

Assumpties & Uitsluitingen

Uno Automatiseringdiensten B.V. — Raamovereenkomst Catering- en
Horecadiensten voor Gemeente Middenstad

Datum: 11/26/2025

Doel en scopekader

- Scopeklaring: aanbod betreft ICT-beheer-, security- en continuïteitsdiensten voor de (cloud- en infrastructuur)systemen die de gemeentelijke dienstverlening ondersteunen, inclusief eventueel horeca- en cateringgerelateerde systemen (bijv. kassa/POS, reserveringssystemen, netwerk/Wi-Fi, backoffice). Geen levering van catering- of horecaproducten, personeel of exploitatie. Juridisch voorbehoud: fysieke catering- en exploitatieactiviteiten vallen expliciet buiten scope.
- KO-conformiteit: ISO 27001 en ISO 9001 aanwezig; 24/7 bereikbaarheidsdienst geborgd. Bewijs: actuele certificaten en dienstrooster beschikbaar op verzoek.

Assumpties (SMART, PDCA-conform)

- A-01 Toegang en informatie
 - SMART: opdrachtgever levert binnen 5 werkdagen na gunning noodzakelijke toegangen (tenant, admin, netwerk), documentatie (huidige architectuur, CMDB, leverancierslijst) en een lijst kritieke systemen.
 - PDCA: Plan (inventarisatie), Do (toegang inrichten), Check (toegangsreview per kwartaal), Act (intrekken/aanpassen).
 - KPI: onboarding gereed binnen 20 werkdagen na volledige toegang.
 - Risico: vertraging onboarding → impact op SLA-start.
 - Bewijs: toegangsmatrix, change- en ticketlog.
- A-02 Locatietoegang en bereikbaarheid
 - SMART: alle locaties zijn tijdens kantoortijden vrij toegankelijk; voor P1 24/7 toegang indien on-site nodig.
 - PDCA: Plan (calamiteitenpas), Do (on-site), Check (toegangstests), Act (escalatieroute).
 - KPI: P1 on-site inzet binnen 2 uur indien vereist.
 - Risico: vertraagde toegang → overschrijding oplostijd.
 - Bewijs: toegangspassenregister, dispatch-logs.
- A-03 Netwerk- en internetkwaliteit
 - SMART: internet- en LAN/WAN-verbindingen voldoen aan performance- en beschikbaarheidsnormen passend bij 99,8% systeem-uptime.
 - PDCA: Plan (baseline), Do (optimalisaties), Check (monitoring), Act (verbeterplan).
 - KPI: Beschikbaarheid kritieke systemen ≥ 99,8%/maand.
 - Risico: ondermaatse connectiviteit → KPI-falen buiten toerekenbaarheid.
 - Bewijs: monitoringrapporten, ISP SLA's.
- A-04 Licenties en rechtsgeldigheid
 - SMART: Microsoft 365 en overige softwarelicenties zijn rechtmatig; licentiebeheer wordt actueel gehouden.
 - PDCA: Plan (SaaS-inventaris), Do (true-up), Check (kwartaalreview), Act (correcties).
 - KPI: 0 licentie-tekortmeldingen per kwartaal.
 - Risico: compliance-issues → operationele blokkades/kosten.
 - Bewijs: licentieoverzichten, auditrapporten.

- A-05 EU-dataverwerking en privacy
 - SMART: alle data wordt binnen EU verwerkt; geen doorgifte buiten EU zonder schriftelijke instemming.
 - PDCA: Plan (DPA, subprocessor-lijst), Do (EU-locaties), Check (jaarlijkse review), Act (mitigaties).
 - KPI: 100% EU-dataroute conform beleid.
 - Risico: AVG-non-compliance → juridisch/boeterisico.
 - Bewijs: DPA, datalokatieverklaringen, DPIA-registraties.
- A-06 VOG en personeel
 - SMART: waar vereist VOG beschikbaar vóór on-site inzet; onboarding lead time 2 weken.
 - PDCA: Plan (screeningsbeleid), Do (aanvragen), Check (geldigheid), Act (toegang intrekken).
 - KPI: 100% VOG-conformiteit.
 - Risico: toegangswijziging → vertraging onsite-werk.
 - Bewijs: screeningsoverzicht (geanonimiseerd).
- A-07 Change governance
 - SMART: changes via goedgekeurde CAB-procedure; doorlooptijden afgestemd op impactclassificatie.
 - PDCA: Plan (RFC), Do (implementatie), Check (post change review), Act (standaardisatie).
 - KPI: 0 high-impact changes zonder CAB-goedkeuring.
 - Risico: ongecontroleerde wijzigingen → verstoringen.
 - Bewijs: ITIL-change logs, CAB-notulen.
- A-08 24/7 incidentafhandeling voor P1
 - SMART: P1 responstijd < 30 min, oplostijd < 4 uur; P2/P3 conform kantoortijden tenzij anders overeengekomen.
 - PDCA: Plan (roosters), Do (tier-1/2/3), Check (SLA-rapport), Act (capaciteitsbijsturing).
 - KPI: P1-respons en -oplossing conform SLA.
 - Risico: capaciteitsdruk → escalatie naar vendor.
 - Bewijs: NOC-roosters, incidentstatistieken.

