Bijlage 5 Programma van eisen

Het is de verantwoordelijkheid van de Opdrachtnemer dat de door of namens hem te verrichten Diensten op vakbekwame wijze worden uitgevoerd. Bepaalde werkzaamheden acht de Opdrachtgever echter zodanig van belang voor het resultaat van de dienstverlening of voor eigen activiteiten, dat de Opdrachtgever aan die werkzaamheden eisen heeft gesteld. Deze eisen zijn opgenomen in de voorliggende bijlage.

Door het indienen van een Inschrijving gaat Inschrijver uitdrukkelijk akkoord met alle eisen en voorwaarden die in dit document zijn neergelegd en verklaart Inschrijver dat hij gedurende de gehele uitvoeringsperiode van de gesloten Raamovereenkomst aan deze eisen zal blijven voldoen.

Wanneer gedurende de contractduur blijkt dat een of meer van de onderstaande eisen niet (meer) behaald kunnen worden en dit te wijten valt aan de Opdrachtnemer, herstelt de Opdrachtnemer de situatie zodanig dat alsnog (weer) aan de eis(en) wordt voldaan. De hieraan direct of indirect te relateren kosten zijn volledig voor rekening van de Opdrachtnemer.

In deel 1 staan alle eisen t.a.v. dienstverlening zoals beschreven in de scope in de Inschrijfleidraad onder paragraaf 2.4.

In deel 2 staan eisen die nu al zijn meegenomen t.a.v. dienstverlening onder de herzieningsclausule zoals in de Inschrijfleidraad onder paragraaf 2.6.

Deel 1: onderdeel van de scope

Nr.	Algemene eisen / bepalingen
1.	Gestelde eisen en voorwaarden gelden voor alle locaties van Rijnland. Bij wijziging(en) in locatie(s), door bijvoorbeeld het toevoegen en/of vervallen van kantoorhuisvesting of installaties, blijven deze eisen en voorwaarden ongewijzigd.
2.	Opdrachtnemer beschikt gedurende de looptijd van de Raamovereenkomst over alle voor de uitvoering vereiste vergunningen (een Nederlands dienstnummer), registraties en toelatingen voor particuliere beveiligingsorganisaties en voldoet aantoonbaar aan de geldende eisen uit wet- en regelgeving voor particuliere beveiliging zoals de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr) en Regeling particuliere beveiligingsorganisaties en recherchebureaus (Rpbr).
3.	Opdrachtnemer past de voor de werkzaamheden geldende cao correct toe en kan dit op verzoek aantonen. Indien Opdrachtnemer is gecontroleerd door het Sociaal Fonds Particuliere Beveiliging dient het bedrijfsoordeel voldoende te zijn. Indien sprake is van een onvoldoende beoordeling, dient opdrachtnemer aantoonbaar doeltreffende zelfreinigende maatregelen te hebben genomen. De doeltreffendheid van deze maatregelen kan aangetoond worden door een verklaring van het Sociaal Fonds Particuliere Beveiliging.

4.	Alle ingezette medewerkers en onderaannemers zijn contractueel gehouden tot geheimhouding van vertrouwelijke informatie. De Opdrachtnemer ontvangt een Geheimhoudingsovereenkomst (bijlage12) voor ondertekening en dient die na te leven. Tevens draagt Opdrachtnemer zorg dat, voordat een onderaannemer wordt ingezet, ook deze de geheimhoudingsovereenkomst van HHR heeft getekend en retour gedaan aan HHR. Deze verplichting geldt eveneens voor stagiaires, uitzendkrachten en overige door Opdrachtnemer ingezette derden.
5.	Opdrachtnemer beschikt gedurende de gehele contractperiode over een geldig en toereikend ISO 27001-certificaat. Opdrachtgever behoudt zich het recht voor de geldigheid hiervan gedurende de looptijd van de Raamovereenkomst te verifiëren. Opdrachtnemer is gehouden hieraan zijn medewerking te verlenen. HHR aanvaardt gelijkwaardige certificaten van in andere lidstaten van de Europese Unie gevestigde instanties.
6.	Opdrachtnemer beschikt gedurende de gehele contractperiode over een geldig ISO 9001-certificaat. Opdrachtgever behoudt zich het recht voor de geldigheid hiervan gedurende de looptijd van de Raamovereenkomst te verifiëren. Opdrachtnemer is gehouden hieraan zijn medewerking te verlenen. HHR aanvaardt gelijkwaardige certificaten van in andere lidstaten van de Europese Unie gevestigde instanties.
7.	Inzet van onderaannemers is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Opdrachtgever. Op een onderaannemer mogen geen uitsluitingen op grond van de Aanbestedingswet 2012 van toepassing zijn, zoals verwoord in paragraaf 3.2.1 van de Inschrijvingsleidraad. Opdrachtnemer blijft gedurende de gehele looptijd van de Raamovereenkomst integraal verantwoordelijk voor kwaliteit, aansturing, uitvoering en continuïteit van de onderaannemer.
8.	Opdrachtnemer komt in het bezit van de benodigde sleutel(s), toegangspassen, resetcodes en een gebruiksvoorschrift voor de elektronische beveiligingssystemen (brandmelding, inbraakdetectie en toegangscontrole hierna: “middelen”)) van de te beveiligen locaties. Opdrachtnemer dient voor ontvangst van deze middelen een uitgifteformulier voor toegangsmiddelen te ondertekenen. Opdrachtnemer is verantwoordelijk voor het instrueren van haar medewerkers in het juiste gebruik van de verstrekte middelen en beveiligingssystemen voordat zij zelfstandig werkzaamheden uitvoeren. Opdrachtnemer draagt zorg voor een aantoonbaar en deugdelijk beheer van alle in bruikleen verstrekte middelen. Indien deze middelen niet bij Opdrachtnemer in gebruik zijn, worden zij bewaard in een afgesloten sleutelkluis of gelijkwaardige beveiligde voorziening. Indien sleutels of toegangsmiddelen worden meegenomen in voertuigen, worden zij opgeborgen in een afgesloten en tegen diefstal beveiligde voorziening.

	Toegang tot sleutels en toegangsmiddelen is beperkt tot geautoriseerde medewerkers.
9.	Opdrachtnemer dient ervoor te zorgen dat de ter beschikking gestelde toegangsmiddelen niet in onbevoegde handen kunnen komen en neemt passende maatregelen om verlies, diefstal, misbruik of ongeautoriseerd gebruik te voorkomen. Opdrachtgever stelt Opdrachtnemer volledig aansprakelijk voor schade die is ontstaan als gevolg van onbevoegd, onvoorzichtig of nalatig handelen of gebruik, dan wel door opzet of grove schuld van Opdrachtnemer of diens Personeel.
10.	Opdrachtnemer dient binnen 24 uur nadat hij een verlies, diefstal, (vermoedelijke) compromittering van toegangsmiddelen, ongeautoriseerde kopieën of ongeautoriseerd gebruik van sleutels, toegangspassen, resetcodes of andere toegangsmiddelen heeft geconstateerd, dan wel daarvan redelijkerwijs op de hoogte had behoren te zijn, hiervan melding te maken bij fysiekebeveiliging@rijnland.net. Bij diefstal doet Opdrachtnemer onverwijld aangifte bij de politie en informeert Opdrachtgever binnen 24 uur telefonisch en per e-mail. Op verzoek van Opdrachtgever verstrekt Opdrachtnemer een afschrift van de aangifte. In geval van verlies, diefstal, misbruik, compromittering of onbevoegd gebruik van sleutels, toegangspassen, resetcodes of andere toegangsmiddelen komen alle noodzakelijke kosten voor rekening van Opdrachtnemer. Hieronder vallen onder meer (maar niet beperkt tot): de kosten voor het vervangen van sloten, sleutels, toegangspassen en overige beveiligingsmaatregelen die Opdrachtgever noodzakelijk acht om de beveiliging van locaties, gebouwen, installaties of systemen te herstellen of te waarborgen.
11.	Indien geconstateerde gebreken de veiligheid van het object of pand in het geding brengen, neemt Opdrachtnemer onverwijld contact op met de contactpersoon van Opdrachtgever. Partijen bepalen in overleg welke maatregelen noodzakelijk zijn en dragen zorg voor de uitvoering daarvan.
12.	Opdrachtgever wil Opdrachtnemer de mogelijkheid geven studenten c.q. leerlingen van beveiligingsopleidingen, onder begeleiding, relevante ervaring op te laten doen op haar locaties. Voorwaarde is dat maximaal ~~één~~ twee stagiaires per locatie en uitsluitend boven de sterkte mag worden ingezet onder volledige begeleiding van Opdrachtnemer en na instemming van Opdrachtgever. De inzet van een stagiaire dient minimaal ~~één maand~~ 2 weken voor aanvang door Opdrachtnemer aan Opdrachtgever te worden voorgelegd onder opgave van de stageperiode, uit te voeren werkzaamheden en begeleider. De stagiaire is vóór aanvang van de werkzaamheden schriftelijk tot geheimhouding verplicht. Opdrachtnemer blijft volledig verantwoordelijk voor het handelen en nalaten van de stagiaire.

