Managed Netwerkdiensten en Infrastructuurbeheer Parkeren

Formulier D-1 Conformiteitenlijst

Minimum-eisen Perceel 1

Deze verklaring dient door de Inschrijver naar waarheid te worden ingevuld en dient te worden ondertekend.

Hiermee verklaart Inschrijver ondubbelzinnig met de strekking van het antwoord "JA" te voldoen aan de gestelde Minimum-eisen van Perceel 1

Gemeente Amsterdam

Minimum-eisen Perceel 1 Managed Netwerkdiensten

Functionele Eisen

Nr	Gevraagde dienstverlening	Akkoord (ja/nee)
P1-F1	De Opdrachtnemer voorziet Opdrachtgever van Aansluitingen en biedt transport van IP verkeer met alle Eindlocaties (zie Begrippen & zie Bijlage 07) en Besturingslocaties (zie Begrippen & Bijlage 07) van Opdrachtgever en ten behoeve van communicatie met externe netwerken.	
P1-F2	Directe communicatie tussen eindlocaties (parkeergarages, terreinen of fietsenstallingen) onderling hoeft niet gefaciliteerd te worden.	
P1-F3	De bekabeling en netwerkapparatuur op de parkeerlocaties (de switches, etc.) vallen onder verantwoordelijkheid van de Opdrachtnemer.	
P1-F4	De Opdrachtnemer dient een aantal technologisch verouderde switches en routers te vervangen door managed switches. Opdrachtnemer dient de oude apparatuur af te voeren.	
P1-F5	De Opdrachtnemer levert, beheert en onderhoudt de netwerkverbindingen. Beheer op de netwerkverbinding wordt, binnen het Service Window, pro-actief uitgevoerd. Dat wil zeggen dat eventuele optredende Incidenten door de Opdrachtnemer zelf worden gedetecteerd, geregistreerd en vervolgens worden opgelost.	
P1-F6	De Opdrachtnemer dient de dienstverlening te garanderen tijdens de overgangsfase / uitvoering van het Implementatieplan.	
P1-F7	De netwerkverbindingen dienen geschikt te zijn voor intercom netwerkverkeer (vergelijkbaar met VOIP).	
P1-F8	De netwerkverbindingen dienen geschikt te zijn voor CCTV netwerkverkeer (multicast streaming video).	
P1-F9	De netwerkverbindingen dienen geschikt te zijn voor Pinnen over IP, Parkeer Management diensten, toegang tot internet voor interne gebruikers, kantoorautomatisering.	
P1-F10	De netwerkverbindingen dienen geschikt te zijn voor gebouwgebonden installaties en gebouwbeheersystemen.	
P1-F11	Het netwerk dient geschikt te zijn voor ICS/SCADA netwerkberichten met heel veel korte sturingsberichten.	
P1-F12	De locaties van de MER en de meldkamer van opdrachtgever dienen een 1 GB verbinding te hebben met het netwerk van Opdrachtnemer.	
P1-F13	Een beveiligde verbinding dient mogelijk te zijn tussen leveranciers en het netwerk opdat leveranciers de door de gemeente ingekochte SaaS services aan kunnen bieden of om hun servers en andere apparatuur die binnen het Netwerk draait, op afstand te kunnen beheren. Het type verbinding zal per verbinding tussen partijen en de Gemeente moeten worden afgestemd.	
P1-F14	Gebruikers dienen op basis van hun profiel alleen toegang te verkrijgen tot de omgeving die ze managen op basis van segmentering en toepassing van Identity en Access Management.	
Nr	**Implementatie**	

P1-F15	Oplevering van de dienstverlening cq migratie van de huidige leverancier naar de Opdrachtnemer geschiedt per locatie binnen twaalf (12) weken. Dagen waarop door onvoorziene omstandigheden, waaronder mede begrepen weersomstandigheden, werkzaamheden onmogelijk zijn en waarmee de Opdrachtnemer redelijkerwijs geen rekening kon of hoefde te houden, worden niet meegeteld in deze opleveringsperiode. Indien Leverancier meer tijd nodig denkt te hebben voor een bepaalde locatie, dan dient Leverancier dit te motiveren.	
Nr	**Schaalbaarheid**	
P1-F16	Naast de Verbindingen met alle in Bijlage 07 aangegeven Eindlocaties dient uitbreiding van deze Eindlocaties, in aantallen Verbindingen en in capaciteit (bandbreedte) en beschikbaarheid mogelijk te zijn.	
Nr	**Toekomstvastheid**	
P1-F17	De verbindingen dienen toekomstvast te zijn. Hier wordt onder verstaan: de mate van geschiktheid van de verbindingen om nieuwe ontwikkelingen te kunnen faciliteren. Patches en besturingssysteem op alle netwerkcomponenten, ook bijvoorbeeld firewalls dienen actueel te blijven met marktontwikkelingen opdat altijd supported hardware/software gebruikt worden. Wijzigingen dienen te worden voorgelegd aan Opdrachtgever, met inschatting van consequenties in termen van kosten, afhankelijkheden, doorlooptijd en risico's. Opdrachtgever dient finale toestemming te geven voor het doorvoeren van wijzigingen.	
Nr	**Oplossingsrichting**	
P1-F18	De koppeling tussen het netwerk van garageparkeren en Amsterdam Digitale Poort (ADP) zal buiten Perceel 1 vallen. Deze koppeling zal door de ADP leverancier Motiv geïnitieerd worden. Wel moet Opdrachtnemer zich conformeren aan de aansluitvoorwaarden van ADP: • Voor de verbinding zal een leased line of closed user group via Amsterdam Internet Exchange (AMS IX) gekozen worden. • Firewalls en Customer Premise Equipment (CPE) worden op de eigen locatie van de Opdrachtnemer geplaatst; hieraan dient Opdrachtnemer medewerking te verlenen. • Opdrachtnemer dient zich te houden aan de IP adres conventies welke worden uitgegeven door ADP; • Eventuele Network Address Translation vindt bij Opdrachtnemer plaats en niet binnen ADP.	
P1-F19	Het dient mogelijk te zijn om een verbinding aan te brengen met een eventueel nieuw te contracteren datacenter (locatie nog nader te bepalen, in directe omgeving van Amsterdam).	
P1-F20	Opdrachtnemer biedt een gerouteerd netwerk aan op basis van OSI-model laag 3 inclusief Aansluitingen tussen locaties. De huidige sterpunttopologie op basis van point to point verbindingen van garage naar MER behoeft niet gecontinueerd te worden. De Opdrachtnemer is daarbij vrij in de inrichting van de voor de Dienstverlening benodigde netwerktopologie mits deze aantoonbaar effectief en efficiënt is. De Verbinding voldoet daarbij aan de binnen de industrie gangbare standaarden voor de toegepaste technologie. De Dienst ondersteunt daarbij alle op IP gebaseerde communicatie- en routeringsprotocollen conform de binnen de industrie gangbare TCP/IP standaarden. De geboden routering ondersteunt tenminste het BGP4, OSPF en RIP routeringsprotocol.	

