmee live doorlopend een groep beelden kan worden gevolgd, en van waaruit Camera's kunnen worden bestuurd (Pan, Tilt, Zoom) en beelden kunnen worden doorgeschakeld naar betrokken derden, zoals bijvoorbeeld het Operationeel Centrum Politie.
Terugkijkplek	Een voorziening waarmee, zowel live als opgenomen, doorlopend een groep beelden kan worden gevolgd. Live Camera's kunnen worden bestuurd (Pan, Tilt, Zoom), waarbij ook een videowall is aangekoppeld en waar beelden kunnen worden veiliggesteld en ter beschikking van derden kunnen worden gesteld.
Tijdelijke-/Spoedcamera	Dit is een tijdelijke Netwerkkomponent en eventuele bijbehorende netwerkvoorzieningen op huurbasis die één of meer live videostreamen uitstuurt die in het Cameratoezichtstelsel geïntegreerd dienen te worden. Tijdelijke Camera's vallen onder perceel 2 van deze aanbesteding.
Uitkijkplek	Een voorziening waarmee live doorlopend een groep beelden kan



	worden gevolgd, en van waaruit Camera's kunnen worden aangestuurd (Pan, Tilt, Zoom), waarbij ook een videowall is aangekoppeld
Update	Een update van software (niet firmware) betreft een nieuwe versie waarin fouten worden hersteld en er geen significante nieuwe functionaliteit wordt toegevoegd. Het versienummer wijzigt niet. In het geval van firmware is elke wijziging van de firmware een update, ook als het versienummer wijzigt.
Upgrade	Een upgrade van software (niet firmware) betreft een nieuwe versie van de software met nieuwe functionaliteit waarbij het major of minor versienummer wijzigt.
Verkeerscamera	Dit is een Camera met als primaire doel het voorzien van de Verkeerscentrale van een live videostroom.
Verkeerscentrale	De locatie waar de beelden van de Verkeerscamera's worden uitgekeken.
VMS	Videomanagement-systeem, de door Contractpartner in samenhang met de Hardware gebruikte programmatuur voor het aansturen van Camera's en opslag van beelden.
Voorrijkosten	Dit betreffen kosten die in rekening gebracht mogen worden voor voorrijden van een servicemonteur voor het verrichten van onderhoud en/of reparatie aan het Cameratoezichtstelsel buiten de SLA.

Technische begrippen

Camerastream	De digitale live stroom van videobeelden die door een Camera, of door een encoder naar het VMS en/of uitkijk- en meekijkstations wordt gestuurd.
DVI-D	De volledig digitale variant van de Digital Visual Interface. Deze wordt gebruikt voor uitwisseling van video-informatie tussen de grafische kaart en de monitor.
Energystar	Energy Star is een internationaal programma voor de vrijwillige labeling van energie-efficiënte apparaten, in het leven geroepen door de US Environment Protection Agency (EPA) in 1992. Door middel van een Overeenkomst met de Amerikaanse overheid participeert de Europese Unie in het Energy Star Programma voor zover het kantoorapparatuur betreft.
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.
Gbps	Gigabit per seconde, zie ook Mbps
GMK	Gemeenschappelijke Meldkamer. Centrale voorziening in het Hoofdbureau van de politie waar onder andere camerabeelden getoond kunnen worden.
HD	Een resolutie van 1280x720 pixels.
HDMI	High-Definition Multimedia Interface. Digitale interface voor de uitwisseling van video- en audio-informatie.
IKxx	Onderdeel van de Europese Norm EN62262 die de bescherming van apparatuur tegen mechanische impact specificeert.
IP66	Code die de bescherming van elektrische apparatuur tegen stof en vocht aangeeft. IP66 betekent dat een elektrisch apparaat volledig beschermd is tegen indringing van stof en beschermd tegen indringing van water bij een krachtige waterstraal (100 l./min.) onder een willekeurige hoek.
IP67	Code die de bescherming van elektrische apparatuur tegen stof en vocht aangeeft. IP67 betekent dat een elektrisch apparaat volledig beschermd is tegen indringing van stof en beschermd tegen indringing van water bij onderdomping tot 1 meter gedurende 30 minuten.
Mbps of Gbps	Megabit of Gigabit per seconde, een maat voor de hoeveelheid informatie die wordt verzonden en/of ontvangen.
MP	Megapixel. Een Camera met een resolutie van bijv. 3MP levert een beeld met ca. 3 miljoen pixels.
Netwerkkomponent	Elk elektrisch apparaat met een eigen IP-adres.
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.
SAAS	Software as a Service. De te gebruiken software wordt niet bij de gebruiker geïnstalleerd, maar bij de SaaS-aanbieder. De gebruiker heeft toegang tot de software via internet of een privénetwerk.
Salvo	Een groep samenhangende Camera's en eventueel kaarten die met één handeling wordt opgeschakeld.
SDK	Software Development Kit voor integratie met producten van derden.
SNMP	Simple Network Management Protocol. Een protocol voor het management van de netwerkkomponenten in een IP-netwerk. Via



Gemeente Amsterdam

	SNMP-boodschappen kunnen apparaten elkaar of een netwerkmanagementsysteem 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.

1 Algemene eisen

1.1 Eisen aan de opdracht

eis -1	Leverancier draagt zorg een volledig functionerend systeem bestaande uit alle geleverde componenten, overgenomen bestaande componenten en integratie met andere systemen (intern of van derden). De gedurende de looptijd van het contract overgenomen en geleverde producten dienen één geïntegreerd geheel te vormen.
eis -2	Alle aanpassingen en uitbreidingen gedurende de looptijd van het contract leiden ertoe dat er sprake is en blijft van een volledig werkend systeem conform de eisen uit dit document.
eis -3	Leverancier zal aan alle toepasselijke en/of verplichte normen en richtlijnen voor installatie van datanetwerken, laagspanningsinstallaties en beveiligingsnetwerken voldoen waaronder: <ul style="list-style-type: none"> • Laagspanningsrichtlijn 73/23/EEG • EMC – richtlijn 89/336/EEG • NEN 5152 Elektrotechnische symbolen, inclusief de Aanvullingen. • NEN 1010, Veiligheidsbepalingen voor laagspanningsinstallaties. • NEN 3140, Bedrijfsvoering van elektrische installaties – Laagspanning.
eis -4	De Leverancier zal de integratie met het reguliere cameranetwerk van Spoed Camera's door de leverancier van spoedcameratoezicht uitvoeren binnen één uur na oplevering van een Spoed Camera.
eis -5	De Leverancier zal samenwerken met alle leveranciers van systemen die raken aan het te leveren systeem. Voorbeelden hiervan zijn: <ul style="list-style-type: none"> • De leverancier van Spoedcameratoezicht. • De koppeling met Coppweb voor incidentmanagement via de Genetec SDK. • Het systeem van de Verkeerscentrale, ProRail, JC Arena (verbonden via Federation-koppelingen). • Ontsluiting van Verkeerscamera's via draadloze verbindingen van Opdrachtgever. • Leveranciers van netwerkverbindingen zoals bijvoorbeeld KPN en Ziggo. • Leveranciers van producten die buiten de scope van de aanbesteding vallen. • Leveranciers van producten van derden die met het VMS geïntegreerd dienen te worden. • Experimentele systemen voor videoanalyse die via het VMS één of meer videostromen ontvangen.
eis -6	De Leverancier zal samenwerken met alle partijen die zich manifesteren in de openbare ruimte die werkzaamheden uitvoeren die raken aan de Camera's.
eis -7	Kantoortijden gelden op officiële werkdagen van 8.00 tot 18.00 uur. Avonduren gelden van 18.00 – 24.00 uur. Nachturen gelden van 24.00 – 6.00 uur. Vroege ochtend geldt van 6.00 – 8.00 uur.
eis -8	Alle installatieonderdelen en de installatie als geheel dienen te worden gerealiseerd voor een 24 uren continu 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 -9	Leverancier zal gedurende de looptijd van het contract een functionaris aanstellen die als primair

	aanspreekpunt zal dienen. Deze functionaris zal ten minste elk kwartaal overleg met de Opdrachtgever hebben over o.a. lopende of verwachte wijzigingen van het systeem, de staat van het onderhoud en het behalen van de afgesproken beschikbaarheidscriteria.
eis -10	Indien Leverancier een door Opdrachtgever aangedragen aannemer of leverancier (bijv. Ziggo, Liander voor elektra, gemeentelijk vergunningenloket) inzet zullen deze indien mogelijk direct hun facturen naar de betreffende Opdrachtgever sturen rekening houdend met de geldende financiële richtlijnen. Indien directe facturatie aan Opdrachtgever niet mogelijk is dan zal verrekening lopen via de Leverancier met een maximumopslag van 5% en een maximum bedrag van Euro 500 (laagste van de twee bedragen geldt).
eis -11	Het gedurende de contractperiode niet voldoen aan contractueel overeengekomen verplichtingen kan leiden tot een boete voor de Leverancier. De hoogte van deze boete is in de Overeenkomst opgenomen. Dit document maakt deel uit van de Overeenkomst en vallen dus onder de noemer "contractueel overeengekomen verplichtingen".

1.2 Prijzen inschrijving en gedurende looptijd contract

eis -12	Alle eenheidsprijzen genoemd in de Inschrijving, zullen gelden als verrekenprijzen bij aanpassingen, bijv. bij uitbreiding van het aantal Camera's, clients, servers, etc. Voor elke aanpassing wordt een verzoek tot offerte gedaan aan de hand waarvan een Offerte wordt opgesteld op basis van de vastgestelde eenheidsprijzen. Indien er voor bepaalde leveringen of diensten geen eenheidsprijzen bekend zijn dient de Leverancier marktconforme tarieven in rekening te brengen. Indien Contractpartner van mening is dat de tarieven niet marktconform zijn, dan kan dit reden zijn om de Offerteaanvraag, of delen hiervan, elders onder te brengen, of onderdelen als directielevering aan Leverancier beschikbaar te stellen. Bij opvolgers van de aangeboden producten dient minimaaldezelfde korting te worden gehanteerd op de listprice van de fabrikant.
---------	---

1.3 Eisen Hardware en Software

eis -13	Er dient gebruik te worden gemaakt van generieke hardware voorzien van genormeerde interfaces, die niet gebonden is/zijn aan een specifieke merkgebonden systeemoplossing.
eis -14	De aangeboden combinatie van producten voldoet aan de eisen gesteld aan individuele producten. Bijvoorbeeld: eisen gesteld aan een Camera zijn ook realiseerbaar in combinatie met het gebruikte VMS, werkstations, etc.
eis -15	Producten en installatie hiervan dienen te voldoen aan de geldende EMI- en EMC-normen waarbij de apparatuur onderling geen verstoringen veroorzaken of verstoringen veroorzaken op andere apparatuur. Daarbij dient rekening gehouden te worden met een geconditioneerde kantooromgeving.
eis -16	Alle componenten dienen bij het daarvoor bestemde gebruik geen gevaar op te leveren voor gezondheid of het milieu, zowel tijdens installatie, bij gebruik, als bij afvalverwerking.
eis -17	Bij alle te leveren materialen wordt gebruikgemaakt van nieuwe kwaliteitscomponenten van lopende productie van een producent met een eigen serviceorganisatie. Materialen en onderdelen zijn nog ten minste 5 jaar na te leveren of middels reserveonderdelen of vervangende onderdelen in bedrijf te

	houden zonder afbreuk te doen aan de systeemeisen en vormgeving (bijvoorbeeld monitoren). Reserve-onderdelen dienen minimaal een gelijkwaardige kwaliteit te hebben vergeleken met het origineel.
eis -18	Alle apparatuur moet geleverd worden met de CE-markering.
eis -19	<p>Op het prijzenblad, kolom Toelichting door leverancier, levert Inschrijver een specificatie van merk en type van alle relevante (potentieel) te leveren apparatuur (zoals gespecificeerd in het Prijsinvalformulier) incl. maximaal stroomverbruik, gemiddeld stroomverbruik en, indien van toepassing, ruimtegebruik bij plaatsing in 19"-kast (HE) of straatkast (br x hg x dp in mm). Het betreft hier ten minste:</p> <ul style="list-style-type: none"> • Camera's (alle uitgevraagde types) • Werkstations • Servers • Apparatuur voor draadloze verbindingen • Switches en andere netwerkapparatuur • Monitors <p>Dit overzicht wordt geleverd in tabelvorm (bijv. Excel-bestand), ondersteund met separate productdocumentatie. Deze producten dienen overeen te komen met de producten genoemd in het prijsinvalformulier.</p>
eis -20	Op het prijzenblad, kolom Toelichting door leverancier, levert Inschrijver een specificatie van merk en type van alle relevante (potentieel) te leveren straatkasten, junctionboxen en stroomkasten zoals gespecificeerd in het Prijsinvalformulier.
eis -21	<p>De apparatuur (inclusief cameraconfiguraties) dient volledig conform de bijbehorende specificaties te functioneren indien aangesloten op een elektrische installatie met de volgende eigenschappen:</p> <ul style="list-style-type: none"> • Spanning 200 - 240 Volt; • Frequentie 47 - 53 Hertz; • Spanningsonderbreking 20 msec. maximaal. <p>Indien aanbevolen volgens bijvoorbeeld NEN-normen en/of eigenaar van een object waarvan gebruik wordt gemaakt dit nodig acht en/of noodzakelijk volgens de wet, dan dient de Leverancier zelf voor de aarding van de apparatuur zorg te dragen. De serverkasten in de dataruimtes die beschikbaar worden gesteld zijn geaard.</p> <p>Het is toegestaan om camera's te voeden via PoE en een switch via een 24/48V voeding. Echter, de voeding zelf wordt uiteindelijk weer gevoed via 230V en in een dergelijk geval dient deze voeding om te kunnen gaan met de specificaties zoals hierboven genoemd.</p>
eis -22	Leverancier levert Hardware en Software incl. alle benodigde licenties voor onderhoud, ondersteuning, updates en software-upgrades gedurende de looptijd van het contract.
eis -23	Hardware zoals clients, wordt, tenzij expliciet aangegeven dat dit niet het geval is, geplaatst in 19"-racks in de ruimte van de Opdrachtgever. Hierbij mag er van worden uitgegaan dat deze racks staan opgesteld in een geconditioneerde ruimte met een maximum temperatuur van 27°C. De verantwoordelijkheid van de Leverancier omvat ook de levering van alle patchkabels. Apparatuur dient waar mogelijk specifiek geschikt te zijn voor montage in een 19"-rack. Indien dit niet mogelijk is dan wordt apparatuur op een nette manier geplaatst, bijv. een legbord of montagerail. Leverancier is

	verantwoordelijk voor dergelijke montagevoorzieningen.
eis -24	Alle systemen dienen na herstel van de spanningsuitval automatisch te herstarten en operationeel te zijn binnen 15 minuten na terugkomen elektriciteitsvoorziening.
eis -25	Elk Netwerkcomponent dient manageable te zijn via een netwerkmonitoring systeem (o.b.v. laatste versie SNMP (v3 bij start contract). Apparatuur dient te kunnen communiceren met een monitoring-server (van de Contractpartner, zie ook Hoofdstuk 8) en via zgn. SNMP-traps een alarm naar dit monitoringsysteem te kunnen sturen.
eis -26	Binnen het gehele Cameratoezichtstelsel is er sprake van één systeemtijd. Het is niet toegestaan dat servers en clients een verschillende tijd hebben. Leverancier is er verantwoordelijk voor dat de systeemtijd max. 200ms afwijkt van de lokale absolute tijd. Leverancier mag uitgaan van beschikbaarheid van tijdservers over internet.
eis -27	Alle licenties dienen in beginsel op naam van de opdrachtgever te worden gesteld. Indien dit niet mogelijk is, dan is afwijking hiervan alleen mogelijk na overleg en toestemming van de opdrachtgever. Na beëindiging contract zal de tenaamstelling door Opdrachtnemer weer gewijzigd dienen te worden naar Opdrachtgever of de nieuwe partij voor regulier cameratoezicht.
eis -28	De toegang tot alle netwerkcomponenten verloopt via een systeem met accounts en passwords. Bij installatie dienen wachtwoorden te zijn ingesteld. Het is niet toegestaan om fabriekswachtwoorden te handhaven. Leverancier dient een systeem te gebruiken dat voorkomt dat bij meerdere klanten dezelfde wachtwoorden worden gebruikt. Er moet minimaal voldaan worden aan de laatste BIO basisnorm (op moment van schrijven: BIO2 v1.3).
eis -29	Gebruikslicenties dienen gebaseerd te zijn op het aantal simultane gebruikers of het aantal client-werkstations waarop de software is geïnstalleerd.
eis -30	Leverancier garandeert dat de test of implementatie van nieuwe releases of aanpassingen in hard- en software niet zullen leiden tot verstoringen afgezien van een korte downtime bij updates. Updates zijn altijd binnen één uur terug te draaien indien er problemen optreden.
eis -31	De te leveren apparatuur gaat zuinig met energie om. Bij gelijke geschiktheid dient gekozen te worden voor energiezuinige varianten.
eis -32	Indien een producent kritische updates uitbrengt van één van de producten die onder het beheer van de Leverancier vallen, dan dienen deze één week te worden doorgevoerd (waarbij eerst getest wordt of de updates tot problemen leiden).
eis -33	Leverancier zorgt gedurende de looptijd van het contract voor onderhoud van het aangeboden systeem resulterend software-updates in elk kwartaal. Dit betekent in ieder geval dat Contractpartner tijdig kan overschakelen op nieuwe Windows-versies, browser-versies e.d. Indien Contractpartner door het uitblijven van updates gedwongen wordt niet meer ondersteunde of onveilige software-producten te handhaven dan is er sprake van onbeschikbaarheid van het Cameratoezichtstelsel en is de boeteclausule van toepassing.
eis -34	Het systeem mag niet afhankelijk zijn van software die end-of-life of niet ondersteund is. Software die end-of-life is dient verwijderd te worden.
eis -35	De Leverancier zorgt ervoor dat gedurende de looptijd van het contract alle door hem geleverde of overgenomen systeemonderdelen werken op recente firmware- of software-versies (in het geval het

	niet de laatste versie betreft, niet ouder dan 3 maanden) van de softwareproducten die volledig ondersteund worden door de fabrikant. eis -32 prevaleert boven deze eis. Indien Leverancier hiervan af wil wijken dient toestemming (incl. motivatie) aan Contractpartner te worden gevraagd.
eis -36	Producten of productlijnen die in de afgelopen twee jaar van US CERT (http://www.us-cert.gov) een CVSS v3 base score van 9.5 of hoger hebben gehad worden uitgesloten van levering. Indien tijdens de looptijd van het contract blijkt dat geleverde producten een ernstige bedreiging vormen voor de netwerkveiligheid van het Cameratoezichtsysteem, blijkende uit een CVSS v3 base score van 9.5 of hoger van US CERT, en de producent niet binnen 1 maand met een oplossing komt, dan dienen alle betrokken producten op kosten van Leverancier binnen 1 maand vervangen te worden voor een gelijkwaardig product. Indien fabrikant met een oplossing komt wordt dit product desondanks uitgesloten van elke nieuwe levering.
eis -37	Na elke wijziging aan de configuratie van een component die onder beheer van de Leverancier valt dient een back-up van de instellingen uitgevoerd te worden zodat bij uitval van een component deze vervangen kan worden 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. Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest.