Uitsluitingen en juridische voorbehouden

- Scope-uitsluitingen
 - Geen levering/exploitatie van catering/horeca, geen fysieke uitserver-/keukenwerkzaamheden.
 - Levering en beheer van on-site hardware buiten scope, tenzij separaat overeengekomen.
 - Third-party SaaS/applicatiesupport beperkt tot redelijke inspanningen en vendor-coördinatie; vendorkosten doorbelast.
 - Projecten buiten regulier beheer (migraties, grote upgrades) vallen niet onder vast maandtarief; separaat voorstel.
 - Eindgebruikersadoptie/training uitsluitend op verzoek en separaat geoffreerd.
- Juridische voorbehouden
 - Aansprakelijkheid: beperkt tot directe schade conform toepasselijke voorwaarden; geen aansprakelijkheid voor gevolgschade, gederfde winst of vendor/utility-storingen.

- Overmacht: o.a. uitval nutsvoorzieningen, grootschalige cloudprovider-storing, stakingen buiten invloedssfeer.
- AVG: DPA vereist; opdrachtgever is verwerkingsverantwoordelijke, Uno Automatiseringdiensten B.V. verwerker.
- Veiligheid: encryptie in transit (TLS 1.2+) en at rest (AES-256) als standaard; afwijkingen alleen na schriftelijke goedkeuring opdrachtgever.
- Subverwerkers: inzet conform vooraf gedeelde lijst; wijzigingen met tijdige notificatie.
- Toetsing: auditor-toegang op redelijke basis en met inachtneming van security.

Financiële consequenties (bij afwijking van aannames/scope)

- Extra inzet buiten scope (projectmatig, spoedchanges, vendor-escalaties) wordt vooraf geoffreerd; uitvoering na akkoord.
- On-site inzet buiten kantoortijden op verzoek opdrachtgever bij niet-P1 wordt separaat in rekening gebracht.
- Kosten van derde partijen (cloudproviders, ISV's, ISP's, hardware vendors) worden 1-op-1 doorbelast conform hun voorwaarden.
- Herstelwerk na niet-autorisierte wijzigingen door derden wordt als meerwerk behandeld.
- Indien vereiste toegangen/informatie niet tijdig worden geleverd en SLA's daardoor niet haalbaar zijn, vervalt de boeteplicht voor dat deel en kunnen extra kosten ontstaan voor versnelling/herstel.

Randvoorwaarden en afhankelijkheden opdrachtgever

- Beschikbaar stellen van key-contacts (functioneel, technisch, security, privacy).
- Tijdige besluitvorming binnen afgesproken termijnen voor changes en uitzonderingen.
- Vaststelling onderhoudsvensters per locatie/organisatieonderdeel.
- Up-to-date architectuurdokumentatie en CMDB-exports bij start en per kwartaal.
- Veiligheids- en huisregels per locatie vooraf beschikbaar.

Kruisverbanden W-xx ↔ KPI ↔ Risico ↔ Bewijs

- W-01 Beschikbaarheid kritieke systemen (Monitoring + Continuïteit)
 - KPI: $\geq 99,8\%$ /maand
 - Risico: single points of failure, ISP-storing
 - Bewijs: monitoringrapporten, failover-tests, BCP/DR-testverslagen
- W-02 P1 incidentrespons 24/7
 - KPI: respons < 30 min, oplos < 4 uur
 - Risico: escalatievertraging bij leveranciers
 - Bewijs: incident- en escalatielogs, roosters, call-records
- W-03 Patch- en kwetsbaarhedenmanagement
 - KPI: kritieke patches binnen 7 dagen uitgerold
 - Risico: exploit van bekende kwetsbaarheden
 - Bewijs: patchkalender, tooling-rapporten, change logs
- W-04 ITIL-servicedeskprocessen
 - KPI: first-time-fix $\geq 65\%$ (P3/P4), klanttevredenheid $\geq 8/10$
 - Risico: langere doorlooptijden door procesafwijkingen
 - Bewijs: procesaudits ISO 9001, CSAT-rapporten