	Het beheer zal daarbij moeten worden uitgevoerd op basis van het uitgangspunt dat niet gebruikte protocollen kunnen worden uitgezet.	
P1-F21	Opdrachtnemer biedt de mogelijkheid om Virtual Private Networks (VPN's) te realiseren. VPN's zijn dusdanig gescheiden dat dataverkeer tussen VPN's niet mogelijk is en het dataverkeer binnen een VPN niet zichtbaar is vanuit andere VPN's. Toekenning van verkeer aan een VPN dient mogelijk te zijn op basis van fysieke poort en Ethernet VLAN-ID. De private netwerk optie dient daarbij het gebruik van Network Address Translation toe te staan.	
P1-F22	De verbinding biedt volledig werkende ondersteuning voor de Open Standaarden IPv4 én IPv6 ('dual stack') -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent in ieder geval dat gebruikers en andere ICT-systemen het ICT-systeem kunnen bereiken via zowel IPv4 als IPv6 of eventueel andere toekomstig protocol zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen.	
P1-F23	Locale Private IP Address Range class A dient behouden te blijven opdat end devices niet omgenummerd hoeven te worden.	
P1-F24	Opdrachtgever eist standaardoplossingen, waarbij configuratie mogelijk is, doch geen maatwerk.	
Nr	**Apparatuurkeuze**	
P1-F25	Voor het realiseren van de verbindingen wordt primair gebruik gemaakt van connectiviteit op basis van vaste fysieke dragers, bijvoorbeeld in de vorm van koper of glasvezel technologie. Indien Opdrachtnemer ten behoeve van de beschikbaarheidseis kiest voor redundante verbindingen dan mag ook gekozen worden voor draadloze oplossingen, mits voldaan wordt aan de beveiligingseisen en voldoende rekening is gehouden met het toegestane frequentiebereik op basis van van toepassing zijnde omgevingswetten/zendvergunningen.	
P1-F26	De huidige apparatuur wordt om niet ter beschikking gesteld aan Opdrachtnemer. Aan het einde van de contractduur dient Opdrachtnemer het eigenaarschap van de dan aanwezige apparatuur over te dragen aan Opdrachtgever.	
P1-F27	Indien er extra hardware en/of software nodig is voor het aansluiten van de dienstverlening, dan vallen deze onder het beheer van de Opdrachtnemer. Dit omvat onder meer onderhoud, firmware updates, monitoring, configuratieaanpassingen, softwaregebruikersrecht en dergelijke.	
P1-F28	De Opdrachtnemer is vrij in de keuze van routers, switches, transmissiemedia en overige middelen nodig voor de realisatie van de gevraagde Netwerkdiensten en is vrij in de wijze van verwerving (zelf aanleggen of inkopen).	
P1-F29	Alle hardware en software componenten dienen op basis van Life Cycle Management te zijn voorzien van actuele (n dan wel n-1) besturingssystemen en beveiligingsupdates. N-1 geldt niet voor beveiligingsupdates; hiervoor geldt dat alle beveiligingsupdates direct geïnstalleerd dienen te zijn. Gebruik van out-of support netwerkonderdelen is niet toegestaan. Wijzigingen dienen te worden voorgelegd aan Opdrachtgever, met inschatting van consequenties in termen van kosten, afhankelijkheden, doorlooptijd en risico's. Opdrachtgever dient finale toestemming te geven voor het doorvoeren van wijzigingen.	
P1-F30	Hosting van apparatuur (switches, firewalls) dient voor zover mogelijk op eigen locatie van de Opdrachtnemer te geschieden.	

P1-F31	De toegepaste technologie is 'state of the art' maar dient daarbij wel te voldoen aan de eis van 'proven technology'.	
P1-F32	De toegepaste technologie dient te voldoen aan de gemeentelijke beleidsuitgangspunten ten aanzien van duurzaamheid en milieu, waarbij aspecten zoals herbuikbaarheid, laag stroomgebruik en lage CO_2 uitstoot dient te worden meegewogen.	
Nr	**Beschikbaarheidseisen**	
P1-F33	De Inschrijver garandeert beschikbaarheid van > 99,8 % van de parkeerlocaties op jaarbasis (24*7*365). Over één (1) kalenderjaar berekend, is het onderhoud en beheer gemaximaliseerd op twintig (20) uur. De beschikbaarheid wordt bepaald door de formule: TH-S B = ----------x 100% TH - B = Beschikbaarheid; - TH = het totaal aantal uren per maand dat de prestatie beschikbaar dient te zijn, exclusief gepland onderhoud; - S = Totale storingstijd over de afgelopen maand.	
P1-F34	Het dient mogelijk te zijn verbindingen met bepaalde parkeerlocaties op verzoek van Opdrachtgever redundant uit te voeren. Indien hier kosten aan verbonden zijn dan dient u deze op te nemen in het Prijzenblad.	
P1-F35	Voor de redundant uitgevoerde verbinding geldt de volgende beschikbaarheidseis. De Inschrijver garandeert beschikbaarheid van > 99,8 % van de parkeerlocaties op jaarbasis (24*7*365). De beschikbaarheid wordt bepaald door de formule: TH-S B = ----------x 100% TH - B = Beschikbaarheid; - TH = het totaal aantal uren per maand dat de prestatie beschikbaar dient te zijn; - S = Totale storingstijd over de afgelopen maand.	
P1-F36	Bij een redundant uitgevoerde verbinding dienen twee gescheiden accessen te zijn aangelegd, waarbij de fysieke dragers (indien van toepassing) voor de Aansluitingen op twee verschillende plaatsen het betreffende gebouw in gaan. Bij een storing op een Aansluiting, als gevolg van kabelbreuk (bijvoorbeeld in geval van graafwerkzaamheden) of anderszins in één route, dan dient daarmee nog steeds communicatie met de locatie mogelijk te zijn via de andere route.	
P1-F37	In geval van een calamiteit of toepassing van een noodscenario dient het mogelijk te zijn om op snelle en eenvoudige wijze een route aan te passen naar één van de bestaande locaties.	
P1-F38	Het PoIP verkeer via de betaalterminals wordt momenteel in geval van netwerkstoringen op basis van internet breakout gecontinueerd. Bij het realiseren van PoIP dient voldaan te worden aan de desbetreffende van toepassing zijnde veiligheidsvoorschriften.	