1.4 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. Het DAP document kan op basis van de beschikbaarheid, integriteit en vertrouwelijkheid extra worden aangevuld met beheersmaatregelen.

eis -38	Leverancier garandeert dat alle processen van en voor de Contractpartner betreffende de verwerking, opslag en vernietiging van persoonsgegevens conform de Wet politiegegevens (WPG) wordt geborgd. En eventueel waar van toepassing de AVG). Leverancier waarborgt dat persoonsgegevens in het kader van de levering van de ICT-prestatie uitsluitend binnen de Europese Economische Ruimte (EER) worden verwerkt. Doorgifte naar landen buiten de EER is enkel toegestaan wanneer Opdrachtgever daar expliciet voorafgaand toestemming voor heeft verleend en een passend beschermingsniveau ten aanzien van de persoonsgegevens is gewaarborgd.
eis -39	De Leverancier sluit met Opdrachtgever een verwerkersovereenkomst af. De verwerkersovereenkomst is een overeenkomst/afspraken tussen de verantwoordelijke en bewerker in de zin van de Wet politiegegevens (Wpg) of vervangende wetgeving. In een verwerkersovereenkomst wordt vastgelegd hoe de bewerker met de persoonsgegevens dient om te gaan. Tevens worden in het contract afspraken vastgelegd betreffende aansprakelijkheid en schade in geval van incidenten. Het model van deze overeenkomst is te vinden in Bijlage 10.
eis -40	Indien Leverancier zelf producten ontwikkeld dan is Leverancier verantwoordelijk dat de aangeboden producten tijdens de ontwikkeling worden gecontroleerd op mogelijke beveiligingsissues.

eis -41	Leverancier informeert en adviseert de Contractregisseur over de eventueel te nemen maatregelen om beveiligingslekken te dichten. Leverancier dient actief de kwetsbaarheden te volgen die gepubliceerd worden (bv http://www.cvedetails.com) en de nodige acties te nemen.
eis -42	Leverancier heeft patch-management en vulnerability-management ingericht, alle systemen en devices zijn voorzien van de meest recente updates. Hiervoor is een aantoonbaar patchmanagementproces van toepassing.
eis -43	Leverancier heeft een adequaat beveiligingsbeleid voor gevoelige klantinformatie zoals wachtwoorden. Ten minste de volgende uitgangspunten gelden (waarbij de laatste BIO versie leidend is): <ul style="list-style-type: none"> • Minimale lengte: De minimale wachtwoordlengte is 12 posities. • Vernieuwing: Indien er geen tweefactor-authenticatie (2FA) mogelijk is, moet het wachtwoord minimaal halfjaarlijks worden vernieuwd. • Complexiteit: Er wordt geadviseerd om een wachtwoord van ten minste 12 tekens te gebruiken, maar 14 of meer is beter. • Zijn de tekens van een wachtwoord zo willekeurig mogelijk gekozen dat individuele tekens of combinaties van tekens geen voorspellende waarde hebben voor de rest van het wachtwoord • Alle gegevensdragers (memorysticks, laptops, etc.) met klantgevoelige informatie die buiten de vestiging van leverancier komen, worden volledig versleuteld. Bij laptops en tablets wordt gebruikgemaakt van versleuteling van de volledige harde schijf (bijv. Microsoft Bitlocker, VeraCrypt). • De kantooromgeving van de Leverancier is adequaat beveiligd tegen digitale én fysieke inbraak uitgaande van NEN-8131 en VKRI 2.0. • Communicatie van gevoelige gegevens, bijv. via internet of memory-sticks, is altijd versleuteld met ten minste AES-256 bits of gelijkwaardig/beter.
eis -44	Uitwisseling van videobeelden over internet (bijv. via de Genetec Mobile App) dient altijd versleuteld te zijn via HTTPS. TLS 1.2 of hoger.
eis -45	Leverancier implementeert de aanbevelingen van de Genetec Hardening Guide en controleert hier regelmatig op. Indien Leverancier van mening is dat hiervan afgeweken dient te worden dan wordt de afwijking eerst gemotiveerd voorgelegd aan Contractpartner. Afwijking is alleen toegestaan na expliciete schriftelijke goedkeuring van de Contractregisseur.
eis -46	Leverancier zal alle medewerking verlenen bij het uitvoeren van audits door derde partijen in het kader van privacy en beveiliging. De Contractpartner zal ca. eenmaal per twee jaar door een derde partij een zgn. pen en hacktest uit laten voeren. Kritische problemen die hieruit voortkomen dienen binnen één week te zijn opgelost, anders is in het kader van het boeteregime sprake van onbeschikbaarheid van het systeem. Kosten voor de hertest na geconstateerde Gebreken zijn voor Leverancier met uitzondering van de allereerste hertest gedurende looptijd contract. Een hertest zal zich beperken tot de geconstateerde problemen.
eis -47	Leverancier voldoet aan de Cyberbeveiligingswet (Cbw), de Nederlandse vertaling van de Europese NIS2-richtlijn, zodra deze van kracht is. Of minimaal 4 maanden na het ingaan hiervan.
eis -48	Bij afvoer van (apparatuur met) datadragers zal Leverancier toezien op vernietiging van alle aan Opdrachtgever gerelateerde informatie waaronder camerabeelden. Vernietiging van de informatie wordt schriftelijk bevestigd aan Opdrachtgever.
eis -49	Er zullen bij de leverancier geen camerabeelden opgeslagen worden. Ook niet in een

	cloudomgeving.
eis -50	<p>De leverancier zal logging toepassen, waarbij gebeurtenissen die belangrijk zijn voor de beveiliging of voor de analyse van verstoringen in een logbestand worden vastgelegd. Gebeurtenissen die hierbij worden vastgelegd zijn bijvoorbeeld het inloggen in een applicatie of op het systeem.</p> <p>Bij koppelingen (in- en uitgaand) biedt de applicatie een mechanisme dat datamutaties tijdens transport detecteert en logt.</p> <p>Van de logbestanden kunnen rapportages worden gemaakt.</p> <p>De minimale eisen die wij stellen aan de logbestanden zijn:</p> <ul style="list-style-type: none"> - Ze moeten leesbaar zijn; - Ze zijn voorzien van een timestamp; - Ze zijn herleidbaar tot een natuurlijke persoon of indien van toepassing tot een proces en/of handeling; - Ze mogen niet muteerbaar zijn; - Ze mogen de performance van het systeem niet belemmeren. <p>De minimale eisen die wij stellen aan de rapportages zijn:</p> <ul style="list-style-type: none"> - Per omgeving aparte vermelding over de soort logs, incidenten en risico's; - Over bewaartermijnen logbestanden per soort.
eis -51	<p>Met betrekking tot het melden van informatiebeveiligingsincidenten geldt: De leverancier heeft aantoonbaar een incidentmanagementproces voor informatiebeveiliging ingericht. De gemeente Amsterdam wordt d.m.v. incidentrapportages periodiek op de hoogte gehouden, bij kwetsbare incidenten (hoog/midden) is dat per direct. Dit proces is eveneens een borgingaspect van de verwerkersovereenkomst</p>
eis -52	<p>In het te beheren VMS dient Leverancier rollen en rechten te scheiden voor beheer, gebruik en rapportages. Er worden altijd unieke personen geauthentiseerd en geen rollen, dit om uitgevoerde activiteiten tot een uniek persoon te herleiden. Er zijn verschillende gebruikersrollen en per rol wordt bepaald welke functionaliteit aan de rol gekoppeld is.</p> <p>Leverancier heeft hierbij de volgende taken en verplichtingen:</p> <ul style="list-style-type: none"> • Het voorkomen van ongeautoriseerde toegang. • Inactieve accounts moeten automatisch of handmatig worden beëindigd. • Wachtwoorden moeten een beperkte levensduur hebben. Zie BIO voor eisen. • Accounts met een verhoogde rechten (beheerders) moeten bij remote access gebruikmaken van z.g. "multi factor authentication". • Alle gebruikers van applicaties of systemen moeten gebruikmaken van een uniek UserID en wachtwoord of andere identificerende authenticatie methodes om toegang te krijgen tot systemen om deze te beschermen tegen ongeautoriseerd gebruik • Het aanmaken/verwijderen van en verlenen/intrekken van autorisatie voor deze gebruikersaccounts mag alleen via het formeel vastgestelde proces en haar

	<p>subprocessen verlopen.</p> <ul style="list-style-type: none"> • Zodra het vertrouwelijke karakter van het wachtwoord betwijfeld wordt moet de eigenaar van het bijbehorende account het wachtwoord onmiddellijk wijzigen of moet het account disabled worden. • Speciale bevoegdheden moeten worden beperkt en beheerst. • Een beheerdersaccount wordt uitsluitend gebruikt door een functionaris in zijn rol als beheerder • Tweevoudige authenticatie (zoals bijvoorbeeld voor ontsluiting van zakelijke data via remote sessies en/of mobiele devices) dient ondersteund te worden.
eis -53	Bij beëindiging van het contract, stelt de Leverancier de gegevens weer beschikbaar aan de Contractpartner en werkt mee aan de migratie van de gegevens. De Leverancier draagt vervolgens verder zorg voor de vernietiging van de gegevens (in test-, acceptatie en productieomgeving en op de back-ups). Leverancier tekent het Procesverbaal van Vernietiging van de Contractpartner en voert de afspraken hieruit uit.
eis -54	Bij afvoer van (apparatuur met) datadragers zal Leverancier toezien op vernietiging van alle datadragers. Vernietiging van de datadragers wordt schriftelijk bevestigd aan Contractpartner.
eis -55	Gevoelige (vertrouwelijke) gegevens worden beschermd door gebruik te maken van cryptografische technieken in de database, bestanden en/of communicatie.
eis -56	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.

1.5 Eisen aan personeel en organisatie

eis -57	Leverancier garandeert dat de door haar ingezette medewerkers die vaardigheden en eigenschappen bezitten die nodig zijn voor de adequate uitvoering van de dienstverlening of werkzaamheden.
eis -58	De bij de uitvoering van de opdracht betrokken medewerk(st)ers dienen de Nederlandse taal te beheersen in woord en geschrift.
eis -59	<p>Voor de inzet van Personeel van Leverancier geldt dat bij de start de VOG niet ouder mag zijn dan drie maanden.</p> <p>Voor het verlopen van de geldigheidsduur (2 jaar) van de VOG dient deze door Leverancier opnieuw te worden aangevraagd, ten minste drie maanden voor einddatum.</p>
eis -60	Leverancier en zijn personeel zal strikte geheimhouding in acht nemen met betrekking tot de gebouwen, de middelen, de voertuigen, de interne organisatie van de politie, de identiteit van zijn medewerkers, Ingeslotenen en alle overige informatie waarvan het personeel van de Leverancier weet of redelijkerwijs kan vermoeden dat deze vertrouwelijk is. Deze geheimhoudingsplicht blijft ook na het einde van de overeenkomst van kracht. Leverancier zal in geen enkel geval melding doen van zijn werkzaamheden.
eis -61	<p>De Contractpartner houdt zich, in het kader van de wet BIBOB uitdrukkelijk het recht voor het bedrijf van Leverancier en eventuele onderaannemers door te lichten.</p> <p>Leverancier blijft jegens Opdrachtgever volledig verantwoordelijk en aansprakelijk voor de nakoming van alle eisen door deze derden. Opdrachtgever is gerechtigd om, voor zover dit redelijkerwijs noodzakelijk is voor de controle op de naleving van deze eis, inzage te verlangen in de relevante delen van de afspraken tussen Leverancier en de door hem ingeschakelde derden.</p>

1.6 Spare-parts

eis -62	Leverancier neemt het beheer van de voorraad spare-parts over. Bij overdracht zal de laatste stand worden opgemaakt. Dit zal ook als beginstand van het nieuwe contract dienen qua spare-voorraad.
eis -63	Leverancier is gedurende de looptijd van het contract er voor verantwoordelijk dat de spare-partvoorraad voldoende is uitgerust om aan alle contractuele verplichtingen te voldoen.
eis -64	Indien door veranderingen aan het Cameratoezichtstelsel, bijv. operationele inzet of de levering van een nieuw type product, het noodzakelijk is de spare-partvoorraad aan te passen zal Leverancier hiertoe tijdig een voorstel bij Opdrachtgever indienen. Minimaal elk kwartaal zal de Leverancier met een voorstel komen. Indien geen aanpassing nodig is dan zal dit ook expliciet worden vermeld.
eis -65	Er zijn aparte voorraden voor Gemeente Amsterdam en voor de politie (wellicht gedurende looptijd contract ook voor gemeente Amstelveen en eventuele andere gemeentes). Leverancier dient deze strikt gescheiden te houden. Gebruik van elkaars spare-voorraad is alleen mogelijk na expliciete toestemming van de eigenaar.
eis -66	Er dient altijd een actueel digitaal overzicht van de spare-voorraden te zijn. Wijzigingen in de sparevoorraad zijn altijd te herleiden via de volgende gegevens. <ul style="list-style-type: none"> • Bij afname: locatie / project / ticketnummer en datum. • Bij toename: waar onderdelen vandaan komen (locatie / project / bestelling) en datum. • Tevens dient de datum van de laatste fysieke telling bekend te zijn.
eis -67	Elk kwartaal dient de spare-voorraad opnieuw ter plekke geteld te worden en vergeleken te worden met het actuele bestand. Verschillen in aantallen (digitale lijst en fysieke telling), zullen door de Leverancier binnen 1 week worden opgelost en indien geen acceptabele verklaring kan worden gegeven dan zullen in het geval van ontbreken van onderdelen, deze kosteloos door de Leverancier worden aangevuld.
eis -68	Harde schijven worden adequaat gelabeld met het moment van levering. Op deze manier is het mogelijk te controleren of er nog garantie op een harde schijf geldt bij vervanging.
eis -69	Gedurende de looptijd van het contract zorgt de Leverancier er voor dat de voorraad tijdig wordt aangevuld. Indien het producten betreft die door Leverancier zijn geleverd en nog binnen de garantie vallen zijn kosten voor Leverancier. In andere gevallen zijn de kosten voor Opdrachtgever.
eis -70	Naast reguliere sparevoorraad heeft op dit moment één van de opdrachtgevers (de gemeente Amsterdam) ook een strategische sparevoorraad. Denk hierbij bijvoorbeeld aan masten, camera's, stroompaaltjes, zenders, accupacks, ... Eigenlijk alle zaken om een nieuw project zo snel mogelijk operationeel te hebben. De voorraad hiervan zal bij de leverancier liggen en in beheer zijn. Leverancier zorgt dat bij afname deze tijdig weer wordt aangevuld. Andere opdrachtgevers kunnen hiertoe ook besluiten, om een strategische voorraad aan te

	houden bij de leverancier.
--	----------------------------

1.7 Eigen mobiele systemen

Een aantal opdrachtgevers hebben enkele mobiele systemen in eigendom. Deze mobiele systemen hebben een tweeledig doel:

- In een gebied snel mee te kunnen bewegen indien nodig met de overlast. Het mobiele cameratoezicht dient vooral ter ondersteuning van politieacties tegen drugsoverlast en -criminaliteit. Het gaat om mobiele camera's die aanvullend aan het bestaande cameratoezicht worden ingezet op plekken waar de (kans op) (drugs)overlast het grootst is.;
- Het snel operationeel kunnen zijn met een (nieuw) project i.v.m. spoed. Waarbij er een geschikte mast in het gebied moet zijn en een stroompunt (bijvoorbeeld OV-verlichting) waarvan de mobiele camera zijn stroom vandaan kan halen. In geval van OV-verlichting, zullen de accu's worden opgeladen op het moment dat de verlichting aan is en op de momenten dat de verlichting uit is, zal de mobiele camera autonoom draaien.

