

Bijlage 9. Programma van Eisen met bijlagen

Inhoud:

1	Definities en lijst met afkortingen.....	2
1.1	Definities	2
2	Eisen	3
2.1	Uitvoering van de opdracht	3
2.2	Preventief onderhoud	4
2.3	Beheer	5
2.4	Preventief onderhoud	8
2.5	Communicatie en rapportage	11
2.6	Correctief onderhoud en preventief	11
2.7	Ict- en informatieveiligheid	12

1 Definities en lijst met afkortingen

1.1 Definities

Controleren: het op vakspecialistische wijze inspecteren van onderdelen op juiste werking dan wel goede staat, teneinde het optimaal functioneren van de installatie te waarborgen.

Correctief onderhoud: Het opheffen van storingen aan de installaties, al dan niet verrekenbaar. Indien blijkt dat tijdens het uitvoeren van onderhoudswerk (preventief/toestand afhankelijk onderhoud/incidenten) bepaalde onderdelen niet of niet goed functioneren en reparatie of vervanging van deze onderdelen wenselijk of noodzakelijk wordt geacht, dient de opdrachtnemer de opdrachtgever hiervan in kennis te stellen en een gespecificeerde kostenopgave te verstrekken. Het uitvoeren van correctief onderhoud, behoort tot de verplichtingen van de opdrachtnemer.

SMS: Security Management Systeem

SPIE (KPN): De infrastructuur die vanuit de Opdrachtgever ter beschikking wordt gesteld “van poort tot poort”.

Responstijd: tijdsduur tussen melden van een storing door opdrachtgever en het door een, ter zake deskundig en van de juiste gereedschappen voorzien, storingsmonteur aanvangen van het verhelpen van een storing. De status van een storing (urgent of niet urgent) wordt bepaald door de opdrachtgever.

Storing: Een storing is iedere spontaan optredend defect of gebeurtenis waardoor de werking van een systeem afwijkt van de beoogde werking met nadelige en/of schadelijke gevolgen voor personen en bedrijfsvoering zonder dat daarbij sprake is van opzet, dan wel calamiteit.

Systeem: Het Security Management Systeem en de onderdelen, zowel software- als hardwarematig waar onderhoud en service op van toepassing is.

Update: Een gewijzigde versie van de Programmatuur, waardoor gebreken daarin worden hersteld, of de logische samenhang wordt verbeterd.

Upgrade: Een gewijzigde en/of verbeterde versie van de Programmatuur, waardoor de functionaliteit daarvan wordt vergroot.

Opdrachtgever: Gemeente Den Haag.

Opdrachtnemer: de inschrijver aan wie op basis van onderhavige aanbesteding de overeenkomst wordt gegund.

Preventief onderhoud: Het periodiek uitvoeren van werkzaamheden ter instandhouding en bevordering van het optimaal functioneren van de installatie, teneinde de bedrijfszekerheid te handhaven. Inclusief het herstellen van aangetroffen kleine beschadigingen aan de installatie zoals het ontroesten en het bijwerken van corrosiegevoelige onderdelen met het door de fabrikant voorgeschreven product.

De onderhoudswerkzaamheden dienen volgens de in dit document en door de fabrikant/leverancier voorgeschreven methodes, bedrijfsuren en/of tijdsintervallen te worden uitgevoerd.

2 Eisen

2.1 Uitvoering van de opdracht

Eis 1. Beschrijving en functionaliteit Systemen

Inschrijver is bekend en akkoord met de beschrijving van systemen en haar functionaliteit zoals aangegeven bijlage 5 Prijzenblad, tabblad Samenvatting. Bij Acceptatie gaat inschrijver akkoord met de op dat moment bekende status van deze systemen en is op dat moment verantwoordelijk voor de beschikbaarheid van de systemen zoals die aanwezig zijn. Inschrijver vergewist zich van een juiste beschrijving en vermelding van de systemen. Eventuele gebreken of fouten in de in deze aanbesteding verstrekte beschrijving, aantallen of status ontslaan inschrijver niet van haar onderhoudsplicht.

Eis 2. Uitvoering opdracht

Inschrijver is in staat het onderhoud uit te voeren op de in de installed base (bijlage 5 Prijzenblad, tabblad Samenvatting) beschreven systemen. Het onderhoud wordt uitgevoerd volgens de aangegeven onderhoudsintervallen en beschreven werkwijze of certificering. Dit onderhoud betreft zowel preventief en correctief onderhoud op hardware en het uitvoeren van updates en upgrades op software. Opdrachtnemer is daarmee verantwoordelijk voor de juiste werking van het gehele beveiligingssysteem en haar onderdelen behorende bij deze aanbesteding.

Eis 3. Aanvullende leveringen/dienstverlening

Inschrijver is in staat eventuele uitbreidingen en aanvullingen te leveren met betrekking tot het beschreven systeem.