13.	Opdrachtnemer verleent op eigen kosten volledige medewerking aan een ordelijke overdracht naar opvolgende partij gedurende de laatste twee maanden van de Raamovereenkomst.

Nr.	Eisen ten aanzien van de uitvoering van meldkamerdiensten
14.	Opdrachtnemer zorgt bij wijzigingen tijdens de contractperiode dat door de Opdrachtgever nieuw aangeleverde instructies, tijdroosters en contactadressen uiterlijk binnen vijf (5) werkdagen na ontvangst zijn verwerkt in de systemen van Opdrachtnemer en beschikbaar zijn voor geautoriseerde meldkamercentralisten en beveiligers. Opdrachtnemer draagt zorg dat alleen geautoriseerde medewerkers op need to know basis toegang hebben tot deze informatie.
15.	Opdrachtnemer maakt, de in haar systemen vastgelegde instructies, tijdroosters en contactadressen digitaal inzichtelijk voor Opdrachtgever. Opdrachtgever heeft toegang tot het door Opdrachtnemer gebruikte systeem of portaal waarin deze gegevens zijn vastgelegd, zodat controle op actualiteit en juistheid mogelijk is. De toegang voor Opdrachtgever is gedurende de looptijd van de Raamovereenkomst beschikbaar en wordt op passende wijze beveiligd.
16.	De dienstverlening op alarmdiensten wordt elke kalenderdag, 24 uur per dag verzorgd. Opdrachtnemer waarborgt te allen tijde de continuïteit en beschikbaarheid van deze dienstverlening.
17.	In geval van uitval van een systeem of meerdere systemen binnen de meldkamer beschikt Opdrachtnemer over een aantoonbaar werkende back-up- en uitwijkvoorziening zodat de dienstverlening zonder onderbreking kan worden voortgezet. Opdrachtnemer waarborgt dat de continuïteit en beschikbaarheid van de dienstverlening te allen tijde zijn geborgd. Opdrachtnemer test deze voorziening minimaal jaarlijks en verstrekt de resultaten hiervan op verzoek aan Opdrachtgever.
18.	Storingen in systemen die invloed hebben op de dienstverlening worden onverwijld gemeld aan Opdrachtgever via fysiekebeveiliging@rijnland.net. Hierbij wordt tevens aangegeven wat de impact is, welke tijdelijke beheersmaatregelen zijn getroffen en wat de verwachte hersteltijd is.
19.	Opdrachtnemer bewaakt de verbinding naar de inbraakalarmsystemen van de Opdrachtgever en brengt Opdrachtgever onmiddellijk op de hoogte indien deze verbinding niet functioneert. Zie protocol in Bijlage 15.
20.	Opdrachtnemer behandelt en volgt inbraakmeldingen en service/storingsmeldingen van de inbraakalarmsystemen en brandmeldingen van de brandalarmsystemen op volgens een door Opdrachtgever vastgestelde instructie (Bijlage 15). Afwijkingen van de vastgestelde instructies worden vastgelegd en gemeld aan Opdrachtgever. Het staat de Opdrachtgever vrij om de instructie gedurende de contractperiode te wijzigen in overleg met de Opdrachtnemer.

Nr.	Eisen ten aanzien van alarmopvolging
21.	Opdrachtnemer draagt zorg dat minimaal 80% van de Prio 1-meldingen binnen de responstijd van 30 minuten wordt opgevolgd en minimaal 70% van de Prio 2-meldingen binnen de responstijd van 45 minuten. Deze percentages en tijden zijn KPI's waarop de bonus-malusregeling van toepassing is. De responsetijd start nadat het alarmsignaal is binnengekomen bij de alarmcentrale en eindigt op het moment dat de medewerker van Opdrachtnemer op de betreffende locatie aanwezig is en de opvolging daadwerkelijk kan aanvangen. Opdrachtnemer registreert per melding het tijdstip van ontvangst van het alarmsignaal en het tijdstip waarop de medewerker ter plaatse is. Deze registratie wordt gebruikt voor de beoordeling van de KPI's en wordt op verzoek aan Opdrachtgever verstrekt.
22.	Opdrachtnemer draagt zorg dat minimaal 80% van de responsetijd van 30 minuten Prio 1-meldingen wordt behaald en 70% van de responstijd van prio 2- meldingen. Deze percentages en tijden zijn KPI’s waarop de bonus-malus regeling op van toepassing is. De KPI’’s worden beoordeeld op kwartaal-basis op basis van aangeleverde rapportages door de Opdrachtnemer (zie ook verder eis 127 voor invulling).
23.	Indien Opdrachtnemer zich beroept op overmacht, gelden uitsluitend de voorwaarden, procedures en rechtsgevolgen zoals opgenomen in de Raamovereenkomst en de AWVODI 2018. Opdrachtnemer stelt Opdrachtgever onverwijld schriftelijk op de hoogte van de overmachtssituatie en verstrekt desgevraagd alle informatie en bewijsstukken die redelijkerwijs nodig zijn om het beroep op overmacht te kunnen beoordelen. Indien vaststaat dat het niet behalen van een KPI rechtstreeks en aantoonbaar het gevolg is van een geslaagd beroep op overmacht, kan Opdrachtgever besluiten de betreffende gebeurtenis buiten beschouwing te laten bij de beoordeling van de KPI's. De bewijslast van het beroep op overmacht rust op Opdrachtnemer.
24.	Indien na kantoortijd (zie Bijlage 15 voor protocol) door de surveillant bij een alarmopvolging bijzonderheden worden geconstateerd (zoals schade door bijvoorbeeld inbraak) wordt telefonisch contact opgenomen met de wachtdienst van Opdrachtgever. In overleg met de wachtdienst van Opdrachtgever worden de noodzakelijke hulpdiensten ingeschakeld of gepaste acties ondernomen.
25.	De surveillant van Opdrachtnemer blijft bij het object totdat er voldoende maatregelen zijn genomen om de veiligheid van het object te garanderen: • de oorzaak van het incident is vastgesteld; • noodzakelijke nood- en beveiligingsmaatregelen zijn getroffen om onbevoegde toegang, verdere schade of escalatie te voorkomen. Dit gebeurt in overleg met Opdrachtgever.
26.	De surveillant van Opdrachtnemer heeft toegang tot actuele objectgegevens, adressen, GPS-coördinaten, toegangsroutes, contactgegevens en locatie-specifieke veiligheidsinstructies aangeleverd door Opdrachtgever en verwerkt in het systeem van Opdrachtnemer en mag dit uitsluitend gebruiken voor de uitvoering van de Raamovereenkomst.