Dit betreffen twee verschillende mobiele systemen:

- Zonder mast, die aan een bestaande (stevige) mast vast gemaakt kan worden (MSP);
- Met mast (MSU).

eis -71	De hierboven beschreven eigen mobiele camera's worden ondergebracht bij regulier cameratoezicht. De Leverancier zal verantwoordelijk zijn voor het beheer, opslag indien niet gebruikt aan een druppellader of vergelijkbaar, onderhoud en (ver)plaatsing van deze systemen.
eis -72	Leverancier is, op verzoek van een Opdrachtgever in staat om binnen 48 uur (twee werkdagen) een mobiel systeem te (ver)plaatsen op/naar een gewenste locatie.
eis -73	Leverancier kan in principe gebruik maken van bestaande lichtmasten voor de stroomvoorziening. Hierbij dient deze er rekening mee te houden dat deze geschakeld zijn en daardoor niet permanent onder spanning staan. Leverancier is verantwoordelijk voor afstemming met het onderdeel die gaat over de openbare verlichting – OVL en dient de eisen hiervoor te respecteren.
eis -74	Leverancier beschikt over voldoende gediplomeerd personeel om een mobiele camera met tijdelijke stroomvoorziening conform alle geldende normen aan te sluiten. Bij aansluiting van een accu op een lichtmast geldt deze eis nadrukkelijk ook.

2 Overdracht en overname

eis -75	Vanaf de overdracht is Leverancier volledig verantwoordelijk voor de correcte werking, instandhouding, beheer en onderhoud en alle aanpassingen aan het Cameratoezichtstelsel.
eis -76	Alle functionaliteit die bij overname beschikbaar is dient volledig werkend te blijven, tenzij door overeengekomen aanpassingen aan het stelsel gedurende de looptijd van het contract.
eis -77	Ten behoeve van de overdracht zal de Leverancier één centrale contactpersoon aanwijzen.
eis -78	Leverancier dient in de Overdrachtsperiode het Cameratoezichtstelsel incl. de as-built en andere documentatie te controleren op juistheid en correcte implementatie. Fouten, Gebreken, onvolledigheden of onvolkomenheden aangetroffen na de ingangsdatum van het contract dienen door de Leverancier op eigen kosten gecorrigeerd te worden.
eis -79	Leverancier zal het beheer van de lopende onderhoudscontracten overnemen.

3 Videomanagementsysteem

eis -80	Leverancier neemt het bestaande VMS Genetec Security Center over incl. al het bijbehorende onderhoud, en tijdige updates en upgrades.
eis -81	Gedurende de looptijd van het contract zal Leverancier tijdig updates en upgrades doorvoeren en hierbij rekening houden met de versie van de federation partners zodat een koppeling mogelijk blijft. Kosten hiervoor zijn onderdeel van het aangeboden beheer en onderhoud. Bij Security Center is sprake van een upgrade als het major of minor versienummer wijzigt. Updates betreffen Service Releases (SR), CU's, en hotfixes.
eis -82	Leverancier adviseert Contractpartner in uit te voeren updates en upgrades. Het doel is het vinden van een balans in enerzijds het snel beschikking te krijgen over nieuwe relevante functionaliteit en anderzijds alleen te updaten of upgraden nadat is gebleken dat updates en/of upgrades stabiel zijn gebleken, waarbij federation koppelingen niet gestoord mogen worden.
eis -83	Leverancier zal alle door Contractpartner aan te schaffen uitbreidingen, plug-ins, en dergelijke, die voor het VMS-platform beschikbaar zijn installeren en de installatie en onderhoud hiervan faciliteren. Het betreft hierbij ook uitbreidingen van partijen anders dan Genetec.
eis -84	Gedurende de looptijd van het contract dient ten minste elk half jaar het kaartmateriaal te worden geüpdatet.
eis -85	Leverancier zal alle koppelingen van het VMS met systemen van derden onderhouden. Het gaat hierbij o.a. om Federation-koppelingen met ProRail, het Arena-gebied en de Verkeerscentrale, en een koppeling via een analoog scheidingsvlak met GVB. Voor koppelingen tussen een applicatie en gemeentelijke systemen, Richting: van de Applicatie naar een gemeentelijk systeem / van een gemeentelijk systeem naar een Applicatie, Batch/Realtime: Batch/Scheduled en/of Realtime, Transport/Bestandsformaat: Data uitwisseling via REST / SOAP / POX / CMIS over HTTPS of bestandsuitwisseling via SFTP, FTPS of HTTPS. XLSx, JSON, CSV, XML, Beveiliging: Gebruikersnaam + wachtwoord + Certificaat, Gebruikersnaam + wachtwoord, SAML 2.0 / 2-Way SSL Voor koppelingen, integratie, imports en export vindt data uitwisseling plaats via bestanden en protocollen die voorkomen in de lijst van open standaarden (https://www.forumstandaardisatie.nl/open-standaarden).
eis -86	Het VMS registreert in logbestanden minimaal gedurende 12 maanden informatie die betrekking hebben op: <ul style="list-style-type: none"> • User-login gegevens van VMS-stations en servers • Configuratie wijzigingen • Software-updates • Alarmevents • Foutmeldingen • Bedieningsactiviteiten
eis -87	Voor een beperkte groep medewerkers van Contractpartner zal Leverancier accounts aan maken (of in standhouden) met administrator-rechten op de VMS-applicatie en de aangesloten Camera's. Leverancier mag hierbij uitgaan van als functioneel beheerder opgeleide medewerkers die het Cameratoezichtstelsel niet in gevaar zullen brengen. Indien acties van deze medewerkers

Gemeente Amsterdam

	aantoonbaar leiden tot storingen in het Cameratoezichtstelsel dan zijn de kosten voor herstel voor Contractpartner. De tijd voor onbeschikbaarheid die uit deze acties volgt zal Leverancier niet toe worden gerekend.
eis -88	Bij uitval van een willekeurige fysieke of virtuele server treedt een fail-over mechanisme in werking waardoor de functionaliteit binnen één minuut weer beschikbaar is. In het geval van een opslag-server betekent dit dat beelden op de failover-server worden opgenomen. Er wordt niet geëist dat de opslag van de oude server direct beschikbaar is. Wel dient bij herstel van de oorspronkelijke functionaliteit geen beelddata verloren te gaan. De Genetec mobile-server en Plan Manager zijn uitgesloten van de fail-over functionaliteit.
eis -89	Opdrachtgever heeft de sterke wens om voor de Camerastreams end-to-end versleuteling toe te passen. Het betreft hier versleuteling voor het gehele traject van camera naar client/opslag.

4 Werkplekken en servers

4.1 Algemene eisen clients en servers

eis -90	Servers en clients en al haar componenten zijn geschikt voor volcontinu gebruik en hoge prestaties. Dit betekent dat gekozen dient te worden voor professionele productlijnen en niet voor consumentenproducten
eis -91	De clients en servers moeten gebruik kunnen maken van elkaars spare-parts. De behuizing is daarbij ook van voldoende grootte om dit mogelijk te maken.
eis -92	De clients (mits geplaatst in 19"-rack) en servers zijn uitgerust met een dubbele voeding zodat één stroomvoorziening of voeding uit kan vallen zonder enig effect op het functioneren. De status van de voedingen zal gemonitord worden (via SNMP).
eis -93	De Leverancier voorziet in minimaal de door Genetec geadviseerde hardware (met overeenkomstige belasting) zoals grafische kaarten, processor en geheugen. In het geval van grafische kaarten dient gekozen te worden voor de professionele lijn van de aanbevolen hardware.
eis -94	Het operating systeem van een client of server dient geïnstalleerd te zijn op een opslagmedium van type SSD van ten minste 1 TB. Deze wordt ook gebruikt voor de bijbehorende applicatiesoftware.
eis -95	Servers zijn specifiek geschikt voor montage in een 19"-rack.
eis -96	Clients zijn geschikt voor montage in een 19"-rack als deze hierin worden geplaatst. Indien clients in een kantoorruimte worden geplaatst kan er gekozen worden voor een tower-model (indien geen rack beschikbaar is) met speciale aandacht voor stille werking. Levering en installatie van de extenders voor schermen en USB is onderdeel van de opdracht. Daar waar plaatsing in een technische ruimte niet mogelijk is zal gebruik worden gemaakt van ruime tower-modellen.
eis -97	Een te leveren server maakt gebruik van het nieuwste 64-bits Windows Server operating systeem dat wordt ondersteund door de applicatie(s) waar deze voor bedoeld is.
eis -98	Clients maken gebruik van het nieuwste 64-bits Windows Professional (Nederlandstalig) operating systeem dat wordt ondersteund door de applicatie(s) waar deze voor bedoeld is..
eis -99	Geheugen in clients en servers is minimaal 16GB en van type DDR4 2400 of beter.
eis -100	Clients zijn uitgerust met ten minste twee USB-poorten versie 3.0 of beter.
eis -101	Er is een expliciete scheiding tussen de apparatuur van de verschillende opdrachtgevers.

4.2 Uitkijkplek

eis -102	<p>De uitkijkplek bevat de volgende onderdelen die hieronder nader worden gespecificeerd:</p> <ul style="list-style-type: none"> • Werkstation voor de werkplek van de uitkijker. • Werkstation voor de videowall. • Een videowall bestaat uit 2x 50/55"-schermen en beugels voor bevestiging. • Extenders over multimode-glas (OM3) voor zowel de schermen van de videowall, drie schermen op de uitkijktafel, één meekijkmonitor voor de supervisor en senior observant, USB-extender voor de randapparatuur voor de uitkijkplek.
----------	---

	<ul style="list-style-type: none"> • Eén Bedieningsconsole gelijkwaardig aan of beter dan de Axis keyboard T8311 en T8312 voor PTZ-besturing, macrobediening en het opschakelen van camera's. • Alle benodigde patchkabels. <p>Alle uitkijktafels zijn in hoogte verstelbaar tot stahoogte. Hierdoor zijn extra lange kabels (ca. 5m) voor muis/toetsenbord/joystick en monitors noodzakelijk. Apparatuur als mediaconverters kunnen in het technisch compartiment van de uitkijktafel worden gebracht.</p>
eis -103	<p>De communicatie tussen beeldschermen, keyboard, muis en PTZ-controllers in de uitkijkrimte van de CCTR dient door middel van zgn. extenders gerealiseerd te worden. Hiervoor gelden de volgende eisen:</p> <ul style="list-style-type: none"> • De Inschrijver biedt extenders geschikt voor multimode-glasvezelbekabeling o.b.v. type OM3. • Per monitorsignaal dient een aparte extender te worden gebruikt. De extender is in staat een 4K signaal (3840x2160) zonder kwaliteitsverlies over ten minste 75 meter te transporteren over één enkele vezel (dus geen vezelpaar). • De extender dient zelf de Extended Display Identification Data te detecteren en de resolutie hieraan aan te passen. • Het USB-signaal (voor muis, toetsenbord én PTZ-controller) 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 vezels.
eis -104	<p>Het client-werkstation van de uitkijplek wordt met name gebruikt voor gebruik van incident-registratie o.b.v. Coppweb op dit ogenblik. Coppweb voorziet in het bepalen van de inhoud van de bijbehorende videowall, registratie van incidenten, een spotmonitor voor besturing van een Camera, en het doorschakelen van beelden naar andere werkstations, zoals de GMK.</p> <p>Het client-werkstation van de uitkijplek zelf voldoet aan de volgende minimum eisen in aanvulling op eis -90 tot en met eis -99:</p> <ul style="list-style-type: none"> • Het werkstation is in staat gelijktijdig minimaal 8x Full HD-streams (H.265, 3 Mbps) zonder haperingen te tonen. • Ten minste vier digitale video-uitgangen met ten minste 4K schermresolutie.
eis -105	<p>Het client-werkstation van de videowall voldoet aan de volgende minimum eisen in aanvulling op eis -90 tot en met eis -99:</p> <ul style="list-style-type: none"> • De videowall is in staat gelijktijdig minimaal 18 Full HD-streams (H.265, 3 Mbps) zonder haperingen te tonen. • Ondersteuning van vier schermen met ten minste 4K schermresolutie (digitale input).
eis -106	<p>De monitors van de videowall voldoen aan de volgende eisen:</p> <ul style="list-style-type: none"> • De monitors en zijn componenten dienen geschikt te zijn voor 24/7 gebruik. • Ten minste 2x DVI-D of eenvoudig converteerbare digitale video-input. • De resolutie dient 3840x2160 pixels (4k) of beter te bedragen met een beeldverhouding 16:9 • De instellingen van de monitors dienen bij oplevering geoptimaliseerd te zijn voor de beste ergonomische omstandigheden. • De beelddiagonaal dient ten minste 50" te bedragen.

	<ul style="list-style-type: none"> • VESA-bevestiging (het betreft hierbij niet de beugel voor bevestiging op de wand of het bureau) • Anti-reflectielaag op het scherm die reflecties van verlichting in de uitkijkcentrale elimineert. Het is niet toegestaan zelf een coating aan te brengen omdat hierdoor de helderheid zal afnemen. • De typische helderheid dient minimaal 450 cd/m² te bedragen. • Energiezuinig en EnergyStar 8 (of hoger) gecertificeerd. • Maximaal stroomverbruik van 200 Watt. • Contrast-ratio 4.000:1 of beter. • Pixel-responsetijd: max. 8 msec • Kijkhoek horizontaal en verticaal: > 170 graden. • Schermrand van maximaal 8 mm dikte (zijkant).
eis -107	<p>Aan de monitors op de uitkijktafel zelf worden de volgende eisen gesteld:</p> <ul style="list-style-type: none"> • De monitors en zijn componenten dienen geschikt te zijn voor 24/7 gebruik. • DVI-D of eenvoudig converteerbare digitale video-input. • De resolutie dient 3840x2160 pixels (4k) of beter te bedragen met een beeldverhouding 16:9 • De instellingen van de monitors dienen bij oplevering geoptimaliseerd te zijn voor de beste ergonomische omstandigheden. • De beelddiagonaal dient 24" of 35" te bedragen. • VESA-bevestiging (het betreft hierbij niet de beugel voor bevestiging op de wand of het bureau). • Anti-reflectielaag op het scherm die reflecties van verlichting in de uitkijkcentrale elimineert. Het is niet toegestaan zelf een coating aan te brengen. • De typische helderheid dient minimaal 250 cd/m² te bedragen. • Energiezuinig en EnergyStar gecertificeerd. • Maximaal stroomverbruik van 30 Watt. • Contrast-ratio 1.000:1 of beter. • Pixel-responsetijd: max. 8 msec • Kijkhoek horizontaal en verticaal: > 170 graden. • Schermrand van maximaal 9 mm dikte.

4.3 Servers

eis -108	Een server inclusief opslag is geschikt voor de hoge continue belasting die opslag van alle camerabeelden en afspelen van streaming video in hoge kwaliteit stelt.
eis -109	Een server voor opslag van beelden moet fout-tolerant zijn en gebruikmaken van een redundante opslag gelijk aan of beter dan RAID6 zodat per server er ten minste twee harddisks gelijktijdig uit kunnen vallen zonder verlies van data of prestaties.
eis -110	Een fysieke server moet zijn uitgerust met een dubbele voeding en een dubbele netwerkkaart t.b.v. redundantie.
eis -111	Harddisks moeten hot-swappable zijn en geschikt voor het specifieke gebruik van cameratoezicht (d.w.z. een continue datastroom die moet worden weggeschreven).

5 Camera's

5.1 Algemene eisen

De eisen in deze paragraaf gelden voor alle te leveren Camera's gedurende de looptijd van het contract.

eis -112	Onderdeel van een Camera is het bevestigingsmateriaal voor plafond-, hoek-, wand-, gevel-of mastmontage. Een uithouder valt hier niet onder.
eis -113	Alle configuratie-instellingen van de Camera's zijn op afstand in te stellen via een versleutelde verbinding zoals HTTPS. TLS 1.2 of hoger.
eis -114	De camera moet geschikt zijn voor gebruik in alle Nederlandse buitenomstandigheden en de doelstelling om goed toezicht mogelijk te maken in de openbare ruimte.
eis -115	De Camera is digitaal. De Camerastreams zijn van type H.264 of H.265 of beter. De Camera is in staat om gelijktijdig minimaal twee vrij configureerbare streams uitsturen.
eis -116	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.
eis -117	De Camera ondersteunt een beeldfrequentie van zowel 25 als 30 fps.
eis -118	De Camera is uitgerust met automatische witbalans, auto-iris.
eis -119	De Camera is voorzien van een username en password. Standaard- of fabriekswachtwoorden worden direct na installatie aangepast.
eis -120	De Camera ondersteunt TCP, UDP, HTTPS, laatste versie SNMP (v3 bij start contract), ICMP, IEEE 802.1x, QoS, IPv4, IPv6 en multicast (IGMP).
eis -121	De behuizing is neutraal wit of crèmekleurig. Het is mogelijk een Camera te leveren in een RAL-kleur tegen meerprijs.
eis -122	De Camera ondersteunt ONVIF Profile S / T.
eis -123	Na spanningstuitval zal de Camera automatisch herstarten met behoud van de gehele configuratie en binnen twee minuten weer werkend zijn.
eis -124	De Camera is van type dome of 360 graden (of combinatie hiervan). De koepel van de Camera mag geen zichtbare vervorming/verstoring in het beeld introduceren.
eis -125	De Camera wordt zonder voorbehoud ondersteund door Genetec Security Center v5.13 of hoger via een directe (native) integratie.
eis -126	De camera wordt via haar eigen interface / SDK (d.w.z. niet via ONVIF) expliciet zonder voorbehoud of aanvullende voorwaarden ondersteund door Genetec Security Center v5.13 of hoger." verifieerbaar via de website van Genetec. Opmerking: Als onderdeel van de uitvraag dient de inschrijver te specificeren welk type camera aangeboden wordt zodat een controle voor gunning mogelijk is.
eis -127	De Camera dient vanuit Genetec Security Center 5.13 of hoger van een nieuwe firmware te kunnen worden voorzien.
eis -128	De Camera dient vanuit Genetec Security Center 5.13 of hoger van een nieuw wachtwoord op het door Genetec gebruikte account te kunnen worden voorzien.

eis -129	De snelheid van pan en tilt is minimaal 150 graden per seconde.
eis -130	De camera ondersteunt H.265 codering of beter/nieuwer.
eis -131	De Camera zal geen reflecties van de lens in de dome of het venster tonen die hierdoor een goed uitkijkbeeld verstoren.
eis -132	De sensor bij een Camera dient ten minste 1/3 inch en progressive scan te zijn.