P1-F39	In het geval er gekozen wordt voor inzet van draadloze technologie (WiFi) dienen de risico's ten aanzien van exclusiviteit en integriteit ingeschat te worden. Beschikbaarheid en prestaties van de draadloze Verbinding dienen hierbij tevoren inzichtelijk worden gemaakt aan de Opdrachtgever.	
P1-F40	Quality of Service: Diensten met specifieke (strikte) karakteristieken dienen te allen tijde end to end de juiste netwerk-resources toegewezen te krijgen voor een optimale werking. Dit conform een QoS-indeling in de volgende verkeersklassen: • Klasse 1 Real time (ITU-T Y.1541 class 0: low latency, low jitter): Deze klasse is van toepassing op Intercom, Parkeer Management Systeem en Betaalterminals. Zij ondersteunt real-time verkeersstromen en verkeersstromen die een gegarandeerde lage vertragingstijd en weinig variatie in vertragingstijden vereisen. In afwijking van de norm hanteren wij een maximale end-to-end vertragingstijd van 10 ms, met jitter kleiner dan 20 ms en packet loss kleiner dan 0,1%. • Klasse 2 (ITU-T Y.1541 class 4: low loss): Deze klasse is geschikt voor CCTV en gebouwgebonden intallaties.	
Nr	**Local Area Network**	
P1-F41	• Bij nieuwbouw of ombouw naar een nieuw Parkeer Management Systeem moet Opdrachtnemer zich door de PMS-leverancier laten aansturen. • Bij aanleg of aanpassing van het CCTV-systeem moet Opdrachtnemer zich door de CCTV-leverancier laten aansturen. • De Opdrachtnemer moet de huisinstallateur aansturen voor het laten aanleggen van elektra voor gebruik door lokale netwerkcomponenten. • De Opdrachtnemer moet de huisinstallateur aansturen voor het verwijderen van oude bekabeling, het realiseren van kabeldoorvoeren, kabelgoten, veldkasten en alle overige bouwkundige aanpassingen die nodig zijn voor het aanleggen van lokale netwerkverbindingen.	
P1-F42	Het LAN heeft één of meer dedicated (V)LAN segmenten met Voorzieningen ten behoeve van Opdrachtgever. Er is geen verkeer van andere partijen over hetzelfde segment.	
P1-F43	Het moet mogelijk zijn om Power over Ethernet injectors te plaatsen ten behoeve van camera's, tenzij in overleg tussen CCTV leverancier en Opdrachtnemer voor routers/switches wordt gekozen waarbij de POE componenten reeds onderdeel zijn van de apparatuur en er geen aanvullende hardware meer nodig is.	
Nr	**Capaciteit van de verbindingen**	
P1-F44	De VPN Verbindingen bieden een asymmetrische (DSL of telefoonlijnen) of symmetrische (glasvezel) capaciteit vanaf 20 Mbps tot en met 1 GB.	
P1-F45	De capaciteit dient binnen locaties dusdanig te zijn dat de beheerders alle in de desbetreffende garage aanwezige camera's in de beheerdersloges kunnen uitkijken.	
P1-F46	Indien toekomstige techniek dit toestaat dienen garages opgeschaald te worden tot hogere bandbreedtes zonder additionele kosten.	
P1-F47	Het is mogelijk om de bandbreedte per locatie zonder verstoring van de dienstverlening naar beneden en naar boven toe aan te passen. Ingeval van een escalatie dient dit direct mogelijk te zijn of gepland binnen een termijn van maximaal twee (2) weken. Voor afschalen van capaciteit kan een ruimere periode in acht worden genomen.	

P1-F48	Het (tijdelijk) wijzigen van de capaciteit van een Verbinding dient stapsgewijs en zonder tussenkomst van een monteur op de Eindlocatie of Besturingslocatie te kunnen plaatsvinden.	
P1-F49	Eventueel medegebruik door derden van deze middelen mag geen enkele invloed hebben op de exclusiviteit, integriteit, beschikbaarheid en prestaties van de Dienstverlening. Ingeval van medegebruik is encryptie vereist.	
P1-F50	Opdrachtnemer dient op basis van voortschrijdende techniek met voorstellen te komen op basis waarvan beschikbaarheid, capaciteit en/of beveiliging verbeterd kan worden. Opdrachtgever behoudt zich het recht voor hier wel of geen gebruik van te maken.	