Eis 4. Meerwerk installaties en werken

Indien zich tijdens de duur van de overeenkomst situaties voordoen die leiden tot vervangingen of uitbreidingen gelijkwaardig aan een werk, daaronder mede begrepen verbouwingen en/of uitbreidingen van installaties, dient opdrachtnemer op verzoek van opdrachtgever een offerte uit te brengen. Opdrachtnemer verstrekt binnen uiterlijk 10 werkdagen de offerte aan opdrachtgever. De offerte bevat een duidelijke beschrijving van de werkzaamheden en een open kostprijs calculatie op basis van de in de inschrijving afgegeven tarieven voor monteurs en materialen. In het geval geen overeenstemming wordt bereikt staat het opdrachtgever vrij onderhavige werkzaamheden aan derden in opdracht te geven. Opdrachtnemer neemt deze door een derde uitgevoerde werkzaamheden vervolgens in beheer.

De opdrachtgever zal in dat geval de opdrachtnemer schriftelijk, met redenen omkleed, mededeling doen van de beëindiging van de offerteprocedure en de opdrachtnemer daarbij onvoorwaardelijk van eventuele inmiddels gedane aanbiedingen of onderdelen daarvan ontslaan. De opdrachtnemer is in dat geval verplicht tot geheimhouding ter zake van het werk en het daarover gevoerde overleg. Bovendien moet de opdrachtnemer zich volkomen van die werken distantiëren en zich noch openlijk noch bedekt, op enigerlei wijze mengen in de aanbesteding die dan door de opdrachtgever met andere gegadigden zal worden gehouden.

Eis 5. Wijziging van locaties

De locaties waarop opdrachtnemer onderhoud dient uit te voeren op de systemen kan door de loop der jaren wijzigen. Er kunnen locaties worden toegevoegd of worden onttrokken aan het huidige onderhoud.

Eis 6. Uitvoeren werkzaamheden

Bij het uitvoeren van werkzaamheden neemt opdrachtnemer steeds de voorschriften in acht zoals neergelegd in:

- Bijlage 15 Handleiding AsBuild 2.2
- Bijlage 16 CAD-procedureboek Den Haag
- Bijlage 17 BIM Handboek gemeente Den Haag
- NEN 1010

Inschrijver zal altijd de onderhoudswerkzaamheden op veilige wijze uitvoeren (d.w.z. cf. VCA);
De plek waar onderhoud wordt uitgevoerd wordt netjes achtergelaten door inschrijver.
Verpakkingsmateriaal e.d. wordt door inschrijver zelf afgevoerd.

Eis 7. Koppelingen SPIE

Inschrijver dient aan te sluiten bij de voorwaarden en infrastructuur van SPIE.

Eis 8. Facturatie

- Facturatie ten behoeve van preventief onderhoud vindt plaats per locatie, na oplevering en goedkeuring van de onderhoudsrapportage.
- Facturatie ten behoeve van correctief onderhoud vindt plaats per maand achteraf en na goedkeuring door opdrachtgever.
- Facturatie ten behoeve van de implementatie vindt plaats na afronding van deze fase en acceptatie.
- Facturatie ten behoeve van licenties vindt direct na levering en acceptatie plaats.
- Facturatie ten behoeve van projecten (uitbreidingen/wijzigingen) die op later moment plaatsvinden vindt tot een waarde van € 20.000,- (excl. BTW) plaats na goedkeuring achteraf. Voor grotere projecten kan 20% bij opdrachtvertrekking in rekening worden gebracht, 40% bij start werkzaamheden en 40% bij eindoplevering (incl. tekeningen en goedkeuring).

2.2 Preventief onderhoud

Eis 9. Werkprogramma

De opdrachtnemer dient voor aanvang van de onderhoudswerkzaamheden een gedetailleerd werkprogramma met daarbij horende onderhoudsmatrix op te stellen en deze ter goedkeuring aan de opdrachtgever te bieden. In de planning dient aangegeven te worden op welke data de installaties gecontroleerd en/of onderhouden worden. Dit werkprogramma dient elk jaar in januari bij de opdrachtgever te worden ingediend.

Daarbij dient tevens overlegd te worden: de overlegstructuur tijdens de onderhoudsperiode met onder andere een overzicht van welke personen, hoeveel personen en met welke regelmaat overleg wordt gevoerd. Dit werkprogramma neemt de onderhoudsintervallen en –voorschriften in acht zoals deze in deze aanbestedingsdocumenten zijn gesteld.

Pas na goedkeuring van de ter goedkeuring ingediende documenten kan de opdrachtnemer starten met de uitvoering van zijn werkzaamheden.

Alle kosten voor het maken en leveren van een goedgekeurd werkprogramma zijn onderdeel van de opdracht en kunnen niet afzonderlijk in rekening worden gebracht.

De opdrachtnemer dient voor aanvang van werkzaamheden betreffende de uitvoering van het onderhoud, noodzakelijk geachte afwijkingen van tijdstippen van onderhoudswerkzaamheden ten opzichte van het al aanwezige tijdschema in het werkprogramma, goedkeuring te vragen aan de opdrachtgever.

Eis 10. Risicoklasse

Inschrijver is bekend en gaat ermee akkoord dat in overleg met opdrachtgever voor alle locaties een PVE beveiligingsbewijs wordt opgesteld en wordt bijgehouden. Een opleveringsbeveiligingsbewijs ontbreekt op dit moment. Het onderdeel inbraakinstallatie dient te zijn uitgevoerd volgens NEN 8131.