5.2 Beveiligingseisen aan camera's

eis -133	De Camera ondersteunt end-to-end versleuteling in combinatie met Genetec Security Center.
eis -134	De camera vereist geen onveilige protocollen (bijv. telnet of ftp) voor beheer en onderhoud.
eis -135	De camera ondersteunt het IEEE 802.1x toegangsprotocol o.b.v. certificaten. En/of: 802.1AE (MACsec)
eis -136	De camera kan filteren op de netwerkadressen waarmee gecommuniceerd mag worden.
eis -137	De camera kan omgaan met versleutelde wachtwoorden en communicatie kan via HTTPS worden versleuteld. Het gebruik van HTTPS kan worden afgedwongen.
eis -138	De camera dwingt af dat er alleen gecertificeerde firmware kan worden geïnstalleerd.

5.3 Eisen bestuurbare dome-camera (PTZ-Domecamera)

De PTZ-Domecamera zal veruit het meest ingezette model zijn.

eis -139	De te leveren Camera is specifiek geschikt voor omstandigheden met zeer weinig licht. Het betreft hier het model van de producent dat het meest geschikt is voor toepassing in donkere omstandigheden (ook zonder gebruik van eventuele ingebouwde infrarood verlichting). Bijvoorbeeld Axis Lightfinder of IQSIGHT (Bosch) Starlight technologie.
eis -140	De camera betreft een bestuurbare camera met ten minste 30x zoom van type dome zodat niet triviaal zichtbaar is te zien hoe de camera is gericht. De Camera dient bij 3 Mbps (H.265) soepel te sturen zodat het volgen van een persoon dicht bij de Camera geen probleem oplevert.
eis -141	Politie-striping op de rand van de (PTZ-dome) Camera is onderdeel van de levering.
eis -142	De Camera voldoet aan de volgende subeisen: <ul style="list-style-type: none"> • De Camera is geschikt voor alle Nederlandse weersomstandigheden. • De Camera is geschikt voor een omgevingstemperatuur van -20 tot 50 graden Celsius. • De resolutie van de Camerastream is minimaal Full-HD. • De Camera is minimaal genormeerd op IP66 en IK10. • De Camera beschikt over auto-focus.
eis -143	Het is mogelijk de PTZ-domecamera te leveren met een standaarduithouder of eentje van 0.5, 1.0 en 1.5 meter lengte. Langer eventueel via maatwerk.
eis -144	De Camera beschikt over ten minste 24 instelbare privacy masks die hun positie behouden bij PTZ-sturing. Privacymasking mag niet meer dan 0.1 sec. 'na-ijlen' bij door besturing veranderende camerabeelden.
eis -145	Installatie van een Camera is incl. configuratie van privacy-maskering en presets. Het moet niet mogelijk zijn om in woningen te kijken vanaf de 1 ^e verdieping of hoger. Privacy masks dienen pas te verschijnen bij een redelijk zoomniveau zodat deze niet continu zichtbaar zijn in een min of meer

	uitgezoomde staat.
eis -146	<p>Minimale PTZ.dome eigenschappen:</p> <ul style="list-style-type: none"> • Digitale zoom is uitschakelbaar. • Pan snelheid: Variabel 0.1 – 300 °/s. • Tilt snelheid: Variabel 0.1 – 100 °/s. • De snelheid kan automatisch aan worden gepast aan de zoom-factor. • Pan bereik 360 graden continu. • Tilt bereik minimaal -90 tot +90 graden bij volledige zoom. • Aantal presets >30
eis -147	Het is mogelijk een standaard positie (default preset) te definiëren zodat de Camera na een stuuractie automatisch en na een instelbare tijd terugkeert naar deze standaard positie.
eis -148	De Camera is in staat haar PTZ-instellingen te communiceren zodat het mogelijk is om op de werkplek van de gebruiker te tonen in welke richting en met welk zoomniveau de Camera waarneemt.
eis -149	De Camera zal naast voor gedefinieerde presets ook bestuurd kunnen worden via absolute PTZ-coördinaten. Hierbij moet worden gedacht aan externe software die naar aanleiding van een incident een Camera via het VMS naar een willekeurige positie kan sturen.
eis -150	De Camera moet kunnen worden geleverd met ingebouwde glaskoppeling d.w.z. het is mogelijk de Camera direct op glasvezel af te monteren zonder dat een separate junctionbox nodig is.
eis -151	De Camera behoudt de positionering van de privacy masks 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 privacy masks verplaatsen telt dit als een storing en onbeschikbaarheid van de Camera. De Leverancier dient vervolgens de privacy masks en presets in de oude staat te herstellen. Onbeschikbaarheid van een Camera door verlopen privacy masks tellen mee in de bepaling van een eventuele boete door onbeschikbaarheid.

5.4 Vernieuwing

Contractpartner verwacht van Leverancier een instelling waarbij altijd gezamenlijk wordt gekeken hoe het cameratoezicht is te verbeteren, o.a. door experimenten in praktijksituaties, waarbij beide partijen hierin investeren.

eis -152	Leverancier zal gedurende de contractperiode experimenten met nieuwe cameratechnologie faciliteren. Leverancier stelt hiertoe gedurende minimaal twee maanden gratis een proefcamera beschikbaar die op een reeds ingerichte proeflocatie (mast, 230V, en netwerk beschikbaar) dient te worden opgehangen. Kosten voor plaatsing en verwijdering kunnen conform afgesproken tarieven in rekening worden gebracht. Andere kosten kunnen niet in rekening worden gebracht.
----------	--

6 Draadloze verbindingen

6.1 Algemene eisen

eis -153	Alle te leveren apparatuur dient te voldoen aan alle toepasselijke regelgeving van de Rijksinspectie Digital Infrastructuur met betrekking tot het gebruik van licentievrije dan wel gelicenseerde frequentiebanden
eis -154	Wireless apparatuur dient, tenzij anders vermeld in dit document minimaal te beschikken over encryptie van type AES 256-bits of gelijkwaardig/beter. Alle wireless verbindingen dienen voor oplevering adequaat beveiligd te zijn met een wachtwoord dat niet eenvoudig herleidbaar is of te raden door derden.
eis -155	De bescherming van de draadloze apparatuur tegen vocht en stof is IP66 of beter.
eis -156	Onderdeel van een zender is de antenne en bevestigingsbeugels voor mast/statief- dan wel wandmontage.
eis -157	De draadloze apparatuur moet op afstand beheerd kunnen worden en ondersteunt monitoring via Laatste versie SNMP (v3 bij start contract).
eis -158	Technologie biedt minimaal ondersteuning aan VLAN's (IEEE802.1q) en prioritering (IEEE 802.1p). De draadloze apparatuur ondersteunt het gebruik van 1000 VLANs.
eis -159	Er wordt geen gebruik gemaakt van het WiFi-protocol (IEEE 802.11).
eis -160	Een zender moeten voldoende capaciteit hebben onder alle omstandigheden voor de uitgezonden camerastreams en besturing. De beelden van de aangesloten Camera's moeten vloeiend getoond kunnen worden in een constante framerate van 25 fps, Full-HD resolutie en bij 5 Mbps gemiddeld. Doorkomst van een zgn. I-frame zal niet tot haperingen in de videostroom leiden.
eis -161	Alle draadloze apparatuur moet beheerd kunnen worden via een webinterface.
eis -162	Alle draadloze apparatuur moet gevoed kunnen worden via PoE.
eis -163	Leverancier is verantwoordelijk voor het opstellen van vergunningsaanvragen bij de Rijksinspectie Digital Infrastructuur voor zowel PtP-verbindingen als PtMP-verbindingen. De vergunning wordt aangevraagd op naam van de opdrachtgever. Kosten van de Rijksinspectie Digital Infrastructuur, zowel aanvraag als onderhoud, is voor rekening van de Contractpartner en dient direct aan Contractpartner te worden gefactureerd door de Rijksinspectie Digital Infrastructuur. Indien Leverancier om praktische redenen een licentie heeft bij de Rijksinspectie Digital Infrastructuur dienen de kosten aan Contractpartner te worden gefactureerd met een opslagpercentage conform eis -10.
eis -164	Leverancier is verantwoordelijk voor de draadloze verbindingen van diverse camera's van het onderdeel Verkeer & Openbare Ruimte die via het draadloze netwerk van de CCTR ontsloten worden. Leverancier is nadrukkelijk niet verantwoordelijk voor de camera's zelf. Kosten hiervoor worden verrekend o.b.v. reguliere eenheidsprijzen.

6.2 Licentievrij 5GHz

eis -165	In de licentievrije 5GHz-band worden in principe alleen punt-puntverbindingen ingezet. De apparatuur wordt ingezet tot een bandbreedte van max. 50 Mbps en een maximale afstand van 250 meter. Bij hogere bandbreedtes of grotere afstanden dient een verbinding in een gelicenseerde frequentieband of de 60 GHz frequentieband te worden gebruikt.
----------	--

eis -166	Technologie voor licentievrije frequenties dient gebaseerd te zijn op OFDM en MIMO modulatietechniek, werkende in de 5 GHz band.
eis -167	De zenders zijn leverbaar met effectieve (netto) capaciteiten van minimaal 10 tot 50 Mbps (aggregated).
eis -168	De latency per zender bedraagt max. 4 msec.
eis -169	De capaciteit van zenders moet eenvoudig op afstand vergroot kunnen worden met een software-upgrade.
eis -170	De zenders zijn leverbaar met een antenne van ten minste 22 dBi. Het formaat van de antenne mag hierbij niet groter zijn dan 300x300mm.

6.3 Licentievrij 60GHz

Deze paragraaf beschrijft de eisen aan de point-to-point-technologie die in de 60 GHz-band moet worden ingezet.

eis -171	Deze band wordt gebruikt voor het ontsluiten van één of meerdere camera's in die gebieden waar verstoring in de 5GHz-band reëel is. Apparatuur wordt echter ingezet om een maximale afstand van ca. 900m te overbruggen.
eis -172	Apparatuur dient een bereik te hebben van 57 – 64 GHz.
eis -173	De apparatuur ondersteunt versleuteling van AES-256 of gelijkwaardig / beter.
eis -174	De apparatuur is in staat een analyse van het spectrum in de ondersteunde band uit te voeren.
eis -175	De apparatuur ondersteunt ETSI EN 302 217.
eis -176	De apparatuur ondersteunt het RADIUS-protocol
eis -177	De latency per zender bedraagt max. 4 msec.
eis -178	De zenders zijn leverbaar met een antenne van ten minste 35 dBi. Het formaat van de antenne mag hierbij niet groter zijn dan 200x200mm.

6.4 Point-to-point gelicenseerd

eis -179	Bij punt-puntverbindingen over een bereik van meer dan 1km of een capaciteit van 50 Mbps of meer, of bij het verbinden van een base-station met het eigen netwerk dient een gelicenseerde straalverbinding te worden ingezet.
eis -180	De zenders zijn leverbaar met een effectieve (netto) capaciteit tot ten minste 1 Gbps en een latency van max. 5 msec.
eis -181	De apparatuur voor deze verbinding ondersteunt versleuteling o.b.v. AES-256 of gelijkwaardig/beter.

7 Werken in de openbare ruimte, en in en op panden

7.1 Algemene eisen veiligheid en vergunningen

Voor een correcte uitvoering van de werkzaamheden in de openbare ruimte dient de Leverancier te voldoen aan een aantal eisen.

eis -182	Leverancier dient op de hoogte te zijn van de geldende regels, te verkrijgen bij de regelgevende instanties (bijv. vergunningenloketten van stadsdelen, centrale stad/WWU).
eis -183	Leverancier is zelf verantwoordelijk voor het uitvoeren van alle noodzakelijke verkeersmaatregelen zoals pijlwagens, bebording, verkeersregelaars, etc. Kosten zijn onderdeel van het standaard beheer en onderhoud en worden bij projecten als zelfstandige post geoffreerd.
eis -184	Leverancier is verantwoordelijk voor het aanvragen van alle noodzakelijke vergunningen om haar werkzaamheden uit te kunnen voeren.
eis -185	Leverancier dient, indien de tijdsdruk dit toelaat, in Amsterdam te werken volgens procedures vastgelegd in de WIOR. Zie ook https://www.amsterdam.nl/verkeer-vervoer/werken-in-de-openbare-ruimte-(wior)/
eis -186	De vergunningskosten voor eventuele jaarvergunningen en parkeerontheffingen kunnen niet separaat worden doorberekend en zijn onderdeel van de reguliere kosten voor realisatie.
eis -187	Leverancier is verplicht om te allen tijde een veilige werkomgeving te creëren voor de uitvoering van de werkzaamheden, voor de eigen medewerkers, omstanders als ook voor de overige weggebruikers conform gangbare richtlijnen en eventuele aanwijzingen van de gemeente. Indien nodig stelt Leverancier een V&G-plan op voorafgaand aan de uit te voeren werkzaamheden en dient zelf te weten in welke situaties dit nodig is.
eis -188	<p>Voor het werken in de openbare ruimte geldt het werken in basisregime op basis van de CROW-publicatie 400 "Werken in verontreinigde bodem" (https://www.crow.nl/publicaties/werken-in-en-met-verontreinigde-bodem).</p> <p>Voor het uitvoeren van het plaatsen van de mast c.q. het graven van de sleuf voor de kabels en leidingen dient Inschrijver een uitgespecificeerde meerprijs (zie ook Prijsinvalformulier) aan te geven voor het graven in:</p> <ul style="list-style-type: none"> - verontreinigingsklasse "oranje"; - verontreinigingsklasse 'rood'; - verontreinigingsklasse 'zwart'. <p>Inschrijver mag hierbij uitgaan van niet-vluchtige verontreinigingen. Indien dit wel het geval is dan is er sprake van meerwerk.</p> <p>De Opdrachtgever zal zorgdragen voor:</p> <ul style="list-style-type: none"> - Het aanleveren van de noodzakelijke onderzoeksgegevens of gegevens op basis van de bodemkwaliteitskaart. - Een eventueel benodigde BUS-melding, 10 m³-regeling of een saneringsplanprocedure in gang zetten op basis van de ontgravingstekening van de aannemer.