Beheereisen

Nr	Algemeen	Akkoord (ja/nee)
P1-B1	Voor alle geboden dienstverlening geldt dat de procesvoering en de inrichting van (beheer)processen dient te voldoen aan ITIL V3 standaarden (of soortgelijke marktstandaarden).	
P1-B2	Opdrachtnemer wijst ten behoeve van de installatie, migratie en dienstverlening binnen zijn organisatie een vaste contactpersoon (SPOC) en eventuele vervanger aan voor alle communicatie tussen de Opdrachtgever en Opdrachtnemer.	
P1-B3	Opdrachtnemer voert periodiek overleg (minimaal maandelijks, en indien gewenst wekelijks / tweewekelijks) met Opdrachtgever t.a.v. onder meer Key Performance Indicators (KPI's), escalaties en procesverbetering.	
P1-B4	Voor werkzaamheden die zeer frequent voorkomen (Operationeel beheer), of waarbij sprake is van hoge tijdsdruk (oplossen verstoringen) en waarbij de kans op en impact van miscommunicatie hoog is, eist Opdrachtgever dat de werkzaamheden uitgevoerd worden door medewerkers van Opdrachtnemer die de Nederlandse taal zowel mondeling als schriftelijk vloeiend machtig zijn. Tevens eist de Opdrachtgever dat alle communicatie daarover (mondeling, schriftelijk, elektronisch) vanuit de Opdrachtnemer met medewerkers van Opdrachtgever in de Nederlandse taal gevoerd wordt.	
P1-B5	Operationeel beheer kan voor zover mogelijk remote worden uitgevoerd. Toegang tot de on-premise componenten van Opdrachtgever verloopt altijd via ADP; directe toegang tot de te beheren componenten is niet toegestaan. Ruimtes van waar uit remote beheer voor Opdrachtgever wordt uitgevoerd en de beheerdocumentatie zijn alleen toegankelijk voor geautoriseerde beheerders. De locatie, beheerruimtes, beheerders en werkstations bevinden zich binnen Nederland.	
Nr	**Incident Management**	
P1-B6	Opdrachtnemer biedt Opdrachtgever en Gebruikers welke ten behoeve van hun dienstverlening gebruik maken van de netwerkdiensten een 24/7 telefonisch bereikbare Servicedesk waarvan minimaal 5*8 (09.00-17.00 uur) rechtstreekse contactmogelijkheid met ter zake kundig Nederlandssprekend personeel van Leverancier, waar Opdrachtgever en andere leveranciers onder andere terecht kunnen voor inlichtingen over de status van incidenten, changes, rapportages, etc.	

P1-B7	(Informatie)verzoeken dienen 7 * 24 uur gezonden te kunnen worden aan de Opdrachtnemer aan het door de Opdrachtnemer te bepalen e-mailadres dan wel via een door de Opdrachtnemer geboden incident meldingssysteem.	
P1-B8	Alle aan de Servicedesk per telefoon, email dan wel een via door de Opdrachtnemer geboden incident meldingssysteem gestelde vragen dienen binnen 4 werkuren beantwoord te worden dan wel Opdrachtgever dient binnen 4 werkuren aan te geven wanneer de vraag beantwoord kan worden.	
P1-B9	Opdrachtnemer biedt Opdrachtgever de mogelijkheid om geconstateerde problemen direct te escaleren via mail, SMS of telefoon dan wel een incident meldingssysteem van de Opdrachtnemer. Hiervoor moeten door Opdrachtnemer procedures en escalatiepaden opgesteld worden, op te nemen in het DAP.	
P1-B10	De 1e en 2de lijns helpdesk zijn Nederlandstalig. Voor de 3de lijns ondersteuning is een Engelstalige helpdesk toegestaan.	
P1-B11	Opdrachtnemer dient een Responsetijd te garanderen bij Incidenten van maximaal 15 minuten. Dit betreft zowel aangemelde Incidenten als door de Opdrachtnemer zelf geconstateerde incidenten. De Oplostijd wordt bewaakt door de Servicedesk, conform de afspraken in de Service Level Agreement.	
P1-B12	In geval van uitval van een Netwerkdienst geldt een Target Time To Repair (TTTR) van maximaal 2 uur voor storingen > 3 minuten.	
P1-B13	Indien sprake is van een tekortschietende dienstverlening treden Partijen met elkaar in overleg om nakoming van de Overeenkomst zeker te stellen, waarbij in totaal 3 escalatieniveaus zijn te doorlopen. Opdrachtgever zal voorafgaand aan dat overleg schriftelijk of via email aan de Leverancier aangeven op welke punten de Opdrachtnemer is tekortgeschoten.	
P1-B14	Voor onbeschikbaarheid van een enkelvoudige Aansluiting als gevolg van kabel of glasvezel doorgravingen geldt op dat op jaarbasis 80 % binnen 24 uur en 100 % binnen 48 uur is hersteld.	
P1-B15	Aansluiten van netwerkmonitoring op SOC van Opdrachtgever dient mogelijk te zijn.	
P1-B16	Waar nodig onderneemt Opdrachtnemer pro-actief actie om het niet beschikbaar zijn van applicaties en/of diensten te voorkomen, zowel binnen als buiten kantoortijden.	
P1-B17	De monitoring functie van Opdrachtnemer communiceert direct via email met het Incidentbeheer van zowel de Opdrachtgever als van de Gebruikers die verantwoordelijk zijn voor de volgende bedrijfskritische processen: Intercom, Parkeer Management Systemen en Betaalterminals.	
P1-B18	De Opdrachtnemer moet een melding van Gebruikers in behandeling nemen indien Gebruikers een storing in het netwerk detecteren.	
P1-B19	De Opdrachtnemer dient een melding in bij Gebruikers als de netwerkleverancier een storing in apparatuur van Gebruikers detecteert.	
Nr	**Monitoring en rapportages**	
P1-B20	Opdrachtnemer dient 24 x 7 online Service Rapportages aan te bieden welke automatisch te downloaden en te exporteren zijn. Deze rapportages dienen een goed inzicht te geven in zowel de actuele beschikbaarheid als de historische prestaties voor zowel de algehele dienstverlening als voor wat betreft de dienstverlening welke te herleiden is tot een specifieke locatie of verbinding.	
P1-B21	Opdrachtnemer biedt real-time monitoringsinformatie aan zowel Opdrachtgever als Gebruikers aan. In geval van storingen worden Gebruikers actief geïnformeerd.	