Voor nieuwe locaties wordt altijd aan de hand van de VRKI een risicoklasse indeling bepaald.

In het geval dat bij uitvoering van het onderhoud blijkt dat de installed base (bijlage 5 Prijzenblad, tabblad Samenvatting) onvolkomenheden bevat waardoor niet aan deze NEN 8131 kan worden

voldaan, dan dient opdrachtnemer dit zo spoedig mogelijk te melden aan de opdrachtgever. De opdrachtgever zal dan beslissen of er verdere maatregelen genomen worden om alsnog aan deze voorwaarden te voldoen. Het onderdeel inbraakinstallatie dient te zijn uitgevoerd volgens NEN 8131.

2.3 Beheer

Eis 11. Software beheer

De geïnstalleerde software behorende bij de installaties wordt beheerd door de opdrachtnemer. Het betreft de volgende werkzaamheden:

- Het leveren en installeren van de updates en upgrades voor de applicaties binnen het SMS die binnen de omvang van de opdracht vallen: Thorguard, CAM IQ, Command, Digitale sleutelkast;
- Updates vallen binnen de reguliere beheer- en onderhoudskosten, upgrades worden separaat aangeboden en geïnstalleerd na schriftelijk akkoord van opdrachtgever. De systemen dienen te worden voorzien van de meest actuele upgrade/software versie. (Maintenance releases van Command worden gezien als update, Enhancement releases van Command worden gezien als upgrade). Voor het doorvoeren van een upgrade zal een implementatieplan worden aangeleverd (incl fallback).
- Op verzoek van de opdrachtgever muteren van schakelrechten in inbraaksystemen en protocollen in de systemen;
- Onderzoek naar functionele verstoringen, misbruik en sabotage van de beveiligingssystemen
- Opschonen database (minimaal 1 x per jaar).

Eis 12. Autorisatie beheer

Om onbevoegde bedieningen aan het systeem te voorkomen zijn autorisatieniveaus aangebracht met betrekking tot wie welke handelingen in het systeem mag uitvoeren. Informatie opvragen, ingrijpen in de installaties en wijzigen van bedrijfsparameters in het geheugen hebben elk een eigen autorisatieniveau. Elk autorisatieniveau is toegankelijk met een eigen toegangscode, zodat het bedienen van verschillende disciplines door verschillende autorisatiecodes is beveiligd. De autorisatie heeft zowel betrekking op locatie als de tijd van de toegang. Aanpassingen in deze matrix worden in opdracht van opdrachtgever door opdrachtnemer verwerkt.

Eis 13. Toegangspassen

Opdrachtgever schaft zelfstandig toegangspassen aan en laat deze initialiseren door eindfabrikant. Het beheer van toegangspassen wordt uitgevoerd door opdrachtgever. Het in opdracht van de opdrachtgever wijzigen en aanpassen van de autorisatie matrix behoort tot de werkzaamheden van de opdrachtnemer.

Eis 14. Ondersteuning

Opdrachtnemer levert ondersteuning voor het gebruik van het de installaties.

Dit bestaat uit:

- Ondersteuning (ook 1e lijns telefonische ondersteuning) bij het in stand houden van de huidige beveiligingsinstallaties en het SMS;
- Het (op afstand) oplossen van applicatiestoringen aan de beveiligingsinstallaties/SMS;
- Het ondersteunen van de operators met betrekking tot de bediening, gebruik en wijzigingen van het systeem;
- In voorkomend geval dient opdrachtnemer alle benodigde medewerking te verlenen voor het realiseren van koppelingen of samenwerking met andere systemen (b.v. het HR-systeem).

Ten behoeve van het op afstand oplossen van problemen garandeert Opdrachtnemer dat de inlogverbinding zowel veilig is met betrekking tot de connectie met de gemeente Den Haag als de interne procedures bij de opdrachtnemer zelf. Gemeente Den Haag behoudt zich het recht voor de veiligheid van de verbinding en de interne procedures te allen tijde te (laten) auditen.

Eis 15. Logboek Digitale portal

De opdrachtnemer dient voor de start van de onderhoudswerkzaamheden aan het SMS en de daaraan gekoppelde systemen een digitaal logboek te installeren en bij te houden. Dit betreft zowel het registreren van onderhoud aan software als aan hardware. Het logboek dient de gegevens digitaal te kunnen verwerken en dient centraal op een netwerk te worden geïnstalleerd zodat vanuit meerdere locaties het logboek kan worden benaderd. Het logboek dient tijdig ter goedkeuring aan de opdrachtgever te worden voorgelegd.

Pas na goedkeuring van het logboek door de opdrachtgever en nadat het logboek is geïnstalleerd mag met de onderhoud werkzaamheden worden gestart. De opdrachtgever is niet aansprakelijk voor het niet tijdig ter goedkeuring indienen van het logboek.