	<ul style="list-style-type: none"> - De voorlopige veiligheidsklasse laat vaststellen en laat verifiëren door een veiligheidskundige. - De aanvraag tot acceptatie van verontreinigde grond verricht bij de Grondbank Amsterdam of een andere verwerkingsinrichting. - De inzet van eventueel benodigde milieukundige begeleiding (BRL SIKB 6000). - Het indienen van de definitieve evaluatie op basis van de concept-evaluatie opgesteld door de aannemer.
eis -189	<p>Op diverse plekken (bijvoorbeeld: Alticom) zijn zenders geplaatst op grote hoogte en in sommige gevallen op plekken waarbij zonder voorzorgsmaatregelen niet veilig gewerkt kan worden. Leverancier beschikt over werknemers die beschikken over een klimcertificaat en daarmee aantoonbaar in staat zijn tot veilig werken op hoogte. Leverancier is verantwoordelijk voor de inzet van medewerkers die in staat zijn tot veilig werken op hoogte indien de werkzaamheden dit vereisen.</p>
eis -190	<p>Na verwijdering van nog bruikbaar straatmeubilair (masten, straatkasten, fagetpalen) van Gemeente Amsterdam dient dit materiaal robuust en weersbestendig gelabeld te worden met "Cameratoezicht OOV Gemeente Amsterdam" en naar de gemeentelijke opslag (Westpoort) te worden gebracht. Leverancier zorgt voor melding (brengen en ophalen) ten minste 1 werkdag vooraf. Kosten voor opslag zijn voor Opdrachtgever.</p> <p>Verwijderde en nog bruikbaar ander materiaal (camera's, junctionbox, switch en zenders) dienen naar de CCTR te worden gebracht.</p>
eis -191	<p>Bij het werken nabij een bovenleiding dient de Leverancier de veiligheidsvoorschriften van het GVB te volgen (gvb-zakelijk-veiligheidsvoorschriften-veilig-werken GVB).</p> <p>Kosten voor een eventuele afsluiting van de bovenleiding zijn voor Opdrachtgever. Opdrachtnemer zorgt voor de administratieve afhandeling.</p>
eis -192	<p>Contractpartner maakt gebruik van een groot aantal locaties van derden voor plaatsing van een zender. Leverancier dient zich te houden aan de afspraken voor toegangsverlening met deze locaties en de aanwijzingen van medewerkers/eigenaren/personen/... op te volgen.</p> <p>Leverancier zorgt zelfstandig voor contact en contactonderhoud met verantwoordelijke medewerkers/personen of deze locaties en zorgt dat de gegevens up-to-date zijn.</p>

7.2 230V voedingsaansluitingen

eis -193	<p>Leverancier realiseert voor elke nieuwe camerapositie of straatkast een stroomvoorziening o.b.v. een meterloos Liander-stroompunt. Leverancier is verantwoordelijk voor het registreren van de EAN-code in de as-built.</p>
eis -194	<p>Leverancier is in staat een kleine smalle straatkast (fagetpaal) te leveren voor afwerking van een onbemeterd stroompunt. Deze straatkast (fagetpaal) moet voldoen aan de eisen van de netbeheerder (bijvoorbeeld gecertificeerde objecten). Leverancier is verantwoordelijk om eventuele wijzigingen in de eisen te monitoren en hierop tijdig in te spelen.</p> <p>Een fagetpaal dient tegen de mast of ophangpunt van de Camera aan te staan, tenzij het niet anders kan. In dit geval zal de Leverancier eerst in overleg treden met Opdrachtgever en dit opnemen in het opleverrapport.</p>
eis -195	<p>Leverancier is verantwoordelijk voor het aanvragen van een dergelijk meterloos stroompunt. Aanvragen worden op naam gesteld van de Opdrachtgever en abonnements- en/of verbruikskosten worden betaald door de Opdrachtgever. Gedurende de looptijd van het onderhoud is Leverancier</p>

	<p>verantwoordelijk voor het management van storingen in de stroomvoorziening inclusief bestaande of overgenomen voorzieningen.</p> <p>De kosten van Liander zijn geen onderdeel van de vaste prijs (zie ook prijsinvulformulier). Kosten Liander worden waar mogelijk direct aan Opdrachtgever gefactureerd. Indien dit niet kan dienen de kosten aan Opdrachtgever te worden gefactureerd met een opslagpercentage conform eis -10.</p>
--	---

7.3 Tijdelijke stroomvoorzieningen

Regelmatig dient een nieuwe Camera of cameraproject gerealiseerd te worden onder tijdsdruk. In deze gevallen zal er geen tijd zijn om realisatie van een Liander-stroompunt af te wachten. In de meeste gevallen is er in de nabijheid van de positie een lichtmast aanwezig waaruit tijdelijk stroom kan worden betrokken. Let op: vrijwel alle lichtmasten zijn geschakeld waardoor deze alleen gedurende de donkere uren onder spanning staan.

eis -196	Leverancier is in staat om op huurbasis een voorziening te leveren om zo een Camera en bijbehorende apparatuur zoals zenders van stroom te kunnen voorzien, zodat deze 24/7 ononderbroken volledig goed werkt. Deze tijdelijke stroomvoorziening mag geen geluid of stank produceren en een beperkte ruimte innemen.
eis -197	Een tijdelijke stroomvoorziening dient in een vandaalbestendige kast te worden geplaatst met slot met niet algemeen verkrijgbare sleutel (bijv. een driehoeksleutel). Er dient hier een slot te worden gebruikt met een sleutel die genummerd is en waarbij de sleutel niet een standaard-nummer heeft. Alle kabels en leidingen dienen veilig en vandaalbestendig te worden afgewerkt.
eis -198	Leverancier beschikt over voldoende gediplomeerd personeel om een Camera met tijdelijke stroomvoorziening conform alle geldende normen aan te sluiten. Bij aansluiting van een accu op een lichtmast geldt deze eis nadrukkelijk ook.
eis -199	Bij gebruik van een lichtmast dient de aansluiting binnen de mast gemarkeerd te worden met een label "CCTV Politie" zodat voor andere gebruikers duidelijk is dat deze aansluiting ongemoeid moet worden gelaten.
eis -200	Leverancier is in staat om een accu op koopbasis te leveren (in de situaties waarbij een Liander-aansluiting niet of niet snel realiseerbaar is). Deze accu dient vandaal- en weerbestendig te zijn met een opslagcapaciteit van ten minste 120Ah en geschikt te zijn voor minimaal 1500 laadcycli. Indien niet gebruikt dan is Leverancier in staat deze op zijn locatie en onder zijn beheer aan een druppellader te koppelen.

7.4 Cameramasten en andere voorzieningen

eis -201	Cameramasten kunnen worden geleverd als vaste mast en als kantelmast met een lengte van 6, 8 of 9 meter boven maaiveld. Levering van een kantelmast is incl. discusslot met 3 sleutels waarvan één voor Opdrachtgever.
eis -202	Het is mogelijk een cameramast tegen meerprijs te leveren in een door Opdrachtgever te specificeren RAL-kleur o.b.v. poedercoating.
eis -203	Leverancier is in staat tot plaatsing van stabiele cameramasten met een lengte boven maaiveld tot ten minste 9 meter.

eis -204	Installatie van een cameramast is inclusief aanvraag vergunning en legeskosten, KLIC-melding, transportkosten, fundatie, afvoeren grond, herbestrating en andere werkzaamheden.
eis -205	Cameramasten dienen expliciet geschikt te zijn voor cameratoezicht en voldoende stijf te zijn. De fundatie van de masten dient voldoende stevig te zijn, om trillingen van camerabeelden door wind of veroorzaakt door derden (vrachtverkeer, trams, schoppen) minimaal te houden.
eis -206	Cameramasten zijn voorzien van fundatie, een inklimbeveiliging, en eventuele andere aspecten noodzakelijk voor realisatie.
eis -207	De cameramast dient corrosiebestendig en gedurende de eerste 10 jaar geen onderhoud te vragen.
eis -208	De cameramast is voorzien van een ondergrondse voorziening voor doorvoer van kabels.
eis -209	Leverancier is in staat een aanrijbeveiliging te leveren en te installeren voor een cameramast of straatkast die het object beschermt onder een hoek van ten minste 90 graden tegen aanrijdingen.

7.5 Straatkasten en junctionboxen

eis -210	Lokale apparatuur die niet weer- of vandaalbestendig is (bijv. voedingen) dient geplaatst te worden in een afgesloten vandaalbestendig en weerbestendig compartiment (bijvoorbeeld in een straatkast, of junctionbox) indien plaatsing in de camerabehuizing of de cameramast geen optie is.
eis -211	Installatie van een straatkast is inclusief transportkosten, fundatie, aarding, KLIC-melding, voorbereiding straatkast, storten vocht absorberende korrels en aanbrengen montage-rails, en alle andere werkzaamheden.
eis -212	Een straatkast of junctionbox wordt geleverd in een formaat zodat deze niet groter dan nodig is, rekening houdend met de te plaatsen apparatuur en bijbehorende warmtelast.
eis -213	Een straatkast of junctionbox dient de eerste 10 jaar geen onderhoud te vragen.
eis -214	De minimale eisen die aan stratkasten worden gesteld zijn: <ul style="list-style-type: none"> • De kast is voorzien van een slot met drie niet algemeen verkrijgbare sleutels. De Opdrachtgever krijgt ten minste 1 gelabelde sleutel. • De kast is voorzien van een aardlekschakelaar of zekering en middelen voor montage van apparatuur. • De kast is voorzien van montagerails. • De kast is beschermd tegen vocht en stof, IP66 of beter. • De kast dient op openbare grond te staan en goed bereikbaar te zijn vanaf de openbare weg voor onderhoud. • De kast dient vandalismebestendig te zijn. • De kast dient geaard te zijn. • Indien een stroomaansluiting ook in de kast zit, dan dient deze te voldoen aan de eisen van de netbeheerder. • Indien een stroomaansluiting ook in de kast zit, dan dient deze separaat toegankelijk te zijn, zonder dat ook toegang verkregen kan worden tot de overige apparatuur in de kast.
eis -215	De minimale eisen die aan junctionboxen worden gesteld zijn:

	<ul style="list-style-type: none"> • De junctionbox is voorzien van een slot met drie sleutels. De Opdrachtgever krijgt ten minste 1 gelabelde sleutel. • De junctionbox is voorzien van een zekering en middelen voor montage van apparatuur. • De junctionbox biedt IP66 bescherming of beter. • De junctionbox dient vandalismebestendig te zijn.
eis -216	De bekabeling tussen straatkast en mast zal altijd in een mantelbuis worden afgewerkt. Alle gebruikte bekabeling is geschikt voor de toegepaste omstandigheden.

7.6 Montage

eis -217	Alle apparatuur (zowel in in pandige 19"-racks, politiebureaus, straatkasten en junctionboxen) zal door Leverancier worden voorzien van een sticker waarmee het apparaat te identificeren is en is op te zoeken in de as-builtonformatie. De sticker bevat geen gevoelige informatie zoals IP- of MAC-adressen. Stickers dienen robuust te zijn, lang mee te kunnen gaan, en niet eenvoudig te verwijderen zijn.
eis -218	<p>Bij montage op masten van derden gelden de volgende voorschriften:</p> <ul style="list-style-type: none"> • Er wordt niet in masten geboord, tenzij de mast is voorzien van een separaat compartiment, of tenzij dit is toegestaan door de eigenaar van de mast (dan dienen de wensen en eisen van de eigenaar opgevolgd te worden). • Bij alle bevestigingen op een mast, bijv. met klembanden of RVS-profielen, wordt metaal op metaal contact vermeden, bijv. door het aanbrengen van een beschermingslaag die duurzaam het metaal zal beschermen. • Stroomvoorziening wordt buitenlangs de mast geleid beschermd door een RVS omegaprofiel of gelijkwaardig, tenzij de mast is voorzien van een separaat compartiment.
eis -219	De Camera dient vandaalbestendig en waterdicht gemonteerd te worden. Kabels worden zoveel mogelijk uit het zicht weggewerkt. Kabels die buitenlangs en/of in het zicht worden bevestigd lopen door een RVS profielgoot of metalen slang indien deze lager dan 5m vanaf straatniveau of een eenvoudig bereikbare plek worden aangebracht.
eis -220	<p>Leverancier gaat bij elke installatie uit van een checklist die aantoonbaar wordt doorlopen en onderdeel is van de oplevering. Gedurende de looptijd zal deze in gezamenlijk overleg worden geüpdatet. Onderdelen van deze checklist zijn minimaal:</p> <ul style="list-style-type: none"> • Datum van invullen checklist. • Metaal-op-metaalcontact is afgeschermd. • Camera is schoon bij oplevering. • Camera is voorzien van politie-striping. • Camera voldoet aan eis -36. • Camera is voorzien van privacy masks door Leverancier en gecontroleerd door CCTR (naam contactpersoon en datum te vermelden). • Dode hoek van de Camera is afgestemd met de CCTR (naam contactpersoon en datum te vermelden). • Apparatuur is aantoonbaar gelabeld.

	<ul style="list-style-type: none"> • GPS LatLon-coördinaten zijn bekend. • Er zijn foto's gemaakt van de gehele oplevering voor gebruik in de as-buit. • Bij gebruik van stroompunt Liander is de EAN-code opgenomen in de as-buit • Beeldkwaliteit en bediening van Camera's is conform kwaliteitseisen. Bij gebruik netwerk van derden (bijv. Ziggo) is Leverancier niet verantwoordelijk voor beperkingen in dit deel van het netwerk, mits de problemen hier aantoonbaar door worden veroorzaakt. • Rechten tot Camera's zijn correct ingesteld. • Bij gebruik Ziggo-verbinding of andere externe partij is het contractnummer en alle andere relevante informatie doorgegeven aan de Opdrachtgever en aan Ziggo de routecode en factuurgegevens. • Camera's worden getoond in de plattegronden en zijn hieruit opvraagbaar. • Camera's worden opgenomen gedurende 28 dagen. • Apparatuur is voorzien van laatste stabiele versie firmware. • Camera is voorzien van wachtwoorden voor zowel Leverancier als functioneel beheer. Fabriekswachtwoorden zijn gewijzigd. • Van welke (straal)verbinding/zender gebruik wordt gemaakt om het signaal door te zetten naar de CCTR - Netwerkaart
--	---

7.7 Ondergrondse infrastructuur

eis -221	Indien Leverancier ondergrondse werkzaamheden verricht zal altijd een zgn. KLIC-melding worden gedaan en rekening worden gehouden met bestaande ondergrondse infrastructuur.
eis -222	<p>Voor aanleg van ondergrondse infrastructuur gelden de volgende eisen:</p> <ul style="list-style-type: none"> • Databekabeling dient in een mantelbuis te worden aangelegd. • Indien bekabeling voor een stroomvoorziening niet in een mantelbuis wordt aangelegd dan dient deze mechanisch beschermd te zijn. • Onderdeel van werkzaamheden en oplevering zijn revisietekeningen en aanmelding bij de partij die voor Opdrachtgever de KLIC-server verzorgt. • Ondergrondse infrastructuur dient ondergronds adequaat gelabeld te worden zodat een gravende partij weet dat het bekabeling voor gemeentelijk cameratoezicht betreft. • Lege mantelbuizen worden voorzien van trekkoorden en trekputten. • Aangelegde databekabeling zal op correcte werking worden gecontroleerd. In het geval van koperbekabeling wordt dit aangetoond d.m.v. een test met IP-verkeer. In het geval van glasvezelbekabeling met een OTDR-meting waarbij de demping binnen de algemeen geldende normen blijft. • Indien van een revisietekening in een recente Autocad-versie bij de WION/WIBON beheerder van de Opdrachtgever (met cc aan de Contractregisseur).

8 Netwerk-aspecten

8.1 Eisen algemeen

eis -223	Leverancier dient het cameranetwerk gescheiden te houden van andere netwerken. Alle verbindingen met andere netwerken dienen via de bestaande firewall te lopen.
eis -224	Leverancier is verantwoordelijk voor het beheer en onderhoud van alle actieve netwerkcomponenten en draadloze verbindingen. Verbindingen die door derden worden gerealiseerd zoals glasvezelverbindingen onder beheer van bijvoorbeeld KPN, Ziggo en Eurofiber vallen buiten de verantwoordelijkheid van Leverancier. Wel heeft Leverancier in geval van storingen een coördinatieplicht om de storingen op te lossen.
eis -225	Leverancier is verantwoordelijk voor het gehele IP-plan en zal dit gedurende de looptijd van het contract beheren en er voor zorgdragen dat deze altijd up-to-date is..
eis -226	Andere diensten van Contractpartner kunnen gebruik maken van het breed verspreide netwerk van de CCTR. Hierbij moet gedacht worden aan additionele sensoren voor experimentele doeleinden of het meten van luchtkwaliteit. Uitgangspunt is dat deze voorzieningen geen negatief effect mogen hebben op het operationele cameratoezicht. Bij gebruik van draadloze verbindingen zal het verkeer daarom een lage prioriteit krijgen (deze verbindingen zijn alleen toegestaan indien technisch mogelijk). Leverancier zal voor deze toepassing een apart VLAN inrichten en het toevoegen van dergelijke sensoren aan het netwerk faciliteren.