	Standaard levert Opdrachtnemer ten minste monitoring informatie van de diensten aan. Op verzoek van Opdrachtgever dient het ook mogelijk te zijn monitoring informatie aan te leveren op componentniveau.	
P1-B22	Opdrachtnemer mag in eerste instantie haar eigen standaard maandelijkse service rapportage gebruiken. Mocht deze volgens Opdrachtgever naderhand niet toereikend zijn, dan kan Opdrachtgever de Opdrachtnemer verzoeken onderstaande rapportage binnen twee maanden kosteloos te verzorgen. Deze rapportage toont aan in hoeverre de Opdrachtnemer voldoet aan de (contractuele) verplichtingen jegens de Opdrachtgever. De rapportage bevat minimaal: • Uptime van de verbindingen (actueel, maand, kwartaal, kalenderjaar, Rolling 12 months) per locatie; • Tijdstip piek belasting/capaciteitsgroei (dag, week, maand); • Gemiddelde latency (dag,week,maand); • Grafisch overzicht bovenstaande punten; • Trendrapportage over de beschikbaarheid van 99,8 %; • De openstaande issues, changes en problems (incl. doorlooptijd); • Een overzicht van alle verstoringen waaronder verstoringen met een privacy of beveiligingscomponent, intrusion attempts, succesful intrusions. Hierbij dient de oorzaak en structurele oplossing van alle verstoring met hoge prioriteit in voor leken begrijpelijke taal uiteen te worden gezet; • Trendoverzichten van de afgelopen twaalf (12) maanden van aangemelde issues, changes en problems.	
P1-B23	Netwerkverkeer is aantoonbaar beheerst. Misbruik, oneigenlijk gebruik van informatie en sabotage wordt door de Opdrachtnemer traceerbaar gemaakt (audit-trail). De Opdrachtnemer registreert (logging) de netwerk gerelateerde beheerhandelingen die tot op individueel niveau herleidbaar zijn. Opdrachtnemer neemt indien dit binnen zijn opdracht valt passende maatregelen om het misbruik tot een minimum te beperken; voor andere zaken dient Opdrachtnemer contact op te nemen met de desbetreffende Gebruiker(s) opdat deze partijen passende maatregelen kunnen treffen. Opdrachtnemer dient hierover te rapporteren aan Opdrachtgever. Bovengenoemde informatie wordt tenminste één maal per kwartaal in bewerkbare elektronische vorm conform de hiervoor gangbare industrie standaarden door de Leverancier geleverd.	
P1-B24	Opdrachtnemer biedt de Opdrachtgever de mogelijkheid om ten behoeve van monitoring en beheer – op basis van Simple Network Management Protocol (SNMP) - de relevante (onbewerkte) management informatie rechtstreeks uit alle gebruikte actieve netwerk(rand)apparatuur te lezen.	
P1-B25	Opdrachtnemer levert tenminste één maal per etmaal ten behoeve van monitoring en beheer rechtstreeks (onbewerkt) vanuit alle actieve netwerkrandapparatuur de relevante SNMP-traps V2C of V3 (RO).	
P1-B26	Opdrachtnemer levert, in aanvulling op de beschikbaar gestelde SNMP informatie: • tenminste één maal per etmaal de actuele configuratie instellingen van alle actieve kritieke netwerk switches; • tenminste één maal per etmaal de actuele (on)beschikbaarheid van de individuele actieve Aansluitingen en gerelateerde aangesloten diensten of applicaties; • tenminste één maal per etmaal de actuele configuratie instellingen van alle actieve kritieke netwerkcomponenten waaronder tenminste de CPE's en Firewall;	

	• tenminste één maal per etmaal de actuele (on)Beschikbaarheid van de individuele actieve Aansluitingen en gerelateerde CPE. • "real time" security alarmen en security notificaties relevant voor het handhaven van het vereiste beveiligingsniveau.	
P1-B27	Opdrachtnemer wisselt bovengenoemde informatie in bewerkbare elektronische vorm conform de hiervoor gangbare industrie standaarden via een beveiligd communicatiekanaal met één of meerdere door de Opdrachtgever gewenste systemen uit.	
P1-B28	Opdrachtnemer biedt de mogelijkheid om netwerk monitoring apparatuur (probes) op de Eindlocatie van het netwerk aan te (laten) sluiten ten behoeve van monitoring door een derde partij. Informatie afkomstig uit de netwerk monitoring apparatuur wordt via een beveiligd management-besturingslocatie op één of meerdere Eindlocaties aangeboden.	
Nr	**Onderhoudsvenster**	
P1-B29	Opdrachtnemer voert preventieve werkzaamheden enkel binnen het onderhoudsvenster, dagelijks tussen 23:00 – 05:00 uur, uit. Opdrachtnemer dient minimaal drie (3) weken van tevoren deze te bespreken met Opdrachtgever en de Gebruikers. Opdrachtgever en Gebruikers hebben de mogelijkheid om binnen een van te voren met elkaar afgesproken termijn hiervan af te wijken in geval van evenementen, etc. In dit geval treden beide Partijen in overleg om een nieuwe datum vast te stellen.	
P1-B30	Het doorvoeren van software wijzigingen vindt alleen plaats na voorafgaande afstemming met en toestemming van de Opdrachtgever en de Gebruikers (indien en voor zover relevant).	
P1-B31	Gebruikers dienen te allen tijde rechtstreeks contact te kunnen hebben met de Opdrachtnemer ten behoeve van incidenten, changes, etc.	
Nr	**Configuratiebeheer**	
P1-B32	Opdrachtnemer onderhoudt een geactualiseerde CMDB van alle in beheer zijnde netwerkcomponenten en IP adressen, inclusief grafische weergave en locatie specifieke details. Deze CMDB dient te allen tijde en per direct opgevraagd te kunnen worden door de Opdrachtgever.	
P1-F33	Na elke change wordt de CMDB binnen 14 dagen volledig en correct bijgewerkt.	

Commerciële eisen

Nr	Algemeen	Akkoord (ja/nee)
P1-C1	Indien Opdrachtnemer de afspraken met betrekking tot de ICT Prestatie niet, of niet binnen de overeengekomen tijdsduur, nakomt, dan is Opdrachtgever gemachtigd en gerechtigd van Opdrachtnemer te eisen dat deze voor eigen kosten onmiddellijk corrigerende actie onderneemt, waarbij spoeddienstverlening is inbegrepen. Indien Opdrachtnemer hieraan niet voldoet, zal Opdrachtgever de gemaakte extra kosten bij Opdrachtnemer in rekening brengen voor het elders noodzakelijk verwerven van de dienstverlening.	