Het logboek wordt up-to-date gehouden door opdrachtnemer, dit vindt direct na het uitvoeren van de werkzaamheden plaats. Het logboek dient zodanig te worden opgesteld dat de volgende zaken in tabellen kunnen worden vastgelegd:

- Bedrijfsgegevens en telefoonnummers opdrachtnemer (onderhoud/service organisatie);
- Belangrijke telefoonnummers opdrachtgever en opdrachtnemer;
- Datum oproep;
- Naam medewerker opdrachtgever die de oproep/ storingsmelding heeft verricht;
- Naam van medewerker opdrachtnemer waarmee is gesproken (telefonisch ja/nee);
- Omschrijving van de melding (storing)
- Startdatum van de verrichte werkzaamheden;
- Datum gereed melding werkzaamheden;
- Omschrijving reden werkzaamheden;
- Opgave aan welk systeem /onderdeel werkzaamheden zijn verricht;
- Naam opdrachtverstrekker;
- verrichte acties;
- Soort inspectie;
- Bevindingen;
- Reparaties, aard en datum van de ingreep;
- Wijzigingen aan de installatie;
- Naam medewerker opdrachtgever die de werkzaamheden heeft afgenomen;
- Opmerkingen opdrachtgever n.a.v. van de uitgevoerde werkzaamheden;
- Goedkeuring medewerker opdrachtgever voor acceptatie uitgevoerde werkzaamheden;
- Goedkeuring medewerker opdrachtnemer akkoord verrichte werkzaamheden;
- Aantekeningen van de eindgebruiker m.b.t. storingsmeldingen, en aandachtspunten;
- Aantekeningen (indien van toepassing) m.b.t. documenten of deze moeten worden aangepast;
- Verwijzing naar eventuele checklist.

Het logboek is en blijft eigendom van opdrachtgever. Bij beëindiging contract dienen alle gegevens overgedragen te worden aan de nieuwe partij of opdrachtgever.

Eis 16. Documentatie

Inschrijver is ermee bekend en gaat ermee akkoord dat de documentatie met betrekking tot de installaties altijd overeenstemt met de bestaande situatie en op een uniforme en in de markt geaccepteerd formaat is opgesteld. Deze Documentatie wordt steeds door opdrachtnemer bijgewerkt en is opgesteld in de Nederlandse taal (tenzij uitdrukkelijk anders overeengekomen). Dit betreft minimaal de volgende documenten:

- Blokschema's inbraakbeveiliging met S-Art bus;
- Blokschema's toegangsverlening met koppeling op de RS485 bus;
- Stuurstroonschema's;
- IP overzichtlijst;
- Tekeningen die de configuratie (samenhang en koppeling) van de systemen weergeeft;
- Tekening die de configuratie (opbouw en samenstelling) van de servers en computer clients weergeeft;
- Kastindelingstekeningen;
- Functionele- en gebruikershandleidingen;
- PIR instellingen;
- I/O lijsten;
- Projectietekeningen;
- Coderingslijsten;
- Licenties hardware en software;
- CCTV-instellingen.

Eis 17. Uitbreidingen / Wijzigingen

De opdrachtnemer dient bij uitbreidingen van de installaties alle apparatuur en programmatuur/software, inclusief licenties, te leveren die nodig zijn voor de goede werking van de installaties.

De te leveren apparatuur (servers, pc's etc.) dient de laatste technologie te bezitten die op het moment van bestelling leverbaar en inpasbaar is.

Uitbreidingen en wijzigingen dienen altijd uniform en in overleg met de opdrachtgever worden afgestemd.

Eis 18. IP Nummers automatisering

De opdrachtnemer dient bij uitbreidingen rekening te houden met het gebruik van het IP nummerplan van de Gemeente Den Haag. Deze informatie zal na opdracht met de Opdrachtnemer gedeeld worden. Opdrachtnemer is verantwoordelijk voor het correct bijhouden van de in gebruik zijnde IP nummers.

Eis 19. Revisiegegevens

Bij wijzigingen of uitbreidingen aan installaties dienen de revisiegegevens eenduidig te worden verwerkt. De werkzaamheden kunnen pas opgeleverd worden nadat alle revisietekeningen definitief zijn geaccepteerd door de opdrachtgever.

Op het moment van inbedrijfstelling/ingebruikname van de uitbreidingen of wijzigingen dient door de opdrachtnemer aan opdrachtgever ter beschikking gesteld te worden:

- Complete gebruikershandleiding van alle geïnstalleerde of gewijzigde installatieonderdelen;
- Uiterlijk vier weken na inbedrijfstelling dienen de concept revisiegegevens, in enkelvoud, in een ordner en voorzien van inhoudsopgave in het bezit te zijn van opdrachtgever;

- Uiterlijk zes weken na inbedrijfstellingen dienen de definitieve revisiegegevens, in de ordners als genoemd onder eis 17 (en op eerste verzoek digitaal te overhandigen), voorzien van inhoudsopgave, in het bezit te zijn van opdrachtgever.