8.2 Netwerkveiligheid

eis -227	Leverancier is gedurende de looptijd van het contract verantwoordelijk voor het implementeren en bewaken van de netwerkveiligheid.
eis -228	Elke switch die niet in een politielocatie staat zal alle ongebruikte poorten uitschakelen. Daarnaast zullen deze switches alleen netwerkverkeer accepteren van Netwerkcomponenten met een bekend MAC-adres. Bij detectie van poging tot onterechte toegang dient de switch de betreffende poort automatisch uit te schakelen indien het een poort betreft waar alleen verkeer van één camera passeert. In alle gevallen zal een waarschuwing via laatste versie SNMP (v3 bij start contract) worden gegenereerd.
eis -229	Elke Netwerkcomponent die buiten een politielocatie wordt geïnstalleerd dient toegang tot het netwerk te krijgen o.b.v. MAC-adres. Configuratie van deze functionaliteit is onderdeel van de standaard installatiekosten.
eis -230	Leverancier mag uitgaan van continue remote toegang tot het CCTR-netwerk. Contractpartner 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 Leverancier remote toegang tot het netwerk te ontzeggen.
eis -231	Leverancier zorgt voor een adequate netwerksegmentatie. Hiervoor gelden de volgende aanvullende eisen:

	<ul style="list-style-type: none"> • Segmentatie vindt plaats op laag 2 van het OSI-model. • Hosts worden vooraf geclassificeerd, bijv. CIA-triad (Confidentiality, Integrity, Availability). Alleen hosts met dezelfde classificatie worden bij elkaar in een segment geplaatst. • Een segment bevat maximaal 20 hosts. • Hosts die bereikbaar zijn via het internet worden in een DMZ geplaatst. • Elk lokale cameraproject heeft een eigen netwerksegment. • Uitkijkclients hebben een eigen netwerksegment. • Centrale servers hebben een eigen netwerksegment. • Camera's mogen alleen communiceren met centrale apparatuur en relevante uitkijkclients. • Het verkeer tussen netwerksegmenten wordt gefilterd door een interne firewall. Filtering is hierbij strikt, d.w.z. geen verkeer tenzij expliciet toegestaan. Filtering o.b.v. source en destination adres/poortnummers en protocol. <p>Afwijking van bovenstaande is alleen toegestaan na schriftelijke toestemming van de Contractregisseur.</p>
--	--

8.3 Eisen aan switches

eis -232	Alle te leveren switches of routers zijn in staat volwaardig en zonder beperkingen te functioneren met alle bestaande netwerkapparatuur.
eis -233	<p>De te leveren switches dienen voldoende switchcapaciteit te hebben voor de beoogde inzet waarbij er ten minste nog 40% (bandbreedte en CPU) overcapaciteit is voor uitbreidingen en opvang van piekmomenten.</p> <p>Een piekmoment is een willekeurig moment waarbij meerdere databronnen een grotere hoeveelheid data sturen dan gebruikelijk. In een nachtelijke situatie als camera's meer data sturen is daarom niet sprake van een piekmoment omdat deze verhoging elke nacht optreedt en dus gebruikelijk is. Kortom, bij het plaatsen van een nieuwe switch dient rekening te worden gehouden met het feit dat de datastroom in de nachtelijke uren altijd verhoogd is.</p>
eis -234	Netwerkswitches dienen 'managed' te zijn, d.w.z. op afstand te beheren, te monitoren en te configureren.
eis -235	Een voeding is onderdeel van de leveringsprijs.
eis -236	Het geheel van netwerkapparatuur is geschikt voor toepassing van het multicast-protocol.
eis -237	<p>Switches dienen geleverd te worden incl. alle benodigde support en updates van de fabrikant van minimaal drie jaar bij levering. Deze ondersteuning is jaarlijks te verlengen tot minimaal 5 jaar na levering. Kosten van de eerste drie jaar zijn onderdeel van de leveringsprijs.</p> <p>Leverancier is verantwoordelijk voor beheer van de onderhoudscontracten. Bij beëindiging contract worden de nog lopende onderhoudscontracten overgedragen aan Contractpartner of de nieuwe leverancier.</p> <p>Bij apparatuur die op spare aanwezig is, is Next Business Day van toepassing. Op apparatuur waarbij dat niet geldt is 24/7 van toepassing. Bij cruciale apparatuur, bijv. bij de core switch, kunnen hogere</p>

	eisen in overleg worden gesteld.
eis -238	<p>Voor een switch die wordt geplaatst in een niet-geconditioneerde ruimte als junctionbox of straatkast gelden de volgende eisen:</p> <ul style="list-style-type: none"> • Geschikt voor een groot operationeel temperatuurbereik van -20 tot 60 °C. • 2 SFP-poorten van ieder 1 Gbps. • 4 RJ45-poorten van 100 Mbps.
eis -239	<p>Voor de netwerkknooppunten wordt onderscheid gemaakt tussen knooppunten met een standaard capaciteit en knooppunten met een hoge capaciteit (Lijnbaansgracht en Hoofdbureau).</p> <p>Voor een standaard knooppunt gelden de volgende minimale eisen aan de switch:</p> <ul style="list-style-type: none"> • 24x 10/100/1000 Mbps RJ45 netwerkpoort. • 2x SFP 1 Gbps • Mogelijkheid tot uitbreiding met een extra voeding. • Mogelijkheid om ten minste vier fysieke interfaces te combineren tot één logische verbinding met de geaggregeerde capaciteit van de gecombineerde fysieke interfaces. • Het is mogelijk om switches van hetzelfde type te combineren zodat ze zich gedragen als één logische switch-eenheid. • Full-duplex switching-capaciteit van 100 Gbps. • Forwarding-capaciteit van 70 Mpps (uitgaande van 64 bytes Layer 3 pakketten) • 19"-rack mount • Geschikt voor een omgevingstemperatuur van 40°C. • MTBF > 50 jaar <p>Voor een knooppunt met hoge capaciteit gelden bovenstaande eisen en de volgende aanvullende eisen:</p> <ul style="list-style-type: none"> • 2x SFP+ i.p.v. 2x SFP • Forwarding-capaciteit van 90 Mpps (uitgaande van 64 bytes Layer 3 pakketten)
eis -240	<p>Netwerkswitches dienen ten minste de volgende protocollen te ondersteunen:</p> <ul style="list-style-type: none"> • UDP/TCP • IPv4/IPv6 • ICMP (RFC 792 / 950) en ICMPv6 (RFC 2461 / 2463) • IGMP (RFC1112 / RFC2236 / RFC3376) • SNMP v1/v2/v3 • Ondersteuning van QoS (Quality Of Service) en VLANs • NTP (Network Time Protocol, RFC1305) • IEEE 802.1x en Radius

8.4 Netwerkmonitoring

eis -241	Leverancier dient als dienst continu alle netwerkcomponenten met een eigen IP-adres via SNMP te
----------	---

	monitoren. Hier dient de laatste versie SNMP (v3 bij start contract) te worden gebruikt waar mogelijk. Gebruik van een lagere versie mag alleen na expliciete toestemming van de Contractregisseur.
eis -242	SNMP-monitoring zal alle problemen die Netwerkcomponenten zelf melden, af vangen en aan Leverancier doorgeven. Deze dient hierop vervolgens adequaat actie te ondernemen. Het oplossen van het probleem en dit te melden bij de opdrachtgever(s).
eis -243	SNMP-monitoring zal alle relevante statuswaarden van Netwerkcomponenten opvragen en verifiëren of deze zich binnen vooraf vastgestelde waardes bevinden. Indien dit niet het geval is wordt dit gemeld aan Leverancier. Deze dient hierop vervolgens adequaat actie te ondernemen.
eis -244	Het monitoringsysteem zal binnen de organisatie van Contractpartner functioneren. Geconstateerde problemen dienen door te worden gegeven naar het systeem binnen het netwerk van de Leverancier.
eis -245	Leverancier dient alle functionaliteit van de huidige implementatie van het monitoringsysteem Zabbix in stand te houden in een eventueel nieuw te plaatsen systeem.
eis -246	Elke nieuw te implementeren netwerkcomponent dient te worden opgenomen in het monitoring-systeem. Kosten hiervoor zijn onderdeel van de installatieprijs.
eis -247	De volgende gebeurtenissen dienen ten minste door het monitoringsysteem te worden waargenomen en gemeld: <ul style="list-style-type: none"> • Het wegvallen van een verbinding naar een netwerkcomponent. • Storing of overschrijden van ingestelde grenswaardes in een willekeurig netwerkcomponent die via SNMP achterhaald kan worden. • Inbraakpoging, bijv. onbekend MAC-adres. • Afwijkende datastroom (datavolume) op een poort, zowel van als naar een component die zich buiten een politielocatie bevindt. • Het vollopen van de opslag. • Storing in de opslag (bijv. het uitvallen of foutmelding van één of meer harde schijven).

9 Aanpassingen, implementatie en oplevering

9.1 Aanpassingen

eis -248	Aanpassingen aan het Cameratoezichtstelsysteem zullen als Offerte worden aangeboden en als project worden uitgevoerd.
eis -249	Voor elk project zal Leverancier een projectmanager aanstellen die als direct aanspreekpunt voor Opdrachtgever zal functioneren.
eis -250	<p>Werkzaamheden voor uitbreiding, vervanging of nieuwe projecten worden marktconform aangeboden. Hiermee wordt het volgende bedoeld:</p> <ul style="list-style-type: none"> • De Offerte wordt door de Leverancier volledig en open gespecificeerd. Het betreft hierbij ten minste merk en type van te leveren apparatuur en detaillering en uitsplitsing van de uitvoering. • De Offerte hanteert de eenheidsprijzen zoals gespecificeerd in de Inschrijving voor deze aanbesteding. • Opvolgers van in deze aanbesteding aangeboden apparatuur (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 apparatuur. • Vooraf kan door Opdrachtgever een directieraming worden opgesteld waarbij het recht wordt voorbehouden de kosten te maximaliseren. • Indien de Leverancier niet akkoord gaat met de vastgestelde maximumprijs en de argumenten hiervoor niet worden geaccepteerd door Opdrachtgever dan zal een andere leverancier worden gezocht. Aan deze leverancier zullen dezelfde eisen (product, documentatie, oplevering, uniformiteit, etc.) worden gesteld als in deze aanbesteding waarbij het behoud van eenduidigheid van de infrastructuur zal worden geëist. • De leverancier beschikt over vastgestelde procedures voor de vervanging van opslagmedia en/of hardware. <p>Leverancier zal hierbij integratie van het nieuwe project faciliteren. Na succesvolle oplevering en probleemloos functioneren gedurende een maand zal Leverancier het nieuwe project in beheer nemen.</p>
eis -251	Leverancier heeft de verplichting om een eenduidige en consistente technische infrastructuur van het Cameratoezichtstelsysteem in stand te houden.
eis -252	Op verzoek van de Opdrachtgever zal binnen één week een schouw worden uitgevoerd.
eis -253	Een schouw leidt binnen drie werkdagen tot een schouwrapport van de Leverancier. In een schouwrapport wordt, ondersteund door foto's, ingegaan op de locatie van de camera, hoogte camera, zicht vanuit de camerapositie, het al dan niet plaatsen van een mast, realisatie van stroomvoorziening, inzet van eventuele tijdelijke stroomvoorziening, realisatie van verbinding, dode hoek, eventuele uithouders en de lengte daarvan, en mogelijke andere aandachtspunten.
eis -254	Een Offerte zal binnen twee weken na uitgevoerde schouw worden afgegeven en een geldigheidsduur hebben van ten minste drie maanden. Bij een complex traject kan de Leverancier hier meer tijd voor nodig hebben. Dit dient echter bij de schouw of uiterlijk drie werkdagen daarna aannemelijk te worden gemaakt.

eis -255	<p>Nadat Opdrachtgever de opdracht heeft gegeven, bevestigt de Leverancier binnen 2 werkdagen middels een digitale opdrachtbevestiging.</p> <p>De opdrachtbevestiging gaat ten minste in op:</p> <ul style="list-style-type: none"> • Offertenummer • Opdrachtnummer • Projectnummer leverancier • Contactpersoon/projectmanager van de betreffende opdracht • Nogmaals totaalbedrag en de gekozen opties (ter verificatie).
eis -256	<p>Onderdeel van elke Offerte is een realistische planning rekening houdend met levertijden, werkzaamheden derden (bijv. Liander), aanvragen vergunningen en implementatie. Na gunning zal door Leverancier binnen twee weken een realistische voorlopige planning worden aangeleverd. In het geval dat leveringen van derden op het kritieke pad zitten dan zal Opdrachtnemer deze acties direct in gang zetten na opdracht. Indien door derden een aanpassing van de planning noodzakelijk is, dan zal zodra dit bekend is door Opdrachtnemer de planning worden herzien.</p>
eis -257	<p>Bij aanpassingen ten gevolge van projecten van derden in gebouwen dan wel de openbare ruimte dient de planning van het betreffende project gerespecteerd te worden.</p>

9.2 Oplevering

eis -258	<p>Bij elke projectoplevering dient een, door Opdrachtgever vooraf goed te keuren, SAT-protocol te leveren waarin de volgende punten minimaal doorlopen dienen te worden:</p> <ul style="list-style-type: none"> • Controle checklist (eis -220) • Visuele inspectie van alle onderdelen per locatie; <ul style="list-style-type: none"> - Technische controle; - Visuele controle; - Werking beveiligingen; - Bekabeling en labelling van componenten; - Afmontage; • Functionele inspectie van correcte werking binnen het Cameratoezichtstelsel. <ul style="list-style-type: none"> - Beeldkwaliteit en bediening van Camera's en geverifieerd door een senior observant. - Rechten tot Camera's. - Camera's worden getoond in de plattegronden en zijn hieruit opvraagbaar. - Opslag en terugzoeken van beelden. • Bijgewerkte as-built en beschikbaarheid handleidingen. • Het door Opdrachtgever goedgekeurde opleverrapport.
eis -259	<p>Elke projectoplevering wordt na afronding als geheel getest en geaccepteerd in combinatie met de rest van het Cameratoezichtstelsel. De acceptatie door Opdrachtgever vindt plaats na goedkeuring uitkomsten SAT-test en oplossing van alle geconstateerde restpunten, 1 maand probleemloos functioneren én oplevering as-built documentatie.</p>



	LET OP: zonder volledige en goedgekeurde SAT-test inclusief as-builde documentatie zal de oplevering niet geaccepteerd worden en zal er geen betaling plaatsvinden.
--	---

10 Beheer en onderhoud en aanpassingen Cameratoezichtstelsysteem

10.1 Algemeen, beschikbaarheid en regelingen

eis -260	Leverancier zal een SLA en een DAP afsluiten met Opdrachtgever conform de aanbestedingsdocumenten, waaronder dit PVE, en deze naleven.
eis -261	Opdrachtgever maakt onderscheid in belangrijkheid van Camera's (prio 1 en prio 3). De specifieke eisen worden nader uitgewerkt in dit hoofdstuk. Leverancier zal in zijn beheer en onderhoud om kunnen gaan met de verschillende eisen verbonden met de drie prioriteitsstellingen. Gedurende de looptijd van het contract heeft Opdrachtgever op elk moment de mogelijkheid om de prioriteitsstelling van een Camera aan te passen. Verrekening van de kosten zal naar rato op dagbasis plaatsvinden.
eis -262	Na de overdrachtsdatum zal de Leverancier per direct het Cameratoezichtstelsysteem van Contractpartner in beheer nemen.
eis -263	De Leverancier is verantwoordelijk voor al het Beheer en Onderhoud voor alle nieuw te leveren als overgenomen onderdelen van het Cameratoezichtstelsysteem en de koppelingen hiervan met de diverse andere systemen gedurende de looptijd van het contract.
eis -264	Netwerkvoorzieningen van KPN, Eurofiber, Ziggo of andere partijen vallen buiten de verantwoordelijkheid van de Leverancier. Wel heeft de Leverancier hier een coördinatieplicht bij storingen die impact hebben op het Cameratoezichtstelsysteem en waar nodig ondersteuning te verlenen bij het oplossen van de storing dan wel te controleren of de storing is opgelost..
eis -265	Het resultaat van Beheer en onderhoud moet zijn dat het Cameratoezichtstelsysteem beschikbaar is en blijft voor het uitkijken, terugkijken en opslag van beelden. Van onbeschikbaarheid is sprake indien één of meerdere functionaliteiten van het Cameratoezichtstelsysteem niet mogelijk zijn.
eis -266	Gedurende de contractperiode garandeert de Leverancier de functionele beschikbaarheid van het Cameratoezichtstelsysteem conform de volgende minimale beschikbaarheidsniveaus op jaarbasis: <ul style="list-style-type: none"> • Voorzieningen Cameratoezichtstelsysteem op de Eenhoorn of andere gebouwen: 99,9% • Elke individuele Camera prio 1: 99.5% • Elke individuele Camera prio 3: 99.0% Indien dit niet wordt gehaald is de boeteclausule van toepassing. Zie de Overeenkomst voor meer informatie.
eis -267	Onbeschikbaarheid van het Cameratoezichtstelsysteem ten gevolge van storingen of schades door aanrijdingen, natuurgeweld, vandalisme, sabotage of ondeskundig handelen van Contractpartner worden niet meegerekend bij de bepaling van de onbeschikbaarheid die de Leverancier zou zijn toe te rekenen. Leverancier dient duidelijk te maken waarom een dergelijke onbeschikbaarheid hem niet is toe te rekenen. Tevens geldt voor Leverancier een inspanningsverplichting om te doen wat in zijn macht ligt om de storing zo snel mogelijk op te lossen.
eis -268	Onbeschikbaarheid van het Cameratoezichtstelsysteem ten gevolge van stroomuitval in het netwerk van de stroomleverancier worden niet meegerekend bij de bepaling van beschikbaarheid die de Leverancier zou zijn toe te rekenen.
eis -269	Het moment van onbeschikbaarheid gaat in bij de melding van een storing door Contractpartner of

	het monitoringsysteem aan de Leverancier.
eis -270	De hersteltijd en daarmee onbeschikbaarheid eindigt op het moment dat de Leverancier de storing heeft verholpen c.q. functieherstel heeft gerealiseerd en hiervan een e-mail melding is gedaan bij Contractpartner door de Leverancier.
eis -271	Indien een storing niet correct is afgehandeld, gegeven een tweede vergelijkbare storingsmelding binnen drie kalenderdagen aan hetzelfde onderdeel van het Cameratoezichtstelsysteem, wordt de eerste melding niet als afgehandeld beschouwd.
eis -272	Het is noodzakelijk dat er regie wordt gevoerd vanuit Contractpartner op wijzigingen aan het Cameratoezichtstelsysteem. Deze taak is belegd bij de contractregisseur van de gemeente Amsterdam. Leverancier is er daarom voor verantwoordelijk dat bij elke wijziging door één van de Opdrachtgevers deze persoon tijdig op de hoogte wordt gesteld van de wijziging.

10.2 Kosten

eis -273	Alle kosten voor beheer en onderhoud zijn onderdeel van het aangeboden Beheer en Onderhoud. Het betreft hierbij ten minste arbeid, hoogwerker, voorrijkosten, transportkosten, verkeersmaatregelen, vergunningen, materialen en componenten binnen de garantietermijn en de kosten voor kleinmateriaal. Het volgende valt niet onder deze kosten: <ul style="list-style-type: none"> • Aanpassingen aan het Cameratoezichtstelsysteem m.b.t. het realiseren van nieuwe functionaliteit of het verwijderen van bestaande functionaliteit. • Aanschafkosten van componenten na afloop van de garantietermijn. • Correctief onderhoud ten gevolge van storingen of schade door aanrijdingen, natuurgeweld, vandalisme of sabotage en ondeskundig handelen van Opdrachtgever. • Aanvulling van de voorraad spare-parts (tenzij van producten binnen de garantietermijn).
eis -274	Kosten voor onderhoudslicenties van software (SMA) zijn onderdeel van het aangeboden Beheer en Onderhoud.
eis -275	Voorrijkosten kunnen alleen in rekening worden gebracht voor technisch personeel en de projectleider voor werkzaamheden buiten de SLA. Andere reiskosten dienen onderdeel te zijn van de jaarlijkse kosten voor beheer en onderhoud.
eis -276	Kosten voor het aanvullen van de (strategische) sparepart-voorraad van onderdelen binnen de garantietermijn zijn onderdeel van het aangeboden Beheer en Onderhoud.