27.	Surveillant beschikt minimaal over: • mobiele telefoon; • portofoon of redundante communicatie; • zaklamp; • de voor de uitvoering noodzakelijke sleutels, toegangspassen en overige toegangsmiddelen; • een geldig legitimatiebewijs en, voor zover wettelijk vereist, een beveiligingslegitimatiebewijs.

Nr.	Eisen ten aanzien van brand- en sluitrondes
28.	Opdrachtnemer dient de brand- en sluitronde uit te voeren conform de instructie (Bijlage 16) en binnen het door Opdrachtgever vastgestelde tijdsvenster zoals opgenomen in de werkinstructie. Aan het einde van de ronde wordt de alarmering ingeschakeld. De beveiliger legt bevindingen en bijzonderheden vast in de rapportage van de brand- en sluitronde.
29.	Het staat de Opdrachtgever vrij om gedurende de contractperiode de instructie te wijzigen in overleg met de Opdrachtnemer. Opdrachtnemer verleent hieraan alle redelijkerwijs noodzakelijke medewerking. Voor zover de wijziging past binnen de aard en scope van de Raamovereenkomst, is Opdrachtnemer niet gerechtigd hiervoor aanvullende kosten in rekening te brengen.
30.	Brandgevaarlijke situaties die binnen de bevoegdheden van de beveiliger vallen, dienen direct te worden weggenomen. Indien dit niet mogelijk is, dient de situatie direct te worden gemeld aan Opdrachtgever, zijnde de wachtdienst van gebouwenbeheer, en worden passende tijdelijke maatregelen getroffen om het risico te beperken. Andere risico's, zoals ballonnen en overige versieringen in nabijheid van bewegingsmelders, risico op onrechtmatig toetreden en vandalisme, dienen eveneens te worden opgenomen in de rapportage van de brand- en sluitronde.
31.	Op verzoek van Rijnland voert Opdrachtnemer extra sluitrondes uit.

Nr.	Eisen ten aanzien van openen, surveilleren en suppoostwerkzaamheden op verzoek
32.	Opdrachtnemer is in staat 24 uur per dag op verzoek van Opdrachtgever locaties te openen en is binnen 45 minuten, gerekend vanaf moment van contact, aanwezig. Bij aanvang van de Raamovereenkomst betreft het alleen het hoofdkantoor aan de Archimedesweg.
33.	Bij openen van een object worden de in de werkinstructie aangewezen toegangspunten geopend, onregelmatigheden gecontroleerd, systemen bediend en afwijkingen direct gemeld aan de contactpersoon van de locatie.
34.	De beveiliger of een vervanger die er later bij komt, blijft tot de werkzaamheden zijn volbracht en het pand weer kan worden afgesloten, tenzij in overleg met Opdrachtgever anders wordt besproken.

35.	Opdrachtgever heeft incidenteel evenementen met meer dan 50 bezoekers waarvoor extra beveiliging wordt ingezet. Een voorbeeld hiervan is suppoostwerkzaamheden bij de Open Monumentendag.
36.	Beveiligers handelen aantoonbaar conform de wettelijke eisen, locatie-specifieke instructies, huisregels en veiligheidsprotocollen.
37.	Opdrachtnemer beschikt over een centraal meldpunt voor verzoeken voor openen, surveilleren en suppoostwerkzaamheden en reageert altijd binnen 4 uur gerekend na de melding (binnen kantoortijden van 08.00-17.00 uur) op een verzoek.

Nr.	**Eisen ten aanzien van cameraverificatie**
38.	Camerabeelden worden door Opdrachtnemer uitsluitend ingezet voor beveiliging van locaties en incidentonderzoek/alarmverificatie via de meldkamer; gebruik voor arbeidsprestatie- of gedragscontrole van medewerkers is ten strengste verboden. Camerabeelden mogen niet worden gebruikt voor het trainen, verbeteren of valideren van AI-systemen of andere algoritmen van Opdrachtnemer of derden.
39.	Opdrachtnemer waarborgt dat camerabeelden en overige beveiligingsinformatie uitsluitend worden gebruikt voor de toegestane doeleinden en niet worden gekopieerd, gedownload, opgeslagen, gedeeld of overgebracht naar andere dan de daarvoor door Opdrachtgever toegestane systemen, gegevensdragers of locaties. Het gebruik van privéapparatuur, waaronder mobiele telefoons, voor het maken van foto's, video's, schermafbeeldingen of andere opnamen van camerabeelden, medewerkers van Opdrachtgever, bezoekers, locaties of beveiligingsinformatie is niet toegestaan. Het gebruik van USB-sticks en andere niet door Opdrachtgever toegestane gegevensdragers is eveneens uitgesloten. Opdrachtnemer ziet erop toe dat haar Personeel deze verplichtingen naleeft en de verkregen toegang of informatie op geen enkele wijze misbruikt.
40.	Camerabeelden worden niet langer bewaard dan noodzakelijk (richtlijn: maximaal 4 weken), tenzij beelden nodig zijn voor een lopend incident- of opsporingsonderzoek; verlengde bewaring wordt gemotiveerd vastgelegd. Bewaren van gegevens langer dan vier (4) weken is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Opdrachtgever, tenzij een wettelijke verplichting of een vordering van een bevoegde autoriteit tot langere bewaring verplicht.
41.	De rol van de meldkamer/beveiligingsdienst (verwerker, gezamenlijke verwerkingsverantwoordelijke of zelfstandig verwerkingsverantwoordelijke) wordt expliciet vastgelegd in de aparte verwerkersovereenkomst aangeleverd bij de aanbestedingsstukken (Bijlage 10)
42.	De videoverbinding tussen de locaties en de meldkamer is end-to-end versleuteld, loopt via een dedicated/gesegmenteerd netwerkpad (bijv. VPN) en de meldkamer wordt wederzijds geauthenticeerd voordat beelden worden ontsloten. Opdrachtgever is gerechtigd de werking en beveiliging van deze voorzieningen zelf of door een door haar aangewezen deskundige te (laten) controleren en testen.

43.	Alleen geautoriseerde operators bij de meldkamer kunnen live meekijken danwel maximaal 1 minuut terugkijken; er is geen doorlopende toegang tot alle camera's tenzij functioneel noodzakelijk, en elk meekijk-, uitlees- of exportmoment wordt gelogd en is opvraagbaar door de Opdrachtgever.
44.	De beveiligingsorganisatie/meldkamer beschikt over een geldige vergunning onder de Wet particuliere beveiligingsorganisaties en recherchebureaus (WPBR); meldkameroperators met toegang tot de camerabeelden zijn gescreend via de korpschef, conform de eisen die voor beveiligingspersoneel gelden.
45.	De meldkamer is gecertificeerd conform NEN-EN 50518 (Alarm Receiving Centre), inclusief eisen aan fysieke beveiliging van de meldkamerruimte, personeelsbezetting en uitwijkmeldkamer. Op verzoek van Opdrachtgever toont Opdrachtnemer binnen 24-uur na het verzoek daartoe aan dat de certificering gedurende de gehele contractperiode geldig is.
46.	Camerabeelden worden uitsluitend ontsloten na een alarmactivering (event-based verificatie). De cameraverificatie-oplossing is zodanig ingericht dat camerabeelden uitsluitend automatisch beschikbaar komen als gevolg van een alarmactivering. Meldkameroperators kunnen camerabeelden niet zelfstandig of op eigen initiatief openen. Camerabeelden mogen uitsluitend worden geraadpleegd voor de beoordeling en afhandeling van het betreffende alarm. Na afhandeling van het alarm wordt het meekijken beëindigd.
47.	De camera-alarmverificatieoplossing voldoet aan de relevante VRKI-classificatie en de beveiligingsorganisatie is RPBI-erkend, zodat wordt voldaan aan de voorwaarden die verzekeraars stellen aan camera-alarmverificatie.