Opdrachtgever zal de concept revisiegegevens en tekeningen controleren en de eventuele op- en aanmerkingen opgeven aan de opdrachtnemer. De opdrachtnemer zal de eventuele op- en aanmerkingen verwerken en de gereviseerde tekeningen en documenten definitief aanbieden aan de opdrachtgever.

De revisiegegevens bestaan uit (voor zover van toepassing):

- Gegevens van de uitgevoerde werkzaamheden;
- Garantieverklaring voor minimaal 1 jaar;
- Originele of bijgewerkte software die geïnstalleerd is, inclusief licenties;
- Bijgewerkte groepenverklaringslijsten;
- Bijgewerkte uitdraai van de SMS met daarop alle detectoren, technische meldingen en sabotage groepen;
- Onderverdeelinrichting en eindgroepnummer. waar CCS, CCTV, HDVR en/of externe voedingen op aangesloten zijn (230V);
- Bijgewerkte lijst netwerknummer (TCP/IP adres) en de namen van de diverse Pc's binnen het netwerk;
- Kabellijsten;
- Bijgewerkte componentenlijst;
- Tekeningen (conform het gestelde eisen en normen van de opdrachtgever);
- Stuurstroom schema's of bijgewerkte stuurstroom schema's;
- Blokschema's of bijgewerkte blokschema's;
- Kastindelingstekeningen;
- Bijgewerkte in/output lijst;
- Bijgewerkte IP lijst;
- Berekening capaciteit voor de noodstroom voorziening (het aantal accu's);
- Programmeergegevens van de centrales inbraakbeveiliging digitaal aangeleverd;
- Documentatie met bestelnummer en leverancier gegevens van alle toegepaste materialen en apparatuur;
- Gebruikershandleiding of bijgewerkte gebruikershandleidingen (in tweevoud bij revisiestukken);

2.4 Preventief onderhoud

Eis 20. Uitvoering Preventief onderhoud

De Opdrachtnemer houdt de systemen met de daartoe behorende apparatuur in de gewenste conditie. Tevens dient een continu functioneren te worden bewerkstelligd volgens de in deze aanbesteding opgenomen **SLA (Bijlage 11)**.

Eis 21. Frequentie preventief onderhoud

De frequentie van het preventief onderhoud is per installatie en per onderdeel ingevuld, zie bijlage 6

Eis 22. Voorzorgsmaatregelen uitvoering van preventief onderhoud

Om te voorkomen dat tijdens de onderhoudswerkzaamheden oneigenlijke, ongewenste en nodeloze alarmmeldingen leiden tot alarmopvolging, dient de opdrachtnemer voordat wordt gestart met de onderhoudswerkzaamheden direct daaraan voorafgaand CMK en de PAC in kennis te stellen van de voorgenomen werkzaamheden.

Na beëindiging van de onderhoudswerkzaamheden dient de alarminstallatie te worden aangemeld bij de CMK en de PAC en dient het logboek te worden ingevuld.

Eis 23. Preventief onderhoud SMS

- **Hardware:**

Het onderhoud aan de hardware van het SMS dient als volgt te worden uitgevoerd. Controle en desgewenst nemen van passende acties op:

- SMS clients en aansluitingen
- UPS voeding inclusief de accu's
- Harddisk
- servers (ook de back-up server);

- **Functionaliteit:**

Het onderhoud aan het SMS dient als volgt te worden uitgevoerd. Controle en desgewenst nemen van passende acties op:

- van de bediening en de signalering functies deze controles mogen worden uitgevoerd in combinatie met de uit te voeren testen van de melders;
- Actualiteit projectie plattegronden van de locaties;
- Grafische beelden en de alarmen.
- Thor-Guard logbestanden en het desgewenst opschonen hiervan;
- De melders op het centrale presentatie scherm. Deze controles mogen worden uitgevoerd in combinatie met de uit te voeren testen van de melders;
- Het jaarlijks volledig testen en simuleren van de back-up-/uitwijkfaciliteit en redundantie van het netwerk tussen gebouwen onderling;
- Correcte de zomer-/wintertijd instellingen, doorvoeren binnen 12uur na tijdsmutatie.

- **Koppeling mobiele communicatie (portofoonnet):**

Het controleren van de functionaliteit van de koppeling m.b.t. de doormeldingen van het mobiele communicatiesysteem die op het SMS worden gesignaleerd. De storing dient te worden gesimuleerd vanaf de bron. In geval van gebrek in functionaliteit dient dit verholpen te worden.