10.3 Storingsmanagement

eis -277	Onder storingsmanagement wordt in het kader van deze aanbesteding verstaan de taak om waar mogelijk storingen te voorkomen of vroegtijdig op te sporen en bij optreden van een storing deze in behandeling te nemen en binnen de opeeltijden te verhelpen, dan wel coördinatie te voeren met derden om de storing te laten verhelpen. Tot het takenpakket storingsmanagement behoren verschillende activiteiten. De Leverancier garandeert dat ten minste de volgende activiteiten behoren tot het storingsmanagement: <ul style="list-style-type: none"> • Het in behandeling nemen van storingen, zowel telefonisch als via een webapplicatie. • Prioriteitsstelling storing bepalen (prio 1 of 3). • Het leveren van eerste- en tweedelijns-ondersteuning bij vragen en problemen. • Het vroegtijdig ontvangen van storingen d.m.v. het netwerk-monitoringsysteem en het
----------	--

	<p>adequaaf handelen op signalen hiervan.</p> <ul style="list-style-type: none"> • De registratie van de storing en alle statuswijzigingen hiervan in het Storingsmanagementsysteem. • De bevestiging van de storing binnen de overeengekomen Responstijd (via e-mail), met vermelding van de datum en het tijdstip van de eerste melding en een uniek storingsnummer. • Melding aan relevante onderdelen van de organisatie van Opdrachtgever zoals netwerkbeheer en/of servicedesk. • Onmiddellijk informeren Opdrachtgever indien zich onvoorziene ontwikkelingen voordoen bij het verhelpen van de storing. • Het informeren Opdrachtgever na het verhelpen van de storing. • Het tijdig laten uitvoeren van preventief en correctief onderhoud. • De coördinatie met servicediensten (van derden zoals stroomvoorziening en datacommunicatie) en de voortgangsbewaking van de storingsafhandeling. • De storingsrapportage, waaronder storingsen van servicediensten van derden, met een formele herstelmelding van de servicedesk van de Leverancier aan de servicedesk van de Opdrachtgever (zie ook paragraaf 10.5). • Het leveren van correcte overzichtsrapportages zoals beschikbaarheidspercentages voor een bepaalde periode (zie ook paragraaf 10.6).
eis -278	Leverancier stelt aan Contractpartner een Storingsmanagementsysteem beschikbaar waarmee de Contractpartner in staat wordt gesteld storingsen te melden en de status van de storingsoplossing te kunnen volgen, en storingsen uit het verleden in te kunnen zien.
eis -279	Het Storingsmanagementsysteem is beschikbaar als beveiligde webapplicatie (authenticatie en versleuteling van de verbinding via HTTPS met geldig certificaat).
eis -280	<p>Het is toegestaan om via een, door Contractpartner beschikbaar gestelde, beveiligde VPN-verbinding in te loggen op het systeem t.b.v. onderhoudswerkzaamheden, storingsanalyse, configuraties of helpdesk-support.</p> <p>Leverancier mag uitgaan van een functionele internetverbinding (minimaal 500 Mbps symmetrisch en gegarandeerd, deze wordt echter ook gebruikt voor camera's die over internet gekoppeld zijn) en een koppelpunt op het netwerk van Contractpartner.</p>
eis -281	Leverancier heeft de plicht om storingsen (in domeinen van derden of van Contractpartner) 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 -282	Leverancier beschikt over een eigen serviceorganisatie die 24 uur per dag, 7 dagen per week, alle dagen per jaar telefonisch beschikbaar en bereikbaar is en in staat om storingsen op te lossen.
eis -283	<p>De Leverancier is verantwoordelijk voor het aanhouden en beheren van <u>alle</u> benodigde reservematerialen (spare-parts), 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 oplostijden of minimale beschikbaarheidspercentages.</p> <p>Waar dit voor de praktische uitwerking van Beheer en onderhoud efficiënter is, is het ook toegestaan om reservematerialen op te slaan bij Contractpartner die daarvoor ruimte op de uitkijkcentrale (24/7 bereikbaar) ter beschikking stelt.</p>

10.4 Preventief onderhoud en schoonmaak Camera's

eis -284	Leverancier levert duurzaam materiaal dat geen of minimaal (preventief) onderhoud behoeft.
eis -285	Preventief onderhoud dient uitgevoerd te worden volgens afspraken in de DAP.
eis -286	Minimaal één keer per jaar zal de Leverancier preventief onderhoud uitvoeren op het gehele systeem dat in beheer is. Leverancier dient alle betrokken installaties en centrale apparatuur na te lopen en de correcte functionaliteit vast te stellen, te controleren op slijtage, roestvorming, beschadigingen en reinigen waar dit noodzakelijk is en afstellingen te controleren.
eis -287	Aan het begin van elk kalenderjaar wordt door de Leverancier een preventief onderhoudsplan ingediend voor het gehele jaar en afgestemd met Opdrachtgevers. Het plan dient in te gaan op planning en impact van de werkzaamheden.
eis -288	Leverancier draagt zorg voor het tijdig offrenen en doorvoeren van verlenging van bestaande onderhoudslicenties, zoals bijvoorbeeld voor het VMS.
eis -289	Tijdens het preventief onderhoud dient het Cameratoezichtstelsel zoveel mogelijk te blijven functioneren.
eis -290	In het preventief onderhoud worden frequent de relevante software- of firmware-updates doorgevoerd. Voor machines met een Windows OS of de firewalls vindt dit minimaal elke drie maanden plaats. Voor firmware van Camera's, switches en zenders zal dit minimaal elk jaar plaatsvinden. Voor kritische updates zie eis -32. De jaarlijkse update voor camera's, switches en zenders wordt in een script vastgelegd en wordt opgenomen in het jaarlijkse plan voor preventief onderhoud. Updates mogen per cluster/bulk plaatsvinden. Gezamenlijk wordt bepaald hoe clustering wordt ingevuld.
eis -291	Uitvoering van preventieve onderhoudswerkzaamheden dient buiten de belangrijkste of drukste uitkijkuren te worden gerealiseerd. Opslag van camerabeelden dient gedurende deze werkzaamheden niet verstoord te worden. Voordat de werkzaamheden worden gestart dient de Opdrachtgever akkoord te zijn en de CCTR bevestigd of er geen belemmeringen zijn op dat moment.
eis -292	De gehele dome of het venster van elke Camera prio 3 dient minimaal twee keer per jaar grondig te worden gereinigd. Elke prio 1 Camera dient drie maal per jaar grondig te worden gereinigd. Indien in de toekomst een product op de markt komt dat overtuigend voordeel heeft met het voorkomen van vlekken door vuil of slecht opdrogende regendruppers dan dient dit product minimaal éénmaal per jaar bij het preventief onderhoud te worden aangebracht. Aannee hierbij is dat het product op vergelijkbare wijze is aan te brengen zoals nu het geval is met dergelijke coatings. Kosten zijn onderdeel van het reguliere onderhoudscontract.
eis -293	Contractpartner kan binnen de kosten van het reguliere onderhoudscontract Camera's op aanwijzing laten reinigen. Contractpartner beoogt hiermee om Camera's die van groter belang zijn en/of sneller vuil worden vaker te kunnen laten reinigen. Voor elke Camera in het areaal valt één vrij toe te kennen reinigingsopdracht binnen de Overeenkomst. Het reinigen op aanwijzing dient binnen één week te worden uitgevoerd.

	<p>Voorbeeld: Stel in het gehele areaal van de CCTR bevinden zich 350 Camera's. Dit betekent dat vanuit de CCTR er 350 willekeurige Camera's per jaar kunnen worden aangewezen om te reinigen. Typisch zal dit op weekbasis gebeuren waarbij er telkens ca. 5 Camera's worden benoemd.</p> <p>Toelichting: Gemiddeld worden de Camera's dus 3x per jaar grondig gereinigd bij prio 3, en 4x bij prio 1. Het kan dus voorkomen dat sommige Camera's elke maand schoon gemaakt moeten worden, waarbij andere Camera's bijv. maar 2x in dat jaar worden gereinigd.</p>
--	---

10.5 Correctief onderhoud

eis -294	<p>Correctief onderhoud dient te worden uitgevoerd op het Cameratoezichtstelsel, voorzieningen, apparatuur en software die onder verantwoordelijkheid van Leverancier valt. Onder correctief onderhoud wordt verstaan: het opsporen en herstellen van onvolkomenheden en Gebreken, nadat deze door de Contractpartner als storingen zijn gemeld of als deze op andere wijze zijn gebleken, bijv. uit de monitoring. Leverancier mag ervan uitgaan dat voor onderhoud er continu remote toegang tot het netwerk beschikbaar is, én fysiek toegang tot de Eenhoorn.</p>
eis -295	<p>Met betrekking tot correctief onderhoud wordt er onderscheid gemaakt naar drie prioriteitsstellingen bij storingen in het Cameratoezichtstelsel:</p> <ol style="list-style-type: none"> 1. Prio 3. Het betreft hier het grootste deel van de Camera's. Voor prio 3 geldt een Oplostijd van 24 uur (één werkdag), een Responstijd van 4 uur, en een Diagnosetijd van 8 uur. 2. Prio 1. Het betreft hier primair Camera's van de politie die gebruikt worden voor objectbewaking en de camera's bij Amsterdam CS. Voor prio 1 geldt een Oplostijd van 6 uur, een Responstijd van 15 minuten en een Diagnosetijd van 2 uur. Initieel betreft dit ca. 55 tot 60 Camera's incl. draadloze verbindingen.
eis -296	<p>Indien een Camera een bepaalde prioriteit heeft dan gelden de beschikbaarheidseisen voor de gehele keten om deze Camera te kunnen uitkijken of terug te kunnen kijken.</p>
eis -297	<p>Schade of storingen die zijn veroorzaakt als gevolg van overmacht en die niet vanuit het ontwerp, toegepaste materialen en installatie voorkomen hadden kunnen worden door de Leverancier, worden per geval tussen de Contractregisseur en Leverancier besproken en van acties voorzien. De onbeschikbaarheid van het systeem als gevolg van deze schade of defecten wordt dan niet meegerekend in de onbeschikbaarheid toe te rekenen aan de Leverancier. Wel heeft de Leverancier een inspanningsverplichting deze storingen zo snel mogelijk op te lossen.</p>
eis -298	<p>Correctief onderhoud dient te worden uitgevoerd op alle door Leverancier geleverde en/of overgenomen apparatuur en bekabeling. Inpandig aangelegde bekabeling zoals glasvezels of gebouwbekabeling niet aangelegd door Leverancier zijn hiervan uitgesloten.</p>
eis -299	<p>In geval van een storing stelt de Leverancier onmiddellijk de herstelprocedure in werking. De herstelprocedure voorziet onder meer in:</p> <ul style="list-style-type: none"> • Analyse van de storing, incl. inschatting van impact en omvang. • Diagnose van de oorzaak van de storing 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 te beheersen. • Functieherstel. • Registratie in het Storingsmanagementsysteem of aanlevering van alle relevante gegevens t.b.v. Storingsmanagement.

eis -300	Herstelwerkzaamheden van de centrale apparatuur dienen zo spoedig mogelijk te worden uitgevoerd, ook als de beschikbaarheidseisen niet lijken te worden overschreden. Indien werkzaamheden buiten kantooruren uitgevoerd dienen te worden om aan de beschikbaarheidspercentages te kunnen voldoen, dan dient dit gemeld te worden aan de Contractpartner.
eis -301	De onderdelen van het Cameratoezichtstelsel die geen hinder ondervinden van het defect dienen ook geen hinder te ondervinden van correctieve werkzaamheden.

10.6 Rapportage

eis -302	<p>Ten behoeve van de ondersteuning van de contractmanager van de Contractpartner zal door Leverancier een rapportage minimaal per kwartaal worden aangeboden. Het document dient in te gaan op de volgende aspecten:</p> <ol style="list-style-type: none"> 1. Totaaloverzicht beschikbaarheid <ul style="list-style-type: none"> • Aantal meldingen en beschikbaarheid per kwartaal • Beschikbaarheidspercentage kwartaal <ul style="list-style-type: none"> ○ Binnen SLA ○ Buiten SLA, opgesplitst naar oorzaken buiten Leverancier en draadloze verbindingen. • Verdeling aantal meldingen kwartaal per categorie • Storingen buiten SLA kwartaal per reden 2. Meldingen gereed binnen de gespecificeerde oplostijden per prioriteit. 3. Top 25 (eventueel op verzoek uit te breiden): hoogste aantal storingen per camera (aantal meldingen, doorlooptijden). 4. Overzicht meldingen en beschikbaarheid per project. 5. Meldingen binnen SLA <ul style="list-style-type: none"> • Meldingen binnen SLA per categorie (Hardware, Applicaties, Netwerk, Software) • Meldingen binnen SLA per subcategorie (ten minste Camera, VMS, Draadloze verbinding, Werkstation, Monitor, Server, Windows) 6. Meldingen buiten rapportage (bijv. dubbele meldingen of foute meldingen) 7. Het reinigen van Camera's (zowel regulier als op aanwijzing) is onderdeel van de kwartaalrapportage. 8. Toelichting op beschikbaarheidsoverzicht:
eis -303	Leverancier voorziet in de beschikbaarheidsrapportages in zowel de onbeschikbaarheid die de Leverancier is toe te rekenen als de onbeschikbaarheid die de Leverancier niet is toe te rekenen.
eis -304	<p>Per kwartaal dient Leverancier een overzicht te overleggen van alle verrichte werkzaamheden in het kader van Beheer en onderhoud. In het vierde kwartaal dient tevens een jaarrapportage te worden geleverd.</p> <p>In dit overzicht dient in ieder geval opgenomen te zijn:</p>

	<ol style="list-style-type: none"> 1. Overzicht van door gebruiker gemelde storingen. 2. Overzicht van door het monitoringsysteem gemelde storingen. 3. Overzicht percentage beschikbaarheid per component die onder monitoring valt. 4. Overzicht van gerealiseerde hersteltijd per storing, gemiddelde hersteltijd. 5. Overzicht van storingen die niet binnen de contractuele oplostijden zijn opgelost en de genomen tijdelijke maatregelen. Percentage storingen opgelost buiten de contractuele oplostijden opgesplitst naar geëist beschikbaarheidspercentage. 6. Van componenten die vaker dan één keer per kwartaal een storing vertonen de gemiddelde tijd tussen storingen en het aantal storingen in het afgelopen half jaar. 7. Uitgevoerde werkzaamheden ten behoeve van preventief onderhoud. 8. Uitgevoerde werkzaamheden ten behoeve van correctief onderhoud. 9. Overzicht van nieuw geïnstalleerde Hardware en Software. 10. Spare-parts die zijn gebruikt en voor welke storing/project en of het vervangen onderdeel nog garantie had. 11. Actuele lijst van spare-parts. 12. Veiligheidsissues (waaronder: veiligheidsupdates apparatuur, ...)
eis -305	<p>Jaarlijks, bij de rapportage over het tweede kwartaal, dient de Leverancier een voorstel in voor het vervangen van onderdelen en componenten voor het jaar erop. Dit voorstel wordt door Contractpartner beoordeeld, onder meer aan de hand van de rapportage over storingen en de ouderdom van de apparatuur. Vervanging van apparatuur, zowel binnen dit als binnen het vorige contract geleverd, is alleen mogelijk bij een leeftijd van 8 jaar. Na goedkeuring door Contractpartner van het voorstel zal Leverancier een Offerte opstellen tegen de vastgestelde eenheidsprijzen.</p> <p>Indien door Opdrachtnemer aangetoond kan worden dat, bijvoorbeeld door intensief gebruik of omgevingsinvloeden, een component eerder dan de genoemde 8 jaar aan vervanging toe is dan zal Opdrachtgever dit serieus in overweging nemen en hierin in redelijkheid mee omgaan. Ook indien een component end-of-life en end-of-support gaat worden, dient de Opdrachtnemer dit tijdig aan te geven en met een voorstel tot vervanging ervan te komen.</p>
eis -306	<p>Contractpartner wil op elk moment inzicht hebben in alle op dat moment openstaande storingen en welke Camera's of onderdelen dat betreft. Deze informatie dient gestructureerd te worden gepresenteerd wat impliceert dat relevante informatie niet alleen in een veld met vrije tekst wordt beschreven. Het moet eenvoudig te achterhalen zijn welke Camera's en welke onderdelen noodzakelijk voor de toezichtstaak (bijv. uitkijkplekken) niet of gestoord beschikbaar zijn. Idealiter wordt informatie grafisch gepresenteerd. Op dit moment is daarvoor een dashboard vanuit de huidige leverancier.</p> <p>Bijvoorbeeld: indien een netwerkverbinding is gestoord waarmee 40 camera's met de CCTR zijn verbonden dan dient in één oogopslag duidelijk te zijn dat deze 40 camera's niet uit kunnen worden gekeken.</p>

10.7 Garantie

eis -307	Er dient garantie te worden gegeven op alle nieuw te installeren Hardware. De garantietermijn voor de fabrieksgarantie is ten minste één jaar.
eis -308	<p>Inschrijver maakt in de offerte duidelijk wat de eenmalige meerkosten zijn om de garantie te verhogen tot de volgende periodes:</p> <ul style="list-style-type: none"> • Harde schijven: 2 jaar. • Monitors: 3 jaar. • Camera's 5 jaar. • Clients en servers, incl. alle bijbehorende interne componenten: 5 jaar.
eis -309	Garantietermijnen langer dan de fabrieksgarantie vervalt bij beëindiging van het contract. De fabrieksgarantie vervalt niet bij beëindiging van het contract.
eis -310	Gedurende de garantieperiode zijn alle diagnose-, transport-, reparatie- en/of vervangingskosten incl. uren en voorrijkosten, plaatsing hoogwerker, verkeersmaatregelen, etc. voor rekening van de Leverancier.