Nr.	**Eisen ten aanzien van de app en online-portal**
48.	Opdrachtgever heeft 24/7 toegang tot een beveiligd portaal of systeem met actuele gegevens waarin Opdrachtgever minimaal schakelbevoegden kan beheren en activiteitenlogs kan inzien.
49.	Zowel de app als het portaal hebben een up-time van minimaal 99% per jaar. Opdrachtnemer monitort en registreert de beschikbaarheid van de app en het portaal continu en kan aan de hand van objectieve en verifieerbare gegevens aantonen dat aan deze beschikbaarheidseis wordt voldaan.
50.	Opdrachtnemer stelt een app beschikbaar waarin geautoriseerde medewerkers het systeem in test kunnen zetten en schakeltijden van beveiligingssystemen kunnen aanpassen.
51.	Opdrachtnemer biedt Opdrachtgever toegang tot een analyse- en rapportageomgeving, binnen of buiten het portaal, waarmee inzicht kan worden verkregen in aanrijtijden, alarmopvolgingen, KPI's en historische trends. De hierin opgenomen gegevens zijn actueel, volledig en controleerbaar. De gegevens dienen mede als onderbouwing voor de beoordeling van de overeengekomen KPI's en de toepassing van de bonus-malusregeling.

52.	Opdrachtgever kan rapportages en analyses exporteren naar een gangbaar bestandsformaat zoals Excel, CSV of PDF.

Nr.	Eisen ten aanzien van privacy en informatiebeveiliging voor de app/portal en cameraverificatie
53.	Opdrachtgever heeft het recht om gedurende de looptijd van de Raamovereenkomst audits uit te voeren of te laten uitvoeren op de naleving van de privacy- en informatiebeveiligingseisen. Opdrachtnemer verleent hieraan alle redelijke medewerking en verstrekt op verzoek relevante bewijsstukken. De kosten van een audit komen in beginsel voor rekening van Opdrachtgever. Indien uit de audit blijkt dat sprake is van een aan Opdrachtnemer toerekenbare tekortkoming in de nakoming van de Raamovereenkomst of niet-naleving van de toepasselijke privacy- of informatiebeveiligingseisen, komen de redelijke kosten van de audit en de kosten van de noodzakelijke herstelmaatregelen voor rekening van Opdrachtnemer.
54.	Opdrachtnemer legt vast in de Verwerkersovereenkomst welke persoonsgegevens het toegangsbeveiligingssysteem verwerkt, voor welke doelen, welke rollen toegang hebben en welke koppelingen gegevens uitwisselen. Zij levert daarbij een datamodel en verwerkingsregister-input en verwerkingsdoeleinden.
55.	De oplossing (het portaal en de app) moet standaard privacyvriendelijk zijn ingericht: minimale logging, beperkte zichtbaarheid van persoonsgegevens en standaard geen brede rapportages over personen.
56.	Voor ingebruikname wordt door de Opdrachtgever een DPIA of DPIA-check uitgevoerd, zeker bij cloud, camerakoppelingen, biometrie, grootschalige logging of monitoring van medewerkers. De Opdrachtnemer dient hieraan mee te werken. Opdrachtnemer is gehouden de door Opdrachtgever verlangde redelijke beheersmaatregelen uit te voeren indien deze noodzakelijk zijn ter waarborging van de bescherming van persoonsgegevens, de privacy en informatiebeveiliging en/of voortvloeien uit de uitkomsten van de DPIA of DPIA-check.
57.	Het gebruik van biometrie is niet toegestaan tenzij een afzonderlijke juridische toets, DPIA en bestuurlijk besluit aantonen dat dit noodzakelijk, rechtsgeldig en proportioneel is. Opdrachtnemer mag biometrische gegevens niet verwerken zonder voorafgaande schriftelijke toestemming van Opdrachtgever.
58.	Persoonsgegevens, logging, back-ups en supportdata worden binnen de EU/EER verwerkt en opgeslagen, tenzij vooraf schriftelijk anders goedgekeurd en na een juridische toets door Opdrachtgever.
59.	Opdrachtnemer meldt (nieuwe) subverwerkers of wijzigingen in bestaande subverwerkers minimaal 30 dagen voorafgaand aan de wijziging aan Opdrachtgever.
60.	Opdrachtnemer legt vast in een bewaar- en vernietigingmatrix welke systeeminformatie, logs, rapportages en contractdocumentatie bewaard, vernietigd of eventueel openbaar gemaakt kunnen worden. De matrix en

	wijzigingen daarvan worden vooraf ter goedkeuring aan Opdrachtgever voorgelegd. Opdrachtnemer wijkt niet zonder voorafgaande schriftelijke toestemming van Opdrachtgever af van de vastgestelde bewaartermijnen.
61.	Bij beëindiging van de Raamovereenkomst moet Opdrachtgever alle data in gangbaar formaat kunnen exporteren en moet Opdrachtnemer aantoonbaar alle kopieën verwijderen.
62.	Opdrachtnemer levert na voorlopige gunning een mapping op relevante BIO2/ISO 27001/27002-controls voor de aangeboden oplossing en beheerdienst.
63.	Alle beheeraccounts gebruiken MFA (multifactorauthentificatie) en zijn persoonsgebonden en herleidbaar tot een individuele gebruiker; gedeelde beheeraccounts zijn niet toegestaan.
64.	Toegang tot beheerfuncties en persoonsgegevens is rolgebaseerd en minimaal noodzakelijk ingericht. Opdrachtnemer kan dit aantonen met RBAC-matrix en autorisatieprofielen.
65.	Alle beheeracties, autorisatiewijzigingen, exports, raadplegingen van logs en supportacties worden gelogd.
66.	Persoonsgegevens en beheercommunicatie worden versleuteld met TLS 1.3 of TLS 1.2 tijdens transport en opslag. De TLS-instellingen volgen de nieuwste NCSC-richtlijnen voor TLS en alleen de status "Goed" of "Voldoende" zijn toegestaan. Voor beheer op afstand gebruikt de Opdrachtnemer alleen versleutelde protocollen, zoals SSH, HTTPS of een VPN. Onversleutelde protocollen (zoals Telnet, HTTP, FTP en SNMPv1/v2c) staan uit.
67.	Opdrachtnemer hanteert patchtermijnen op basis van risicoclassificatie en meldt kritieke kwetsbaarheden actief aan Opdrachtgever (kritieke kwetsbaarheden binnen 14 dagen, hoog binnen 30 dagen, gemeten vanaf publicatie/CVSS-score).
68.	Opdrachtnemer laat minimaal jaarlijks een onafhankelijke audit op de informatiesysteem of pentest uitvoeren op de applicatie, infrastructuur en relevante koppelvlakken. Opdrachtgever heeft recht op inzage in het audit/pentest-rapport.
69.	Back-ups van configuratie en relevante gegevens zijn versleuteld, getest en vallen onder dezelfde privacy- en beveiligingseisen als in dit Programma van eisen opgenomen.
70.	Toegangsgegevens mogen uitsluitend worden gebruikt voor toegangsbeheer, beveiliging, incidentonderzoek en wettelijke/compliance-doeleinden.
71.	Gebruik van toegangslogs voor prestatie-, aanwezigheids- of gedragscontrole van medewerkers is standaard uitgesloten, tenzij apart juridisch getoetst en vastgesteld door Opdrachtgever.
72.	Het systeem verwerkt niet meer persoonsgegevens dan noodzakelijk; optionele velden staan standaard uit. Opdrachtgever is gerechtigd door middel van steekproeven te controleren of aan deze verplichting wordt voldaan.
73.	Bewaartermijnen voor toegangslogs, bezoekersgegevens, beheerlogs en exports zijn configureerbaar en worden automatisch afgedwongen. Opdrachtnemer toont op verzoek van Opdrachtgever door middel van een demonstratie aan dat de bewaartermijnen daadwerkelijk kunnen worden