- **Inbraakbeveiligingsinstallatie**

De onderhoudswerkzaamheden aan de inbraakbeveiligingsinstallatie betreft controle en desgewenst nemen van passende acties bij:

- Het uitvoeren van visuele controles;
- Doormeten en testen van de voedingen;
- Bijregelen en instellen;
- Reinigen van apparatuur;
- Reinigen van schakelkasten, besturingskasten en apparaatkasten;
- Het uitvoeren van onderhoud en testen conform NEN 8131 en voorschriften fabrikant en controleren of de beveiligingsinstallaties voldoen aan de eisen die gesteld zijn aan NEN 8131.;
- De uitgevoerde testen dienen vastgelegd te worden in het logboek.
- Er dient per gebouw of bouwdeel een lijst (tabel) te worden opgesteld, met de gecodeerde geplaatste componenten. Op deze lijst dienen ook de verschillende testen zoals in dit document zijn omschreven te zijn opgenomen. In de tabel moeten de gecontroleerde en geteste componenten kunnen worden geaccordeerd door middel van een paraaf, een "OK" notering of "niet OK". Na de correcte test dient er door de opdrachtgever of vertegenwoordiger van de opdrachtgever en de opdrachtnemer het betreffende punt te worden geparafeerd voor akkoord. In het logboek dient deze geaccordeerde lijst te worden opgenomen. In de een kolom, onder opmerking, kan een nummer worden genoteerd wat in geval van een afwijking, terug komt op een verzamel-opmerkingenblad;
- Er dient per locatie een gehele functionele test uitgevoerd te worden met betrekking tot de werking van het systeem en het voldoen aan de gestelde eisen.
- Er dient een visuele controle uitgevoerd te worden voor de PIR. Bij de visuele controle dienen de detectoren te worden gecontroleerd op eventuele beschadigingen, bevestiging, toegankelijkheid, (obstakels vrij) detectiebereik en de door de fabrikant voorgeschreven nominale waarde. De afstellingen dienen te worden vastgelegd. Indien zich afwijkingen

voordoen dient de opdrachtnemer dit te melden aan de opdrachtgever en een voorstel te doen voor herstel.

- Er dient een visuele controle uitgevoerd te worden van de magneetcontacten. Bij de visuele controle dienen de Magneetcontacten te worden gecontroleerd op eventuele beschadigingen, bevestiging, toegankelijkheid en de voorschriften van fabrikant. Indien er afwijkingen zich voordoen dient de opdrachtnemer dit te melden aan de opdrachtgever en een voorstel te doen voor herstel.
- Controle Centrale Controle Stuuureenheid
- Doormeldapparatuur

- **CCTV**

Het onderhoud aan het CCTV systeem dient plaats te vinden volgens de voorschriften van de fabrikant en de hieronder beschreven werkzaamheden:

- Het reinigen, controleren en testen van de centrale apparatuur zoals, videosever, videomatrix, multiplexserver, en kwadrantenunit.
- Controle of er geen veranderingen zijn geweest die de werking nadelig beïnvloeden en of er wijzigingen zijn aan de te observeren objecten.
- De opdrachtnemer dient bij het onderhoud van alle camera de setpoints met bijbehorende schermbeelden op te slaan en deze te registreren zodat later bij vervanging of montage na onderhoud de camera op de juiste positie die bij de setpoints horen kunnen worden ingesteld.
- Doorvoeren van de zomer en wintertijd klok aanduiding en setting.
- Het controleren van het activeren van de camera's vanuit het SMS.
- Visuele controle van de camera's en appendages op beschadigingen en bevestigingen.
- Visuele controle van de elektrische aansluitingen op beschadigingen en bevestigingen.
- Reinigen van de lenzen, behuizingen, overige onderdelen en het waar nodig smeren van de draaiende delen.
- Controleren en eventueel bijstellen van de setpoints, scherpte, en diafragma en overige instellingen. De controles dienen uitgevoerd te worden met de aanwezige monitoren waar de beelden normaal op worden weergegeven.
- Het uitvoeren metingen aan de voedingsspanning, videosaal, en eventueel de synchronisatiepuls.
- Het reinigen van de monitoren en controle van de aansluitingen.
- Het controleren van de pane-en til unit.

Het resultaat dient te worden vermeld in het logboek en uitgevoerde testen dienen te worden afgevinkt in de inspectielijst.

- **Toegangsverleningsinstallatie**

Het onderhoud aan de toegangsverleningsinstallatie bestaat uit controle en desgewenst nemen van passende acties, volgens de voorschriften van de fabrikant en betreft minimaal de volgende onderdelen:

- Kaartlezer
- Grendels
- Overneemcontacten

- **Intercomsysteem**

Het onderhoud aan het intercomsysteem bestaat uit controle en desgewenst nemen van passende acties, volgens de voorschriften van de fabrikant.

- **Digitale sleutelkast systeem**

Het onderhoud aan het digitale sleutelkast systeem bestaat uit controle en desgewenst nemen van passende acties, volgens de voorschriften van de fabrikant.

2.5 Communicatie en rapportage

Eis 24. Rapportages

Iedere twee maanden, zijnde uiterlijk de eerste volle week van de daarop volgende maand, dient een managementrapportage en rapportage applicatiebeheer aan opdrachtgever te worden overgelegd met daarin in ieder geval de KPI's en score op kwaliteitsmeting zoals aangegeven in de betreffende wens met betrekking tot KPI's en Kwaliteitsmeting.

De mogelijkheid moet er zijn om aan opdrachtgever managementrapportage te kunnen overhandigen. Hierin moet minimaal de KPI's en kwaliteitsmeting worden weergegeven.

Specifieke bijzonderheden zoals calamiteiten worden terstond overlegd aan opdrachtgever.

Eis 25. Communicatie en Rapportage

Er vindt periodiek overleg plaats tussen opdrachtgever en opdrachtnemer.

Dit vindt plaats op drie niveaus:

- Strategisch: Dit betreft een evaluatie met opdrachtnemer in persoon, dit vindt twee keer per jaar plaats: in de eerste en de zevende maand. Voorafgaand aan deze evaluatie overlegt opdrachtnemer minimaal 2 weken van tevoren de volgende documenten:
 - rapportage uitgevoerde werkzaamheden
 - logboek (wijzigingen sinds laatste overleg)
 - KPI's en kwaliteit
 - lijst s en licentie updates;
- Tactisch: Tactisch overleg vindt plaats tussen de teammanager beveiliging en veiligheid en de betreffende accountmanager van opdrachtgever. In dit overleg wordt de managementrapportage besproken en de planning van inzet voor de komende periode. Dit overleg vindt een keer per kwartaal plaats.
- Operationeel: Dit betreft een voortgangsoverleg waarin het reilen en zeilen op de verschillende panden wordt besproken. Ook hier wordt de managementrapportage van de afgelopen periode besproken. Tactisch/operationeel overleg: een keer in de twee weken.

In de situatie dat opdrachtgever of opdrachtnemer behoefte heeft aan een tussentijds gesprek dient dit ten spoedigste plaats te vinden. Opdrachtnemer beheert in alle overleggen de agenda en de verwerking van het gesprek in een verslag dat ommegaande aan opdrachtgever wordt overlegd.

2.6 Correctief onderhoud en preventief

Eis 26. Correctief onderhoud

De Opdrachtnemer dient correctief onderhoud uit te voeren na melding van een klacht, een storing of een automatische melding. Manuren, voorrijkosten e.d. zijn inbegrepen in de reguliere kosten voor onderhoud, deze worden niet separaat in rekening gebracht. Materiaalkosten worden separaat in rekening gebracht.

Storingen als gevolg van vandalisme, waterschade en andere storingen als gevolg van zaken buiten de invloedssfeer van opdrachtnemer worden separaat in rekening gebracht op basis van de daadwerkelijke ingezette uren en materialen en op basis van de tarieven als aangegeven in de

Inschrijfbladen. Uren en materialen kunnen in rekening worden gebracht. Voorrijkosten kunnen niet in rekening worden gebracht.

Eis 27. Afhandeling en registratie storing

De Opdrachtnemer dient de administratie van de verrichte activiteiten m.b.t. de gemelde storing in het digitale logboek bij te houden. Zie tevens eis 15.

Eis 28. Bereikbaarheid en melding storing

De Opdrachtnemer dient 24 uur per dag telefonisch of fysiek bereikbaar/beschikbaar te zijn voor urgente storingen en calamiteiten (high impact) en zorgt tevens voor reactie en afhandeling hiervan binnen de gestelde responstijden zoals deze in de **SLA (Bijlage 11)** zijn vastgelegd.

De Opdrachtnemer kan op verschillende manieren worden opgeroepen bij storingen en calamiteiten via een bevoegde functionaris van opdrachtgever of via een oproep vanuit de CMK. De Opdrachtnemer krijgt informatie omtrent de aard van de storing, locatie en prioriteit van de melding. Eventuele aanvullende informatie omtrent storingen kan de Opdrachtnemer zelf controleren d.m.v. de SMS cliënt die bij de Opdrachtgever is gestationeerd. Deze storingen worden conform de gestelde tijden in de SLA opgevolgd. De locaties worden geopend door de Opdrachtgever.

Eis 29. Reserve onderdelen

Opdrachtnemer dient voldoende en gangbare reserveonderdelen beschikbaar te hebben om te kunnen voorzien in de SLA.

Eis 30. Inzet servicemonteur

Op verzoek van opdrachtgever kan een servicemonteur worden ingezet (naast preventief of correctief onderhoud, b.v. testen noodstroom) ten tijde van testen en/of wijzigingen aan systemen. Het uurtarief dient inschrijver aan te geven in de Inschrijfbladen.

Aanwezig zijn / stand-by zijn bij werkzaamheden van derde.

Eis 31. Aanbrengen codering

Alle nieuw te installeren of te vervangen componenten worden voorzien van een codering volgens voorschrift van opdrachtgever. Alle aangebrachte coderingen dienen tevens eenduidig te worden weergegeven op de revisietekeningen.

2.7 Ict- en informatieveiligheid

Eis 32. ICT-oplossing binnen informatiebeveiligingssysteem

De ICT-oplossing dient te vallen onder het managementsysteem voor informatiebeveiliging waarover de Inschrijver beschikt.

Eis 33. Verklaring derde

De Inschrijver stelt jaarlijks een verklaring van een onafhankelijke derde beschikbaar waaruit blijkt dat de informatieveiligheid van de ICT-oplossing in lijn is met de eisen van GDH en dat de maatregelen gedurende het gehele jaar goed hebben gefunctioneerd. Dit kan door middel van verklaringen als een SOC 1 type II rapport, een ISAE 3402 verklaring of vergelijkbaar.