P1-C2	In het Prijzenblad worden all-in tarieven gehanteerd. Er kunnen geen kosten, eenmalig dan wel naar gebruik, in rekening worden gebracht die niet in het Prijzenblad zijn opgegeven (verborgen kosten als licenties, reis- en verblijfkosten, etc.).	
P1-C3	Opdrachtnemer gaat akkoord met de Verwerkersovereenkomst van de gemeente Amsterdam (onderdeel van AVG).	
P1-C4	De gemeente Amsterdam en de Opdrachtnemer leggen na gunning en aan de hand van de selectieleidraad en de verkregen antwoorden bij de inschrijving de definitieve Service Level Agreement (SLA) en DAP (Dossier Aanvullende afspraken en Procedures) afspraken vast inzake onderhoud en beheer.	
P1-C5	Opdrachtnemer is verantwoordelijk voor het opstellen en actueel houden van zowel DAP als Dossier Financiële Afspraken (DFA).	
P1-C6	Opdrachtnemer dient aan het eind van de contractperiode volledige medewerking te verlenen aan de overdracht van de dienstverlening aan de Opdrachtgever dan wel aan de door de Opdrachtgever aangewezen partij. Opdrachtnemer stelt hiertoe een Exitplan op. Indien hier kosten aan verbonden zijn dan dienen deze in het Prijzenblad opgenomen te worden.	
P1-C7	Opdrachtnemer is verantwoordelijk voor de projectleiding van het Migratieplan. Opdrachtgever heeft als uitgangspunt dat het capaciteitsbeslag op medewerkers van Opdrachtgever bij de migratie minimaal is. De Opdrachtnemer geeft in het Implementatieplan inzicht, in welke kennis en capaciteit (doorlooptijd) op welk moment (planning) nodig van welke partijen nodig is om de migratie succesvol uit te voeren.	
P1-C8	Opdrachtgever accepteert na Gunning slechts die Onderaannemer(s) die gedurende de aanbestedingsprocedure als zodanig zijn aangemerkt en die voldaan hebben aan alle vereisten die door Opdrachtgever aan Onderaannemers zijn gesteld. Na Gunning is wijziging van Onderaannemer(s) slechts mogelijk indien Opdrachtgever hiervoor schriftelijk goedkeuring heeft gegeven. Goedkeuring is slechts mogelijk in geval Onderaannemer voldoet aan de eisen die aan de Onderaannemers worden gesteld in de Aanbestedingsleidraad.	
P1-C9	Opdrachtnemer voert de regie over en zorgt voor effectieve aansturing van de Onderaannemers. Betreffende deze Onderaannemers is Opdrachtnemer het aanspreekpunt van Opdrachtgever en verantwoordelijk voor de kwaliteit van de uitvoering van de werkzaamheden van deze Onderaannemers en de door hen op te leveren Producten en Diensten.	
Nr	Wijzigingen	
P1-C10	De gemeente Amsterdam kan binnen de looptijd van de Overeenkomst te allen tijde naar een nieuw dienst, product, systeem van de Opdrachtnemer overstappen, indien zij dat wenselijk acht. De kosten voor het gebruik van de nieuwe basis dienstverlening en beheer/ onderhoudskosten blijven ongewijzigd, ook indien er meer functionaliteiten aanwezig zijn.	
Nr	Offerteproces Meerwerk	
P1-C11	Opdrachtgever is vrij om te beslissen of Opdrachtnemer opdracht krijgt tot het uitvoeren van Meerwerk, zoals uitbreiding van de capaciteit van een verbinding, het aanleggen van nieuwe verbindingen dan wel het uitvoeren van consultancyopdrachten.	
P1-C12	Opdrachtnemer zal niet eerder met het Meerwerk aanvangen dan nadat hij daartoe schriftelijk en uitdrukkelijk opdracht van Opdrachtgever heeft gekregen. Indien Opdrachtnemer Meerwerk verricht zonder zodanige schriftelijke opdracht is hij met betrekking tot die werkzaamheden niet gerechtigd tot enige vergoeding.	

P1-C13	Mondelinge afspraken of mondelinge opdrachten tot het verrichten van Meerwerk binden Opdrachtgever niet, ongeacht de persoon door wie ze zijn gemaakt of gegeven. Partijen doen afstand van de mogelijkheid zich ter zake van mondelinge afspraken of mondelinge (opdrachten op artikel 3:61 lid 2 BW dan wel artikelen 3:35 en 36 BW te beroepen.	
P1-C14	Indien Opdrachtgever het wenselijk acht om vanwege doorontwikkeling, aanpassingen van processen en/of procedures wijzigen in de ICT Dienstverlening aan te brengen, zal er hiervoor een Requests for Change (RFC) t.b.v. Meerwerk worden ingediend bij Opdrachtnemer. In deze RFC staat opgegeven wat er gewenst is, welke randvoorwaarden daarvoor gesteld zijn/worden en de gewenste doorlooptijd.	
P1-C15	Opdrachtnemer stuurt maximaal één (1) werkdag nadat de RFC van de Opdrachtgever is binnengekomen een ontvangstbevestiging met een referentienummer.	
P1-C16	Binnen twee (2) weken na binnenkomst van de RFC zal Opdrachtnemer een voorstel bij Opdrachtgever neerleggen van de gewenste werkzaamheden/functionaliteiten. Hierin staat onder meer: • dat de offerte opgesteld is op basis van de voorwaarden / condities komende vanuit de Raamovereenkomst; • het referentienummer van de Opdrachtnemer en de Opdrachtgever; • een omschrijving van de gewenste werkzaamheden/functionaliteiten op detail niveau. D.w.z. dat de Opdrachtgever duidelijk kan herleiden welke Dienst/Producten er (functioneel) worden geleverd, tegen hoeveel uren per expertise, de onderlinge rolverdeling, eventuele randvoorwaarden en risico's, de eenmalige kosten, de terugkerende kosten en de planning.	
P1-C17	Opdrachtnemer verstuurt de offerte aan de Contractmanager van Opdrachtgever.	
P1-C18	Opdrachtgever zal de offerte binnen vijf (5) werkdagen inhoudelijk beoordelen, en de Opdrachtnemer hierover informeren.	
P1-C19	Indien de Opdrachtgever zich niet kan vinden in de opbouw van de totaalprijs, zal getoetst worden of deze reëel en marktconform is. Hiermee wordt bedoeld dat alle gehanteerde werkzaamheden, tarieven en doorlooptijd passend zijn bij een aanbieding van vergelijkbare omvang. Indicatief is een bandbreedte die ligt tussen > 20% en < 20%. De bedragen die zich binnen deze bandbreedte bevinden worden door Opdrachtgever als marktconform aangemerkt. Een toets kan uitsluitend worden gedaan door een (nader te bepalen) onafhankelijke partij. Opdrachtnemer en Opdrachtgever zijn verplicht medewerking te verlenen door het ter beschikking stellen van bescheiden en het geven van in- en toelichtingen.	
P1-C20	Indien blijkt dat na de marktconformiteitstoets de bandbreedte door Opdrachtnemer is overschreden, zal de Opdrachtgever de Opdrachtnemer hierover informeren. Opdrachtnemer is verplicht om hierna zijn offerte binnen 3 werkdagen te herzien, waarbij de offerte valt binnen de hierboven gestelde bandbreedte. Indien Opdrachtnemer niet voornemens is om de offerte hierop aan te passen, wordt de maandelijkse betalingen van de terugkerende kosten tijdelijk opgeschort tot aan voldaan is aan de eis.	
P1-C21	Een offerte wordt uitsluitend goedgekeurd nadat beide partijen hebben ondertekend voor akkoord.	