	geconfigureerd en dat de ingestelde bewaartermijnen automatisch en correct worden toegepast, waaronder het tijdig en onomkeerbaar verwijderen van gegevens na het verstrijken van de toepasselijke bewaartermijn.
74.	Opdrachtnemer ondersteunt afhandeling van inzage-, correctie-, beperking-, bezwaar- (art. 21 AVG) en verwijderverzoeken binnen afgesproken termijnen, namelijk 5 werkdagen, zodat Opdrachtgever kan voldoen aan de termijnen van artikel 12 lid 3 AVG.
75.	Opdrachtnemer meldt informatiebeveiligingsincidenten en mogelijke datalekken onverwijld en uiterlijk binnen 12 uur na ontdekking bij Opdrachtgever (via **security@rijnland.net**), zodat deze zo nodig binnen de wettelijke termijn van 72 uur (art. 33 AVG) bij de Autoriteit Persoonsgegevens kan melden, met voldoende informatie voor beoordeling door Opdrachtgever. • De eerste melding bevat ten minste de aard van het incident, het tijdstip van ontdekking, de (mogelijk) getroffen gegevens en systemen van HHR, de genomen maatregelen en een bereikbare contactpersoon. • Opdrachtnemer levert uiterlijk 48 uur na ontdekking een aanvullende melding en uiterlijk drie weken na ontdekking een eindrapportage. • Opdrachtnemer verstrekt daarnaast alle informatie die HHR nodig heeft om aan zijn wettelijke meldplichten te voldoen en werkt mee aan de afhandeling van het incident.
76.	Export van persoonsgegevens is beperkt tot geautoriseerde rollen, wordt gelogd en is technisch te beperken of uit te schakelen.
77.	Opdrachtnemer heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost. Op verzoek kan dit door Opdrachtgever worden opgevraagd.
78.	Opdrachtnemer zal de bij deze aanbesteding bijgevoegde Verwerkersovereenkomst ondertekenen en meewerken in het actueel houden hiervan. Een eventueel benoemde aansprakelijkheidsbeperking (bijvoorbeeld in de AWVODI 2018) zal niet van toepassing zijn op deze verwerkersovereenkomst.
79.	Voor elke verwerking van persoonsgegevens binnen het systeem is de rechtsgrond (art. 6 AVG) expliciet vastgelegd en opgenomen in het verwerkingsregister.
80.	Opdrachtnemer registreert subverwerkers en schakelt derden alleen in met voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke.
81.	Opdrachtnemer ondersteunt Opdrachtgever bij het voldoen aan meldplichten voortvloeiend uit de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke): vroegtijdige waarschuwing binnen

	24 uur en volledige incidentmelding binnen 72 uur na ontdekking van een significant incident bij het NCSC.
82.	Het systeem kent gedocumenteerd fail-safe/fail-secure gedrag bij stroomuitval, netwerkstoring of systeemcrash, afgestemd op brandveiligheid en ontruiming; Opdrachtnemer specificeert hersteltijd (RTO) en maximaal dataverlies (RPO).
83.	Het systeem is logisch gescheiden van kantoorautomatisering en OT/SCADA-netwerken; koppelvlakken zijn expliciet gedocumenteerd en beperkt tot het noodzakelijke.
84.	Medewerkers van de Opdrachtnemer met fysieke of logische toegang tot het systeem of persoonsgegevens zijn gescreend (bijv. VOG of gelijkwaardig), passend bij de gevoeligheid van de toegang.
85.	Logbestanden worden bewaakt voor traceerbaarheid en worden op elk willekeurig moment op werkdagen tussen 08.00 uur tot 18.00 beschikbaar gesteld voor de Opdrachtgever en toezichthouders. Logbestanden worden minimaal 12 maanden bewaard, zodanig dat integriteit, beschikbaarheid en vertrouwelijkheid zijn geborgd. Logs zijn uitsluitend toegankelijk voor geautoriseerde personen.
86.	Opdrachtnemer levert binnen tien (10) werkdagen na constatering van een tekortkoming op het gebied van informatiebeveiliging een herstelplan aan en voert dit uit. Niet-nakoming van deze uitvoeringsvoorwaarde geldt als een tekortkoming in de nakoming van de Raamovereenkomst.

Nr.	**Eisen ten aanzien van AI (Indien gebruikt)**
87.	Opdrachtnemer is verplicht de AI-verordening en de daaraan verbonden wet- en regelgeving die van toepassing is op de toe te passen AI en/of AI-systeem (aantoonbaar) na te leven.
88.	Opdrachtnemer informeert de contractmanager van Opdrachtgever minimaal vijf (5) weken voorafgaand aan de voorgenomen inzet van AI, AI-systemen of AI-functionaliteiten en vraagt hiervoor vooraf schriftelijke toestemming.
89.	Iedere uitbreiding of wijziging van de AI, het AI-systeem of de AI-functionaliteit ten opzichte van de oorspronkelijk beoordeelde en goedgekeurde inzet geldt als een nieuwe voorgenomen inzet en is derhalve onderworpen aan dezelfde informatie-, toestemmings- en beoordelingsverplichtingen als hierboven omschreven. Opdrachtgever kan van Opdrachtnemer verlangen dat bij een dergelijke wijziging de Leverancierskaart opnieuw volledig en actueel wordt ingevuld en aan Opdrachtgever wordt verstrekt.
90.	Hoog-risico-AI mag uitsluitend worden ingezet indien dit wettelijk is toegestaan en Opdrachtnemer aantoonbaar voldoet aan alle toepasselijke wettelijke eisen. Opdrachtnemer verstrekt vóór de inzet aan Opdrachtgever alle relevante bewijsstukken, zoals (maar niet beperkt tot): conformiteitsdocumentatie, technische documentatie, relevante registraties en documentatie over risicobeheersing, menselijk toezicht en cybersecurity. Opdrachtgever kan aanvullende bewijsstukken verlangen