Eis 34. SLA en informatiebeveiliging

De gemeente Den Haag en de Inschrijver aan wie de opdracht wordt gegund treden na gunning op eerste verzoek van de Gemeente Den Haag in overleg over informatiebeveiliging en het maken van concretere afspraken hieromtrent. Deze worden vastgelegd in een SLA. Inschrijver dient medewerking te verlenen aan het uitvoeren van redelijke verzoeken van de gemeente ten aanzien van verbetering

van informatiebeveiliging. Ook worden in de SLA procesafspraken vastgelegd omtrent het melden van beveiligingsincidenten en de periodieke rapportage daarover.

Eis 35. Standaarden en controles

Het systeem dient te voldoen aan de volgende standaarden en controles:

1. Het systeem dient beveiligd te worden op basis van actuele standaarden zoals te herleiden uit de OWASP guidelines.
2. Ontwikkeling dient aantoonbaar volgens een secure software development framework plaats te vinden.
3. Een auditlog rond toegang en verwerking van persoonsgegevens dient voor de wettelijke maximale periode beschikbaar te blijven voor analyse in geval van een vermeend datalek.

Eis 36. Servers en infrastructuur

De server(s) en infrastructuur waar gebruik van wordt gemaakt bij de levering van het ICT-systeem dienen te voldoen aan de hardeningsrichtlijnen van het SANS, CIS of NIST. Inschrijver mag een hierop gebaseerde eigen hardeningsrichtlijn opstellen, toegespitst op haar eigen IT omgeving. De richtlijn(en) dienen aantoonbaar te worden nagevolgd bij de ingebruikname van o.a. netwerkcomponenten, (web)servers, databases en besturingssystemen.

Eis 37. Cloud oplossing

Inschrijver heeft in geval van een cloudgebaseerde ICT-oplossing de cloudfrastructuur zo ingericht, dat gebruikers van verschillende organisaties niet bij elkaars gegevens kunnen en geen verstoring voor elkaars dienstverlening op kunnen leveren.

Eis 38. Beëindiging overeenkomst

Inschrijver dient de gegevens van de Gemeente Den Haag weer aan de Gemeente Den Haag ter beschikking te stellen als de overeenkomst wordt beëindigd. Hij dient in dit geval volledige medewerking te verlenen aan en ondersteuning te bieden bij het opstellen en het uitvoeren van een plan voor migratie van de gegevens.

Inschrijver dient bij beëindiging van de overeenkomst de kopieën van de gegevens van de Gemeente Den Haag te vernietigen, zowel in de productie-omgeving als de back-up.

Eis 39. Back-up voorziening

Inschrijver beschikt over een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Daarin staan minimaal eisen opgenomen over dataverlies en hersteltijden. Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere. De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.

Eis 40. Test-omgeving

Inschrijver heeft de ontwikkel-, test en acceptatie omgevingen (separaat of geïntegreerd tot één omgeving) gescheiden van productieomgevingen en maakt geen gebruik van persoonlijke gegevens uit de productieomgeving. Inschrijver houdt te allen tijde systemen en databases (logisch) gescheiden van andere klanten van de inschrijver.

Eis 41. Instructie medewerkers

Medewerkers (intern en extern) bij Inschrijver worden doorlopend gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.

Eis 42. Beheer gebruikersidentificaties

Inschrijver beschikt over een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. Het gebruiken van groepsaccounts is niet toegestaan tenzij dit deugdelijk wordt gemotiveerd. Alle uitgegeven toegangsrechten worden minimaal tweemaal per jaar beoordeeld. De rechten van beheerders worden minimaal ieder kwartaal beoordeeld.

Eis 43. Multifactorauthenticatie

Inschrijver biedt multifactorauthenticatie (MFA) aan. Daar waar dat niet mogelijk is, is de wachtwoordlengte minimaal 8 posities, complex van samenstelling en dient het wachtwoord minimaal halfjaarlijks te worden vernieuwd. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.

Eis 44. Beveiliging serverruimtes inschrijver

Inschrijver heeft beveiligde zones ingericht in haar kantooromgeving en ruimtes met IT-apparatuur. Toegang daartoe wordt strikt beheerst en bijgehouden in een registratie.

Eis 45. Beheer framework

Inschrijver beschikt over een formele procedure voor wijzigingsbeheer op basis van een algemeen geaccepteerd beheerframework met minimaal aandacht voor:

- (a) het administreren van wijzigingen;
- (b) risicoafweging van mogelijke gevolgen van de wijzigingen;
- (c) goedkeuringsprocedure voor wijzigingen.

Testen in productieomgeving vindt niet plaats.

Eis 46. Bezit logbestanden

Inschrijver beschikt over een overzicht van logbestanden die worden gegenereerd. Een logregel bevat minimaal:

- (a) de gebeurtenis;
- (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;
- (c) het gebruikte apparaat;
- (d) het resultaat van de handeling;
- (e) een datum en tijdstip van de gebeurtenis.

Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.

Eis 47. Bezit meldloket beveiligingsincidenten

Inschrijver heeft een meldloket waar beveiligingsincidenten kunnen worden gemeld en een procedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.