Gemeente Amsterdam

Beveiligingseisen

Nr	Informatiebeveiliging	Akkoord (ja/nee)
P1-S1	De Opdrachtnemer beschikt over een geldig ISO 27001 certificaat. Het certificaat moet van toepassing zijn op alle te leveren diensten , hetgeen ook moet blijken uit de Verklaring van Toepasselijkheid (VVT)/ Statement of Applicability (SOA).	
P1-S2	Binnen het management systeem voor informatiebeveiliging (conform ISO27001) worden de maatregelen uit ISO27002 toegepast.	
P1-S3	De dienstverlening voldoet (behalve aan ISO27001/ISO27002) aan de normen uit de Baseline Informatiebeveiliging Overheid (BIO) tenminste op het Basisbeveiligingsniveau 2 (BBN2). https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/ De opdrachtnemer toont schriftelijk aan op welke manier aan deze normen wordt voldaan.	
P1-S4	Opdrachtnemer zorgt voor anti virus / anti malware protectie en zorgt voor actieve bewaking van de werking van deze protectie.	
P1-S5	Opdrachtnemer zorgt voor veilige configuratie van de netwerkcomponenten conform industrie standaarden/leverancier standaarden. Niet gebruikte protocollen / diensten moeten worden gedeactiveerd. Onveilige protocollen / diensten mogen niet actief zijn.	
Nr	Zonering en segmentering	
P1-S6	Opdrachtnemer is in staat om verschillende zones te onderscheiden. Een zone is een afgebakend netwerk van IT-voorzieningen, waarin gegevens vrijelijk kunnen worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via gedefinieerde koppelvlakken. De te onderscheiden Zones omvatten: een publieke zone (o.a. Internet), een landingszone van de Gebruikers en de gemeentelijke zone van domein Parkeren. Zones zijn dusdanig van elkaar gescheiden dat dataverkeer tussen Zones op netwerkniveau niet mogelijk is en het dataverkeer binnen een Zone niet zichtbaar is vanuit andere Zones. De Opdrachtnemer maakt voor de inrichting van de Zones gebruik van binnen de industrie gangbare technieken voor verkeerscheiding zoals routering, virtueel private netwerken en firewall functies. Het primaire doel van zonering is het isoleren van risico's zodat bedreigingen en incidenten uit de ene zone niet kunnen doorwerken in de andere zone. Zonering maakt daarmee mogelijk dat minimaal de volgende vertrouwensniveaus onderscheiden kunnen worden: niet vertrouwd en vertrouwd.	
P1-S7	Opdrachtnemer is in staat om verschillende netwerksegmenten te onderscheiden ten behoeve van afzonderlijke bedrijfsfuncties zoals PMS, Intercom, CCTV, opdat dataverkeer ten behoeve van elk van deze bedrijfsfuncties elkaar niet beïnvloeden. Opdrachtnemer maakt voor het onderscheid van de segmenten gebruik van binnen de industrie gangbare technieken zoals bijvoorbeeld belichting. Het primaire doel van segmentering is het isoleren van risico's zodat bedreigingen en incidenten uit het ene segment niet kunnen doorwerken in het andere segment.	

P1-S8	Het is niet toegestaan om een verkeersstroom rechtstreeks door meerdere securityzones van het extern koppelvlak te transporteren.	
P1-S9	Met het oog op security dient fysieke scheiding van netwerkzones mogelijk te zijn. Op de plaats van koppeling van netwerk zones dient verkeer gecontroleerd te worden en zo nodig geblokkeerd en doorgelaten te kunnen worden.	
P1-S10	IP segmentering dient te worden toegepast opdat functionaliteiten zoals Parkeer Management Systemen, Intercom, CCTV en gebouwbeheersing van elkaar gescheiden kunnen worden.	
P1-S11	VLAN over verschillende locaties dient mogelijk te zijn ten behoeve van bijvoorbeeld PoIP of intercom.	
P1-S12	De netwerkverbindingen dienen zodanig versleuteld te worden dat de vertrouwelijkheid op het vereiste niveau gewaarborgd is. Tussen netwerk nodes, servers en/of bedrijfsapplicaties dienen open standaarden gebruikt te worden zoals IPsec, TLS 1.2/TLS 1.3 en HTTPS, Secure FTP, S/MIME en Secure SMTP (TLS 1.2/ TLS 1.3).	
Nr	Firewall	
P1-S13	Opdrachtnemer dient voor alle koppelingen te voorzien in een Firewall functie waarbij wordt uitgegaan van het principe: "alle verkeer met externe (IP) netwerkaansluitingen is afgesloten, tenzij expliciet toegestaan". De firewall oplossing dient eerst ter goedkeuring te worden voorgelegd aan Opdrachtgever.	
P1-S14	Opdrachtnemer dient te voorzien in een reverse path check. Dit houdt in dat verkeer vanaf het externe netwerkaansluitingen alleen wordt toegestaan als het (IP) afzenderadres een legaal (public) IP adres is en niet valt binnen de adresbereiken die binnen en/of ten behoeve van het Metropolitan Area Network worden gebruikt.	
P1-S15	De Firewall dient tenminste de volgende functionaliteiten te bieden: • Packet filtering met stateful inspection op basis van tenminste protocol, IP adres en poortnummer; • Ondersteuning van alle TCP/IP protocollen conform de industrie standaarden. Andere in overleg vast te stellen protocollen moeten tevens ondersteund kunnen worden.	
P1-S16	De Firewall biedt, op verzoek van de Opdrachtgever, Network Address Translation (NAT) voor dataverkeer tussen het M@N en de externe netwerkaansluitingen. De ondersteuning van NAT omvat de adresvertalingen in de gebruikelijke vormen (N:1, N:N; N:M) en de translatie tussen IPv4 en IPv6 verkeer.	
P1-S17	Opdrachtnemer dient in aanvulling op de Firewall te voorzien in tenminste IDS en IPS voorziening. De toe te passen IDS/IPS oplossing dient ter goedkeuring te worden voorgelegd aan Opdrachtgever. Tenminste de volgende acties dienen te worden onderscheiden: Blokkeer, Waarschuw, Log, Quarantaine. In geval van calamiteiten moet Leverancier ons hiervoor waarschuwen plus te adviseren ten aanzien van afdoende maatregelen.	
P1-S18	De Opdrachtgever is verantwoordelijkheid voor het opstellen van algemene richtlijnen van wat voor verkeer wel en niet is toegestaan. Opdrachtnemer dient te voorzien in de vertaling van deze invulling naar de ruleset voor de Firewall/IDS/IPS instellingen inclusief implementatie en het onderhoud hiervan.	
P1-S19	De Firewall/IDS/IPS functie dient te voorzien in logging faciliteiten en in het geval van een Incident het genereren van een melding naar het operationeel beheer van de monitoring partij.	