	indien deze noodzakelijk zijn om de rechtmatige en veilige inzet van het AI-systeem te kunnen beoordelen.
91.	Opdrachtnemer verstrekt vooraf alle informatie en bewijsstukken die Opdrachtgever nodig heeft voor de juridische, privacy- en beveiligingsbeoordeling.
92.	Opdrachtgever kan het gebruik van de AI, het AI-systeem of de AI-functionaliteit weigeren indien de toepassing niet past binnen de aard of scope van de Raamovereenkomst. Opdrachtgever kan toestemming eveneens weigeren indien de toepassing naar haar oordeel onaanvaardbare risico's oplevert voor veiligheid, informatiebeveiliging, privacy en/of gegevensbescherming. Het feit dat een AI-systeem wettelijk is toegestaan, verplicht Opdrachtgever niet tot het verlenen van toestemming. Opdrachtnemer kan dus aan deze opdracht op voorhand geen rechten of toezeggingen ontlenen.
93.	Alle gegevens en informatie die door of namens Opdrachtgever aan Opdrachtnemer worden verstrekt, dan wel in het kader van de dienstverlening voor Opdrachtgever worden gegenereerd of verzameld, blijven van Opdrachtgever. Opdrachtnemer mag deze gegevens uitsluitend gebruiken voor de uitvoering van de Raamovereenkomst.
94.	Opdrachtnemer draagt er zorg voor dat logbestanden worden bewaard overeenkomstig de door Opdrachtgever vastgestelde bewaartermijnen. Na het verstrijken van de toepasselijke bewaartermijn worden de logbestanden automatisch, volledig en onomkeerbaar vernietigd. Opdrachtnemer kan op verzoek van Opdrachtgever aantonen dat de ingestelde bewaartermijnen en vernietiging daadwerkelijk worden toegepast.
95.	Het AI-systeem moet te allen tijde kunnen worden uitgeschakeld of buiten gebruik worden gesteld, zonder dat dit leidt tot onderbreking of vermindering van de overeengekomen dienstverlening. Opdrachtnemer waarborgt dat de dienstverlening in dat geval wordt voortgezet en blijft voldoen aan alle eisen, kwaliteitsnormen, KPI’s en overige verplichtingen zoals vastgelegd in de aanbestedingsstukken en de Raamovereenkomst.
96.	In geval van een (vermoedelijk) datalek, beveiligingsincident of audit verleent Opdrachtnemer alle redelijkerwijs noodzakelijke medewerking aan Opdrachtgever. Opdrachtnemer stelt op eerste verzoek de relevante logbestanden, audittrails en overige beschikbare bewijsstukken ter beschikking voor onderzoek naar de aard, oorzaak, omvang en gevolgen van het incident. De integriteit en beschikbaarheid van deze gegevens worden gedurende het onderzoek gewaarborgd.
97.	Opdrachtnemer verstrekt alle door Opdrachtgever gevraagde informatie, documentatie, verklaringen en bewijsstukken die noodzakelijk zijn voor de beoordeling van AI, AI-systemen of AI-functionaliteiten en de vaststelling van de toepasselijke risicoclassificatie.
98.	Opdrachtnemer toont gemotiveerd aan op basis van welke criteria de vastgestelde risicoclassificatie van de AI, het AI-systeem of de AI-functionaliteit tot stand is gekomen, inclusief de onderbouwing waarom geen sprake is van een verboden praktijk of een hoger risiconiveau dan vastgesteld.

99.	AI, AI-systemen en AI-functionaliteiten dienen gedurende de gehele AI-waardeketen transparant, uitlegbaar, controleerbaar en aantoonbaar beheerst te zijn. Opdrachtnemer verleent alle medewerking aan door Opdrachtgever verlangde beoordelingen, toetsen en audits.
100.	Opdrachtgever behoudt zich het recht voor de inzet van AI, AI-systemen of AI-functionaliteiten geheel of gedeeltelijk te weigeren, beperken of beëindigen indien niet wordt voldaan aan de aanbestedingsdocumenten, de toepasselijke wet- en regelgeving, of indien de inzet leidt of kan leiden tot een wijziging van de aard, omvang, inhoud, verantwoordelijkheidsverdeling of scope van de Opdracht.
101.	AI, AI-systemen en AI-functionaliteiten mogen uitsluitend worden ingezet ter ondersteuning van de uitvoering van de Opdracht. De inzet hiervan leidt niet tot uitbreiding, wijziging of meerwerk van de Opdracht of de overeengekomen dienstverlening.
102.	De inzet van AI, een AI-systeem en/of andere AI-functionaliteiten mag niet leiden tot aanvullende kosten, prijsverhogingen, meerwerk, gewijzigde tarieven of andere financiële aanspraken jegens Opdrachtgever. Opdrachtnemer wordt geacht de overeengekomen werkzaamheden en diensten ook zonder AI, een AI-systeem en/of andere AI-functionaliteiten onder dezelfde voorwaarden, prestaties en tarieven te kunnen uitvoeren.
103.	Opdrachtnemer draagt er zorg voor dat medewerkers die betrokken zijn bij de configuratie, het beheer of het onderhoud van de AI, het AI-systeem of de AI-functionaliteit over voldoende AI-geletterdheid beschikken conform artikel 4 van de AI-verordening, en toont dit desgevraagd aan.
104.	Opdrachtnemer kan aantonen dat hij op passende wijze beveiligingsmaatregelen heeft genomen die noodzakelijk zijn voor de AI, het AI-systeem of de AI-functionaliteit. De inzet en het gebruik hiervan door Opdrachtnemer geschieden voor eigen rekening en risico van Opdrachtnemer. Opdrachtgever is niet aansprakelijk voor schade, boetes, kosten of andere gevolgen die voortvloeien uit de inzet of het gebruik daarvan door Opdrachtnemer.
105.	Opdrachtnemer mag bij het gebruik van AI-systemen geen vertrouwelijke, beveiligingsgevoelige of anderszins niet-openbare gegevens of informatie van Opdrachtgever invoeren, uploaden, verwerken, laten verwerken of anderszins ter beschikking stellen aan een AI-systeem, tenzij Opdrachtgever hiervoor voorafgaand schriftelijk toestemming heeft verleend. Opdrachtnemer waarborgt dat deze verplichting ook wordt nageleefd door zijn Personeel en door derden die hij bij de uitvoering van de Raamovereenkomst inschakelt.
106.	Opdrachtnemer is niet gerechtigd gegevens of informatie van Opdrachtgever, dan wel gegevens of informatie die in het kader van de uitvoering van de Raamovereenkomst worden verkregen of gegenereerd, te gebruiken voor het trainen, verbeteren, testen of anderszins ontwikkelen van AI-systemen of AI-modellen. Dit geldt tevens voor door Opdrachtnemer ingeschakelde derden en leveranciers van AI-systemen. **Let op**: Niet-nakoming van deze eis is een toerekenbare tekortkoming die onmiddellijke ontbinding van de Raamovereenkomst rechtvaardigt. Opdrachtgever is in

	dat geval gerechtigd de Raamovereenkomst met onmiddellijke ingang, buiten rechte, zonder voorafgaande ingebrekestelling, geheel of gedeeltelijk te ontbinden, onverminderd haar overige rechten, waaronder het recht op schadevergoeding.
107.	Opdrachtnemer is bij gebruik van de AI, het AI-systeem of de AI-functionaliteit verplicht zijn medewerking op voorhand te verlenen aan het ondertekenen van de AI-overeenkomst (Bijlage 20), die afgestemd zal worden op de risicoclassificatie van de AI, het AI-systeem of de AI-functionaliteit. Wijzigingen van deze AI-overeenkomst is voorbehouden aan Opdrachtgever.

Nr.	**Eisen ten aanzien van de personen belast met de uitvoering van de dienstverlening**
108.	Alle beveiligers beschikken over geldige screening/toestemming van de korpschef en beschikken minimaal over diploma Beveiliger 2 of aantoonbaar gelijkwaardig. Opdrachtnemer meldt intrekking, schorsing of verval van een toestemming of legitimatiebewijs onverwijld aan Opdrachtgever via fysiekebeveiliging@rijnland.net.
109.	Leidinggevenden beschikken over ministeriële toestemming conform Wpbr.
110.	Medewerkers van de Opdrachtnemer dan wel personen die namens de Opdrachtnemer op locatie van Opdrachtgever werkzaamheden uitvoeren dienen zich te allen tijde te kunnen legitimeren.
111.	De beveiliger stelt zich tijdens de uitvoering van de werkzaamheden te allen tijde professioneel op tegenover medewerkers van Opdrachtgever, bezoekers en overige derden en onthoudt zich van gedrag dat als intimiderend, ongepast of onprofessioneel kan worden ervaren.
112.	In te zetten personeel dient zich representatief te kleden en te gedragen. De in te zetten medewerker draagt daartoe tijdens zijn dienst altijd representatieve en schone, kreukvrije uniforme bedrijfskleding, die te herkennen is als bedrijfskleding van de Opdrachtnemer.
113.	De medewerkers die belast zijn met de uitvoering van de Diensten beschikken over voldoende mondelinge en schriftelijke beheersing van de Nederlandse taal om instructies te begrijpen, te communiceren met contactpersonen van Opdrachtgever en rapportages op te stellen.
114.	Opdrachtnemer zorgt ervoor dat het in te zetten personeel geen gebruik maakt van de bij de Opdrachtgever aanwezige communicatiemiddelen anders dan in geval van nood. Het gebruik van wifi op locaties van de Opdrachtgever is toegestaan.
115.	Het personeel van Opdrachtnemer is gehouden tot volledige geheimhouding van alles wat hen bij de uitvoering van de werkzaamheden ter kennis komt.
116.	Het personeel van Opdrachtnemer houdt zich aan de gedragsregels.
117.	Indien daartoe naar het oordeel van Opdrachtgever aanleiding bestaat (zoals niet naleving van eisen 108 t/m 116), kan Opdrachtgever, na schriftelijke motivatie, verwijdering en vervanging van een door

	Opdrachtnemer tewerkgestelde medewerk(st)er eisen. Opdrachtnemer zal, zonder dat daarvoor extra kosten in rekening kunnen worden gebracht, terstond aan een dergelijke eis gevolg geven.
118.	Opdrachtnemer levert alle voor de werkzaamheden noodzakelijke PBM, communicatie- en werkmiddelen.
119.	Opdrachtnemer is niet bevoegd Opdrachtgever in of buiten rechte te vertegenwoordigen, namens Opdrachtgever op te treden of namens Opdrachtgever verklaringen, toezeggingen of standpunten in te nemen in het kader van een geschil, tenzij Opdrachtgever hiervoor vooraf uitdrukkelijk en schriftelijk toestemming heeft verleend.

Nr.	**Eisen aan interactie met Opdrachtnemer, rapportage en informatievoorziening**
120.	Opdrachtnemer wijst één vaste accountmanager en één vervanger aan als tactisch/strategisch aanspreekpunt. Bij ziekte of afwezigheid stelt Opdrachtnemer binnen vijf (5) werkdagen Opdrachtgever op de hoogte.
121.	Voor urgente operationele aangelegenheden is 24/7 een bereikbaar contactpunt beschikbaar. Minimaal 90% van de oproepen wordt binnen 5 minuten beantwoord of opgevolgd.
122.	Voor aanvang van de dienstverlening levert Opdrachtnemer een escalatiestructuur met ten minste drie niveaus evenals een communicatiematrix voor de belangrijkste operationele zaken.
123.	De Opdrachtnemer dient de Opdrachtgever terstond te informeren over alle zaken en onregelmatigheden die van belang zijn voor de continuïteit van de uitvoering van de opdracht of een bedreiging vormen voor de continuïteit van de bedrijfsprocessen van de Opdrachtgever.
124.	De Opdrachtgever organiseert minimaal eens per kwartaal (maar zo vaak als nodig is) een overleg, waarbij de periodieke rapportages en de geleverde prestaties worden besproken. De Opdrachtnemer dient deel te nemen aan deze overleggen.
125.	De oorzaak van een alarm wordt genoteerd in een interventierapport (of uitrukrapport) dat wordt toegezonden aan de contactpersoon van het betreffende object en naar fysiekebeveiliging@rijnland.net en contractmanagementbod@rijnland.net. Het interventierapport wordt uiterlijk de volgende werkdag toegezonden. Ten minste opgenomen is: • Datum; • Tijdstip ontvangst melding; • Tijdstip surveillant ter plaatse; • Tijdstip vertrek surveillant; • Welk gebouw en welke zone; • Hetgeen ter plekke is waargenomen, bijzonderheden • Eventueel genomen maatregelen • Eventuele vervolgacties
126.	Na iedere brand- en sluitronde wordt, uiterlijk de volgende dag, een rapport toegezonden aan fysiekebeveiliging@rijnland.net en contractmanagementbod@rijnland.net met daarin minimaal:

	• Datum; • Tijd aankomst • Tijd vertrek • Bijzonderheden (zoals aangetroffen personen en locatie van die personen, open ramen/deuren, brand onveilige situaties etc) • Bijzonderheden worden waar mogelijk gespecificeerd per gebouwdeel, verdieping of object. Bijvoorbeeld (zoals aangetroffen personen en locatie van die personen, open ramen/deuren, brand onveilige situaties etc).
127.	Opdrachtgever zorgt dat Opdrachtnemer minimaal elk kwartaal, twee weken voorafgaande het kwartaaloverleg, inzage krijgt, door middel van rapportage, in de afgesproken KPI's, EMVI-belofte en het totaal aan alarmopvolgingen en bestaat dus minimaal uit: • Aanrijtijden van Prio 1 en Prio 2 meldingen inclusief het % dat binnen/buiten afgesproken responstijden liggen • Bereikbaarheid van de meldkamer inclusief % binnen afgesproken tijd • Inzicht in het totaal van alarmopvolgingen per locatie en type alarm • % Elektrisch gereden
128.	Na beëindiging van de Raamovereenkomst retourneert Opdrachtnemer alle door Opdrachtgever verstrekte fysieke middelen, waaronder sleutels, toegangspassen en overige toegangsmiddelen en daarnaast alle informatie dat eigendom is van HHR zoals volledige en actuele overdrachtssets aan protocollen en werkinstructies, rapportages, toegangsrechten en contactgegevens.
129.	Na beëindiging van de Raamovereenkomst verwijdert Opdrachtnemer onverwijld alle digitale gegevens van Opdrachtgever uit haar systemen, waaronder protocollen, rapportages, sleuteladministratie, toegangsrechten, contactgegevens, exports, back-ups en eventuele kopieën daarvan, tenzij wettelijke bewaartermijnen anders voorschrijven. Op verzoek van Opdrachtgever toont Opdrachtnemer aan dat de digitale gegevens zijn verwijderd.

Nr.	**Eisen ten aanzien van facturatie**
130.	Aanvullend op AWVODI-2018 artikel 15 lid 3 dient op de factuur te worden vermeld/ bij de factuur te worden gevoegd: • Het door Opdrachtgever opgegeven bestelnummer (orderkenmerk). Bestelnummers worden eens per jaar, voor start van een nieuwe contractperiode, aan Opdrachtnemer doorgegeven door Opdrachtgever.
131.	Geannuleerde en niet gereden alarmopvolgingen worden niet gefactureerd aan Opdrachtgever.
132.	Facturatie van abonnementen/aansluitingen/vaststaande brand en sluit-rondes gebeurt eens per jaar, in de eerste maand van de contractperiode.

	Facturatie voor alarmopvolging, cameraverificatie, incidentele verzoeken voor openen/sluiten en suppoost wordt op een verzamelfactuur eens per kwartaal ingediend. Op de verzamelfactuur wordt per dienst minimaal inzicht gegeven in de uitgevoerde werkzaamheden, aantallen, locaties, data en de gehanteerde tarieven.
133.	Opdrachtnemer dient eerst een proforma-factuur in via contractmanagementBOD@rijnland.net die binnen vijf (5) werkdagen gecontroleerd wordt door de contractmanager. Eventuele fouten worden doorgegeven door Opdrachtgever en uitgezocht door Opdrachtnemer en indien nodig aangepast. Na akkoord van de Opdrachtgever wordt de factuur ingediend via E-facturatie bij de administratie van Opdrachtgever.