10.8 Documentatie

eis -311	<p>De as-builtonformatie van het Cameratoezichtstelsel dient actueel te zijn en na elke wijziging moet de as-builtonformatie binnen één maand aangepast worden en beschikbaar worden gesteld aan de Contractpartner. Indien blijkt dat de as-builtonformatie niet actueel is, is de boeteclausule van toepassing tot aan het moment dat de Leverancier de up-to-date documentatie oplevert.</p> <p>Het bijwerken van as-builtondocumentatie n.a.v. een Aanpassing is een standaard verplichting van de Leverancier.</p>
eis -312	De as-builtonformatie wordt digitaal beschikbaar gesteld als doorklikbare webpagina's. Webpagina's zijn onderling via hyperlinks verbonden zodat snel gerelateerde informatie kan worden gevonden. De as-builtonformatie zal lokaal bij Contractpartner worden gehost. Elk kwartaal wordt een volledige up-to-date versie van de as-builtonformatie beschikbaar gesteld en na elke projectoplevering.
eis -313	De brondocumenten van de as-builtondocumentatie zijn nadrukkelijk ook onderdeel van de as-built. Bijvoorbeeld: Excel-documenten met daarin tabelinformatie die vervolgens is omgezet naar webpagina's of pdf in de uiteindelijke as-built worden mede opgeleverd. Hiermee wordt Contractpartner in staat gesteld om na looptijd van het contract een nieuwe partij de documentatie in beheer te laten nemen. Leverancier mag ervan uitgaan dat de brondocumenten van de huidige as-built beschikbaar worden gesteld.
eis -314	Onderdeel van de as-built zijn kaartgegevens met daarop de posities van de Camera's. Het is mogelijk via de kaart de gerelateerde componentpagina's in de as-built te vinden. Politiecamera's dienen met een andere kleur dan de gemeentelijke camera's te worden weergegeven.
eis -315	Onderdeel van de as-built en het exit-plan is een duidelijke beschrijving waar en hoe het Camerastelsel afhankelijk is van infrastructuur van Leverancier. Het doel hiervan is voor Contractpartner inzichtelijk te maken waar problemen kunnen ontstaan indien een nieuwe leverancier het stelsel in beheer dient te nemen.
eis -316	Onderdeel van de as-built zijn schematische tekeningen van de door de leverancier geïnstalleerde

	<p>installatie, waaronder:</p> <ul style="list-style-type: none"> • Overzichtstekeningen. • Kaarten met daarop locaties van Camera's, draadloze verbindingen (per frequentie een eigen kleur of andere opvallende markering), PoP-locaties en uitkijklocaties. • Aansluit- en bekabelingstekeningen. • Logische schema's. • Indeling van de systeemkasten.
eis -317	<p>Van elke component met een eigen IP-adres wordt in de as-built de volgende informatie gespecificeerd:</p> <ul style="list-style-type: none"> • Naam. • Merk en type. • Objectcode waar het component onderdeel van is. • IP-informatie en MAC-adres. • Interfacemode/IP-adres/subnet-mask/gateway. • Softwareversie en/of Firmware-versie. • Relevante configuratiesettings. • Wijze van verbinding met de uitkijkcentrale en relevante bijbehorende gegevens zodat storingsen door Leverancier te coördineren zijn. • Installatiedatum • Foto(s) (in hoge resolutie) van de installatie incl. bijbehorende randapparatuur (bijv. junctionbox bij een Camera). • Locatie, bijv. ruimte en kastnummer bij interne plaatsing, adres en GPS-coördinaten bij plaatsing in de openbare ruimte. • Stroomvoorziening. Bij aparte Liander-stroomvoorziening dient de EAN-code vermeld te worden. • Contactpersoon en aandachtspunten m.b.t. toegankelijkheid.
eis -318	<p>Leverancier is verantwoordelijk voor het up-to-date houden van contactpersonen, aandachtspunten m.b.t toegankelijkheid van bijvoorbeeld gebouwen of objecten en andere zaken (minimaal jaarlijks bij een servicebeurt op locatie wordt dit gecheckt). Deze up-to-date- gegevens staan ook in de as-built of een andere lijst die minimaal jaarlijks ook naar de betreffende opdrachtgever(s) wordt verstuurd.</p>
eis -319	<p>Bij Camera's zijn relevante en te documenteren configuratie-instellingen per uitgezonden Camerastream ten minste de resolutie, framerate, wel of geen versleuteling van de verbinding en bandbreedte-gebruik.</p>
eis -320	<p>Onderdeel van de as-built is documentatie van het netwerk, zowel laag 2 als laag 3, IP-plan, gebruikte VLANs, segmentering van het netwerk, en alle andere relevante informatie.</p>
eis -321	<p>Onderdeel van de as-built is een accuraat overzicht van alle lopende onderhoudslicenties, incl. einddatum, op VMS en alle andere relevante componenten.</p>
eis -322	<p>De wachtwoorden en codes waarmee informatie is versleuteld van het systeem zijn geen onderdeel van de as-built. <u>Alle</u> wachtwoorden en codes worden in een aparte, gedateerde en verzegelde envelop aangeleverd en beschikbaar gesteld aan de politie. Met deze wachtwoorden moet een eventuele nieuwe beherende partij in staat zijn alle beheertaken op zich te nemen.</p> <p>De wachtwoorden zijn door Contractpartner zonder opgaaf van redenen op te vragen. Contractpartner zal hier echter alleen gebruik van maken indien dit strikt noodzakelijk is voor het</p>

	operationeel houden van het systeem.
eis -323	Bij tussentijdse aanpassing van wachtwoorden wordt binnen één week een nieuwe envelop met alle actuele wachtwoorden en codes in depot gegeven. Bij het niet tijdig bijwerken van de envelop met wachtwoorden is de boeteclausule van toepassing.
eis -324	<p>Als onderdeel van de as-built is er een separate overzichtstabel (MS Excel) voor snel overzicht van alle Camera's, verbindingen, werkplekken en servers beschikbaar. Dit overzicht wordt bij elke aanpassing geactualiseerd binnen één week. Van elke Camera dient het volgende te worden gespecificeerd:</p> <ul style="list-style-type: none"> • Referentienummer camera. • IP-adres. • Objectcode. • Stadsdeel en projectnaam. • Opdrachtgever • Prioriteitsstelling (indien van toepassing) • Merk en type. • Datum installatie. • Opnameduur. • Locatie gespecificeerd als XY-coördinaten verkregen via een GPS-meting. • Adres en postcode.
eis -325	Van elke actieve component wordt de fabrieksdokumentatie aan de as-built toegevoegd (handleiding en specsheet). In de as-built is er een overzichtspagina waarmee bij merk en type een doorklikbare referentie naar deze documenten gevonden kan worden.
eis -326	De gebruikershandleidingen worden in de Nederlandse taal aangeleverd. Technische documentatie mag in de Engelse taal gesteld zijn.

11 Uitstootvrij vervoer en transport

11.1 Algemeen

eis -327	<p>Voor de vervoers- en transportbewegingen ten behoeve van de uitvoering van de Raamovereenkomst gelden de volgende milieueisen voor gemeente Amsterdam:</p> <ul style="list-style-type: none">· Vanaf start Overeenkomst binnen de ring A10 zijn vervoerscategorieën:<ol style="list-style-type: none">a. M1 en N1 (tot 3.500 kg) verplicht uitstootvrij;b. M2 en N2 (3.500 tot 12.000 kg) verplicht uitstootvrij en;c. N3 en M3 (vanaf 12.000kg) verplicht EUROVI. <p>Uitstootvrij betekent zonder uitlaatmissie van broeikasgassen, verontreinigende gassen en deeltjes. Dit geldt voor alle voertuigcategorieën, tenzij het bijzondere voertuigen betreft die in aanmerking komen voor ontheffing. Openbaar vervoer wordt ook gezien als uitstootvrij.</p> <p>Opdrachtnemer kan voor de uitvoering van deze eis bijvoorbeeld gebruik maken van hubs buiten de ring: Logistieke hubs</p> <p>Informatie over beschikbare laadpalen en aansluitingen is te vinden via www.stroomkaart.nl, waarop de meeste gemeentelijke aansluitingen en laadpunten inzichtelijk zijn.</p> <p>Indien tijdens de overeenkomst de eisen aangescherpt worden, dan zal de Opdrachtnemer zich conformeren aan de nieuwe eisen.</p>
----------	--

12 Ketenverantwoordelijkheid

12.1 Algemeen

De gemeente Amsterdam streeft ernaar misstanden op het gebied van arbeidsomstandigheden, mensenrechten en milieu in de toeleveringsketen zoveel mogelijk te voorkomen. Dit wordt aangeduid als ketenverantwoordelijkheid. Een belangrijk instrument hiervoor zijn de Internationale Sociale Voorwaarden (ISV). De gemeente verwacht van opdrachtnemers dat zij inzicht hebben in hun toeleveringsketens en transparant zijn over de herkomst van materialen en producten. Via een due diligence-proces beoogt de ISV de naleving van internationale arbeidsnormen en mensenrechten in de productieketens van leveranciers te bevorderen. Due diligence houdt in dat bedrijven inspanningen verrichten om negatieve impact in hun ketens te voorkomen, te stoppen of te beperken (op het gebied van schendingen van arbeidsnormen, mensenrechten en milieu).

Voor deze aanbesteding worden de Internationale Sociale Voorwaarden specifiek opgenomen voor camerasystemen. Camerasystemen vallen binnen de door de gemeente aangeduide risicocategorieën vanwege complexe mondiale toeleveringsketens in de productie van optische sensoren en halfgeleiders, risico's op mensenrechtenschendingen door betrokkenheid van bepaalde fabrikanten bij surveillance en etnisch profileren, arbeidsintensieve processen bij de productie van camera's en bijbehorende hardware, en het gebruik van zeldzame metalen en gevaarlijke chemicaliën bij de vervaardiging van elektronische componenten.

eis -328	Door in te schrijven op deze aanbesteding committeert de inschrijver zich aan het naleven van de ISV, gericht op de keten van camerasystemen en bijbehorende componenten.
eis -329	<p>De Internationale Sociale Voorwaarden (ISV) dragen bij aan het uitbannen van sociale misstanden in de toeleveringsketen, zoals kinderarbeid, hongerlanden en onmenselijke arbeidsomstandigheden. Via een due diligence-proces beoogt de ISV de naleving van internationale arbeidsnormen en mensenrechten in de productieketens van leveranciers te bevorderen.</p> <p>Opdrachtnemer dient in dit kader een due diligence-proces uit te voeren conform het onderstaande:</p> <p>1. Transparantie</p> <p>Binnen 6 maanden na de gunning van het contract zal de opdrachtnemer redelijke en evenredige inspanningen verrichten om de aanbestedende dienst te voorzien van informatie over specifieke productielocaties in de toeleveringsketen van de via het contract aangeschafte goederen. Deze informatie dient te worden verstrekt in het door de aanbestedende dienst gevraagde format en moet de wettelijke naam en volledige fysieke adressen van de productielocaties bevatten.</p> <p>De specifieke productielocaties waarover informatie moet worden verstrekt zijn die waar respectievelijk de ontwikkeling en productie van firmware en software, de fabricage van optische sensoren en halfgeleiders, de productie van elektronische componenten en printplaten, en de</p>



assemblage van de camerasystemen plaatsvinden.

2. Risicoanalyse productieketen camerasystemen

Niet later dan 9 maanden na de definitieve gunning van het contract dient de opdrachtnemer een risicoanalyse te verstrekken met betrekking tot de gehele keten van het productieproces, waaronder:

Een analyse van de risico's op schending van arbeids- en mensenrechten in de keten van camerasystemen. Waar mogelijk, onderscheid risico's per niveau - voor drie niveaus: grondstofwinning (zeldzame metalen, silicium), productie van optische sensoren, halfgeleiders en elektronische componenten, en assemblage van de camerasystemen inclusief ontwikkeling van firmware. Voeg een toelichting toe over de gebruikte bewijsbronnen en hoe verschillende actoren in de toeleveringsketen, waaronder rechthebbenden, vakbonden en andere belanghebbenden, hebben deelgenomen aan het proces.

3. Plan van aanpak mitigeren risico's

Niet later dan 9 maanden na de definitieve gunning van het contract dient de opdrachtnemer een actieplan te verstrekken om de in de risicoanalyse geïdentificeerde risico's te beperken.

Het actieplan dient te omvatten:

- Een overzicht en beschrijving van de inspanningen die de opdrachtnemer zal verrichten om de risico's te beperken;
- Een tijdschema betreffende de inspanningen die de opdrachtnemer zal verrichten;
- Een toelichting over hoe het actieplan is ontwikkeld, bijvoorbeeld informatie over betrokkenheid van belanghebbenden;
- Een toelichting over hoe de impact van het actieplan zal worden beoordeeld, inclusief informatie over de rol van belanghebbenden in dat proces, hoe middelen voor het actieplan worden verstrekt: aantal medewerkers, hun expertise en hun training;
- Een beschrijving van hoe belanghebbenden, waaronder rechthebbenden en vakbonden, betrokken zullen worden bij het herstelproces voor eventuele negatieve mensenrechteneffecten op rechthebbenden in de toeleveringsketen tijdens de uitvoering van het contract.

Als de opdrachtnemer is aangesloten bij een IMVO (Internationaal Maatschappelijk Verantwoord Ondernemen) sectorconvenant, kan dit worden gezien als een actie om de risico's in zijn keten te verminderen. De opdrachtnemer kan dit in het actieplan vermelden als onderdeel van een bredere aanpak van risicovermindering in lijn met de OESO-richtlijnen. Ook als de opdrachtnemer zich heeft aangesloten bij een keteninitiatief, kan dit in het actieplan worden gerapporteerd. Dit betekent echter niet dat de opdrachtnemer daarmee aan alle due diligence-verplichtingen voldoet. De opdrachtnemer moet controleren of het keteninitiatief alle risico's dekt. Als wordt vastgesteld dat dit niet het geval is, zal de opdrachtnemer in zijn actieplan moeten specificeren welke inspanningen zullen worden verricht om de (resterende) risico's te beperken.

Naleving van het plan zal gedurende de looptijd van het contract worden geëvalueerd, met een focus



op continue verbetering en toewijding aan een voortdurende dialoog over mensenrechten en due diligence. De aanbestedende dienst hanteert een samenwerkingsbenadering die leveranciers aanmoedigt om eerlijk en transparant te zijn over uitdagingen en knelpunten in hun toeleveringsketen, zonder dat dit leidt tot contractuele sancties of negatieve beoordeling.

4. Jaarlijkse rapportage

Gedurende de contractperiode dient de opdrachtnemer jaarlijks vanaf de startdatum van de overeenkomst (of in het geval van een overeenkomst met kortere looptijd: bij afronding daarvan) te rapporteren over zijn inspanningen met betrekking tot de naleving van de ISV. Dit moet aantonen dat de opdrachtnemer een 'redelijke inspanning' heeft geleverd om aan de ISV te voldoen.

Het rapport wordt in twee versies opgesteld:

- Een openbare versie gepubliceerd op de website van de opdrachtnemer, al dan niet als onderdeel van een breder rapport zoals een (duurzaamheids)jaarverslag.
- Een interne versie met meer details voor gebruik door de aanbestedende dienst.
- Beide rapporten moeten duidelijk het verband aantonen tussen het onderwerp van het contract en de gerapporteerde activiteiten, aangezien deze verbinding essentieel is voor de waarde van de informatie.
- Het openbare rapport dient ten minste de volgende hoofdpunten te bevatten:
- Een samenvatting van de risicoanalyse zoals beschreven onder 2;
- De belangrijkste maatregelen die in het gerapporteerde jaar zijn genomen om risico's te verminderen en eventuele schendingen van de ISV in de keten te verhelpen;
- De aanpak en belangrijkste resultaten van het monitoren van de naleving van de ISV;
- Algemene informatie over hoe eventueel ontvangen signalen (intern en extern) over schending van de ISV zijn behandeld.

De interne versie voor de aanbestedende dienst bevat meer gedetailleerde informatie over de bovenstaande punten. Het rapportageformat is vrij, maar moet voor de bruikbaarheid in het Nederlands of Engels zijn.

Bij de invulling van deze verplichtingen dient opdrachtnemer uit te gaan van:

- de handreiking due diligence voor bedrijven, zoals raadpleegbaar via de handreiking due-diligence voor bedrijven
- Opdrachtnemer kan daarnaast ook gebruik maken van onderstaande informatie en handreikingen:
- PIANOo website over internationale sociale voorwaarden;
- OESO due diligence handreiking voor maatschappelijk verantwoord ondernemen;
- RBA Practical Guide.