P1-S20	De Firewall/IDS/IPS dient zodanig geconfigureerd te zijn dat deze maximaal 25 ms vertragingstijd toevoegt aan het berichtenverkeer met Internet en andere aangesloten externe netwerken.	
P1-S21	De firewall dient minimaal laag 7 stateful pakketfiltering te ondersteunen.	
P1-S22	Port security: het dient verhinderd te worden dat een ongeautoriseerd device aangesloten wordt op het netwerk en daarmee toegang wordt verkregen tot andere devices. Aanloggen op het VPN netwerk in de vorm van bijvoorbeeld VPN-clients op basis van IPSec en SSL dient op profiel basis mogelijk te zijn om onder andere partijen remote dan wel lokaal beheer uit te kunnen voeren.	
P1-S23	Encryptie, identificatie en authenticatie dienen op applicatieniveau ingeregeld te kunnen worden.	
P1-S24	Alle autorisaties en authenticaties dienen te worden gelogd, inclusief VPN en mutaties van rechten.	
P1-S25	Bij iedere aansluiting op het netwerk van een Gebruiker binnen het netwerk is sprake van een ander beveiligingsniveau en dient er derhalve een beveiligd koppelvlak gebruikt te worden dat logging en inspectie mogelijk maakt.	
P1-S26	Actieve bewaking en Malware detectie dient te worden toegepast, en te worden gerapporteerd aan de Opdrachtgever.	
P1-S27	Opdrachtnemer heeft een uitgewerkt protocol om cyberaanvallen te weren of de eventueel geleden schade op een gestructureerde en adequate manier op te lossen.	
P1-S28	Opdrachtnemer heeft voldoende maatregelen genomen tegen (D)DOS aanvallen, waarbij gewaarborgd wordt dat Gebruikers geen hinder ondervinden in de vorm van netwerkvertragingen tijdens dergelijke aanvallen.	
P1-S29	Opdrachtnemer moet direct virusuitbraken melden aan zowel Opdrachtgever als Gebruikers, en direct passende maatregelen treffen om de gevolgen van de uitbraak te beperken.	
Nr	Change Management	
P1-S30	Bij elke wijziging dient Opdrachtnemer de Opdrachtgever te wijzen op beveiligingsrisico's.	
Nr	Pen- en hack, security tests en audits	
P1-S31	Opdrachtnemer zal jaarlijks een rapport opleveren van een uitgevoerde pen- en hacktest welke door een gerenommeerde derde partij is uitgevoerd op de door de Opdrachtnemer aangeboden oplossing. Indien de Opdrachtnemer niet daar toe in staat is heeft Opdrachtgever het recht tot het uitvoeren van een pen- en hacktest welke zal worden uitgevoerd door een door de Opdrachtgever aan te wijzen derde partij. De kosten hiervan zullen worden doorbelast aan de Opdrachtnemer. Een dergelijke test zal alleen wanneer daar aanleiding toe is meerdere keren per kalenderjaar worden uitgevoerd. Opdrachtnemer zal naar aanleiding van de bevindingen zijn medewerking verlenen aan het oplossen van issues en het uitvoeren van verbeteracties.	
P1-S32	Opdrachtgever zal jaarlijks een assurance verklaring (SOC 2/SOC3 of ISAE3402) opleveren op de door de Opdrachtnemer aangeboden oplossing. Indien de Opdrachtnemer niet daar toe in staat is heeft Opdrachtgever het recht tot het uitvoeren van een audit welke zal worden uitgevoerd door een door de Opdrachtgever aan te wijzen derde partij. De kosten hiervan zullen worden doorbelast aan de Opdrachtnemer.	

	Een dergelijke test zal alleen wanneer daar aanleiding toe is meerdere keren per kalenderjaar worden uitgevoerd. Opdrachtnemer zal naar aanleiding van de bevindingen zijn medewerking verlenen aan het oplossen van issues en het uitvoeren van verbeteracties.	
P1-S33	Opdrachtnemer voert periodieke / maandelijkse vulnerability scanning uit met een met de Opdrachtgever af te stemmen tool. Gevonden kwetsbaarheden worden onderzocht op hun potentiele impact en waar mogelijk gedicht. Dienstverlener rapporteert hierover, ook bij een goed resultaat, aan Opdrachtgever.	

Ondertekening:

Naam Inschrijver: .....

Naam persoon: .....

Datum: .....

Handtekening: .....

Deze Appendix dient te worden ondertekend door een daartoe rechtsgeldig bevoegd persoon.