Deel 2 behorende bij de herzieningsclausule

Nr.	Eisen ten aanzien van opvolging 'alleen-werken' (Optionele dienst)
134.	Met betrekking tot locatiebepaling van een alleenwerk-melding moet de meldkamer: • actuele locatie kunnen raadplegen; • laatste bekende locatie kunnen ophalen; • locatiehistorie kunnen terugzien; • locatiegegevens kunnen delen met hulpdiensten.
135.	Afhandeling van een alleenwerk-melding gebeurt altijd (100%) conform het vastgestelde protocol (zie Bijlage 19). Na ontvangst van een alleenwerk-melding wordt onverwijld gestart met de in het protocol voorgeschreven opvolgingsacties
136.	Tweezijdige spraakcommunicatie moet mogelijk zijn tussen meldkamer en alleen-werker.
137.	De meldkamer kan de Alleen-werker actief oproepen.
138.	Gesprekken tussen meldkamer en Alleen-werker dienen worden vastgelegd en 1 maand beschikbaar blijven.
139.	Communicatie tussen Alleen-werker en meldkamer werkt ook bij stil alarm.
140.	95% van alle Alleen-werk alarmen worden binnen 1 minuut aangenomen en vervolgens binnen 2 minuten beoordeeld door meldkamer. Deze percentages en tijden zijn KPI's waarop de bonus-malus regeling op van toepassing is. Elk kwartaal wordt beoordeeld of voldaan wordt aan de KPI's.
141.	Na ieder incident ontvangt Rijnland binnen 24 uur een rapportage met: • tijdstip alarm; • oorzaak alarm; • responstijden; • uitgevoerde acties; • betrokken hulpdiensten; • afhandeling.
142.	Elk kwartaal wordt een rapportage door Opdrachtnemer aangeleverd met daarin: • KPI-overzicht; • analyse van trends en valse alarmen.
143.	Meldkamer medewerkers hebben de volgende ervaring en opleidingen: • Hebben minimaal 1 jaar ervaring in alarmopvolging bij alleenwerkers; • kennen de escalatieprotocollen van Rijnland;
144.	Jaarlijks oefenen meldkamer medewerkers en surveillanten minimaal éénmaal de volgende scenario's: • medische noodsituatie; • agressie/geweld; • vermissing medewerker. Opdrachtnemer legt de bevindingen, leerpunten en verbetermaatregelen van de oefening vast en verstrekt deze op verzoek aan Opdrachtgever.

145.	Surveillant bezit (naast diploma beveiliger 2) ook de volgende opleidingen en competenties: • BHV-certificaat incl reanimatie en AED; • training omgaan met agressie en geweld; • instructie over risico's binnen waterbeheerobjecten. • aantoonbare kennis van risico's met betrekking tot gevaarlijke atmosferen, besloten ruimten, H2s, Ch4 ATEX- omgevingen en het veilig gebruik van een gasmeter.
146.	De Surveillant mag ter plaatse de volgende taken op zich nemen: • locatie verifiëren; • contact leggen met medewerker; • eerste hulp verlenen binnen eigen competentie; • hulpdiensten opvangen; • locatie veilig stellen.
147.	Het is niet toegestaan dat de Surveillant de volgende acties uitvoert: • reddingsacties uitvoeren waarvoor specialistische middelen nodig zijn; • besloten ruimten betreden; • risicovolle technische werkzaamheden verrichten.
148.	Surveillant beschikt, aanvullend op eis 27, het volgende: • BHV-kit; • AED in voertuig; • navigatiesysteem met GPS-coördinaten. • Gasmeter H2s CH4 O2(LEL) • Reddingsvest
149.	Surveillant is maximaal 30 minuten, na ontvangst van het alarm door de meldkamer, aanwezig op locatie. Opdrachtnemer zorgt dat minimaal 90% van de meldingen binnen afgesproken aanrijtijd van 30 minuten wordt gehaald. Deze aanrijtijd en dit percentage zijn KPI's waarop de bonus-malusregeling van toepassing is. Elk kwartaal wordt beoordeeld of voldaan wordt aan de KPI's.

Nr.	**Eisen ten aanzien van centralistendienst (optionele dienst)**
150.	De centralistendienst wordt 24 uur per dag en 7 dagen per week uitgevoerd door bevoegde en geïnstrueerde centralisten.
151.	Centralisten beschikken over kennis van de beveiligingssystemen, protocollen, calamiteitenprocedures en toegangsprocedures van Opdrachtgever.
152.	Centralisten beschikken minimaal over een geldige screening/toestemming conform de Wpbr voor zover wettelijk vereist voor de uit te voeren werkzaamheden.
153.	Alle handelingen van de centralist worden vastgelegd in een digitaal logboek waarin ten minste datum, tijdstip, uitgevoerde actie, aanleiding en gebruikte autorisatie worden geregistreerd.

154.	De centralist verifieert de identiteit van personen alvorens toegang te verlenen, toegangsrechten te wijzigen of gevoelige informatie te verstrekken.
155.	Opdrachtnemer zorgt voor voldoende bezetting zodat de continuïteit van de centralistendienst bij ziekte, verlof, opleidingen en calamiteiten is gewaarborgd.
156.	De centralist heeft toegang tot actuele contactlijsten, instructies, escalatieschema's en calamiteitenprocedures van Opdrachtgever.
157.	Uitval van de centralistendienst wordt onverwijld gemeld aan Opdrachtgever. Opdrachtnemer beschikt over een aantoonbaar werkende back-up- en uitwijkvoorziening.
158.	Opdrachtnemer rapporteert maandelijks over de uitgevoerde werkzaamheden, het aantal meldingen, toegangsverzoeken, bijzonderheden en eventuele afwijkingen van procedures.
159.	Centralisten zijn aantoonbaar geïnstrueerd over privacy, informatiebeveiliging, geheimhouding en de omgang met persoonsgegevens.
160.	Het is centralisten niet toegestaan autorisaties, toegangsrechten of protocollen te wijzigen zonder voorafgaande toestemming van Opdrachtgever, tenzij sprake is van een calamiteit of een vooraf overeengekomen werkinstructie.
161.	Alle gesprekken en meldingen die voortkomen uit de centralistendienst worden conform de geldende wet- en regelgeving en de instructies van Opdrachtgever geregistreerd en bewaard.

Nr.	**Eisen ten aanzien van beveiligingsdienst (optionele dienst)**
162.	De beveiligingsdienst wordt uitgevoerd door bevoegde en geïnstrueerde beveiligers.
163.	Beveiligers beschikken over kennis van de beveiligingssystemen, huisregels, calamiteitenprocedures, toegangsprocedures en veiligheidsinstructies van Opdrachtgever.
164.	Beveiligers beschikken minimaal over een geldige screening/toestemming conform de Wpbr.
165.	Opdrachtnemer zorgt voor voldoende bezetting zodat de continuïteit van de beveiligingsdienst bij ziekte, verlof, opleidingen en calamiteiten is gewaarborgd.
166.	De beveiliger heeft toegang tot actuele contactlijsten, instructies, escalatieschema's en calamiteitenprocedures van Opdrachtgever.
167.	Uitval van de beveiligingsdienst wordt onverwijld gemeld aan Opdrachtgever.
168.	Opdrachtnemer rapporteert na elke dienst over de uitgevoerde werkzaamheden, incidenten, bijzonderheden en eventuele afwijkingen van procedures.
169.	Beveiligers zijn aantoonbaar geïnstrueerd over privacy, informatiebeveiliging, geheimhouding en de omgang met persoonsgegevens.

170.	De beveiliger handelt binnen de aan hem verstrekte instructies, bevoegdheden en werkinstructies van Opdrachtgever.