- W-05 AVG/EU-dataverwerking
 - KPI: 100% EU-dataverwerking, 0 datalekken met ernstige impact
 - Risico: sancties en reputatieschade
 - Bewijs: DPA, subprocessor-lijst, verwerkingsregister, ISO 27001-certificaat
- W-06 Escalatie- en continuiteitsplan (BCP)
 - KPI: jaarlijkse BCP-test, RTO/RPO conform afgesproken profielen
 - Risico: onvoldoende herstelcapaciteit bij calamiteit
 - Bewijs: BCP-document, testrapportages
- W-07 Proactieve netwerk- en endpointmonitoring
 - KPI: detectie-tijd kritieke alerts < 15 min
 - Risico: late detectie → grotere impact
 - Bewijs: SIEM/NOC-alertlogs, rapportages
- W-08 Microsoft 365 ondersteuning
 - KPI: tenant health 100% compliant met baseline, 0 mislukte kritieke beveiligingscontroles
 - Risico: accountcompromis, dataverlies
 - Bewijs: Secure Score-rapport, Conditional Access policy-overzicht

Bewijs en conformiteit

- Certificering: ISO 27001 en ISO 9001 actueel; certificaten beschikbaar ter inzage.
- Processen: ITIL-gebaseerde servicedesk, change- en incidentmanagement ingericht en aantoonbaar toegepast.
- Security: logging en audittrails bewaard conform beleid; toegang gebaseerd op least privilege en periodieke review.
- Rapportage: maandelijkse SLA-rapportage; kwartaalreview (PDCA-verbeteracties).

Specifieke juridische uitsluitingen m.b.t. aanbestedingskader

- Deze aannames & uitsluitingen zijn bedoeld als verduidelijking van scope en randvoorwaarden en laten aanbestedingsrechtelijke bepalingen van de opdrachtgever onverlet. In geval van strijdigheid prevaleert de definitieve contracttekst na gunning, met uitzondering van non-negotiables inzake AVG, informatiebeveiliging en datalocatie (EU-only), die essentieel zijn voor het behalen van de SLA's en KO-criteria.

Financiële en operationele samenvatting (SMART)

- SLA-inwerkingtreding: start per datum volledige toegang en afronding onboarding; SLA-meting vanaf eerste volledige kalendermaand.
- Garantie: 12 maanden op projectmatige opleveringen (deliverables), niet op doorlopende beheerprestaties; defects verholpen zonder meerkosten binnen redelijke termijn.
- Prijzen: tarieven vast conform pricing policy; meerwerk enkel na voorafgaande schriftelijke akkoordverklaring.

Aannames uit extras bevestigd

- Opdrachtgever levert tijdig toegangen en informatie aan.
- Locaties binnen kantoortijden toegankelijk.

- Besluitvorming binnen afgesproken termijnen.
- Netwerkverbindingen voldoen aan minimale eisen.
- Licenties (M365 en overige) zijn rechtmatig.

Uitsluitingen uit extras bevestigd

- On-site hardwarelevering/-beheer buiten scope.
- Third-party SaaS/appsupport buiten directe verantwoordelijkheid.
- Projectwerk buiten regulier beheer niet in vast tarief.
- Onvoorziene meerwerkzaamheden separaat.
- Adoptie- en trainingen alleen op verzoek.

Benodigde input:

- Overzicht kritieke systemen en prioritering (P1/P2/P3).
- Actuele netwerk- en internetovereenkomsten per locatie (SLA's ISP).
- Microsoft 365 tenantdetails en security-baseline (huidige Secure Score).
- Locatielijst met toegangsprocedures en on-site veiligheidsregels.
- Contactlijst (operationeel, escalatie, privacy/security).
- Subprocessor-/leverancierslijst en bestaande supportcontracten.
- Concept DPA en gewenste RTO/RPO-profielen per dienst.
- CAB-kalender en onderhoudsvensters per omgeving.

Benodigde input: