Assumpties & Uitsluitingen

Digital Ease B.V. — Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad

Datum: 12/8/2025

Aannames & Uitsluitingen – Digital Ease B.V. – Referentie: GV-IT-2026-001

1. Toepasselijkheid en scope

- Scope-clarificatie: dit document ziet op IT-beheer, -onderhoud en -beveiliging (cloud/infrastructuur) conform de KO/must/SLA-eisen in de aanbesteding. Titelincongruentie (“Catering- en Horecadiensten”) wordt geacht een administratieve vergissing. Indien de feitelijke scope catering/horeca betreft, is dit document niet van toepassing en vervalt zonder kosten.
- Raamovereenkomst: dienstverlening op basis van raamovereenkomst (diensten) met inzet 24/7 bereikbaarheidsdienst voor P1, conform EMVI-kaders.
- Voorrang: bij interpretatieverschillen prevaleren aanbestedingsstukken. Dit document geeft aannames, uitsluitingen en financiële consequenties transparant weer.

2. Operationele aannames (SMART en PDCA)

- Toegangen en informatie (P): opdrachtgever levert tijdig accounts, autorisaties, netwerktekeningen en CMDB (D: binnen 5 werkdagen na gunning; C: check in kick-off; A: escalatie naar stuurgroep na 2 werkdagen vertraging).
- Locatietoegang (P): toegang tot alle locaties binnen kantoortijden en gepland voor changes buiten productie (D: vensters do–vr 20:00–06:00; C: change-kalender; A: herplannen + impactanalyse).
- Connectiviteit (P): internet- en LAN-verbindingen voldoen aan minimale eisen (≥100 Mbps, latency <30 ms binnen NL) (D: pre-check; C: meetrapport; A: mitigatie/advies upgrade).
- Licenties (P): rechtmatige Microsoft 365- en overige licenties door opdrachtgever of inkoop via Digital Ease (D: licentie-audit; C: SAM-rapport; A: non-compliance-ticket).
- Dataruimte EU (P): alle data binnen EU, subverwerkers binnen EER (D: DPA’s; C: jaarlijkse controle; A: stopzetting datastromen buiten EU).
- Besluitvorming (P): besluiten binnen afgesproken termijnen (D: 5 werkdagen standaard; C: besluitlog; A: escalatie-ladder).
- Onsite hardware (P): levering/beheer on-prem hardware uitsluitend indien separaat overeengekomen (D: separate PO; C: aftekenlijst; A: uit scope).
- Third-party SaaS (P): functionele applicatiesupport ligt bij leverancier; wij leveren infra/connectiviteit en M365-administratie (C: RACI; A: warme overdracht).
- Monitoring & patching (P): 100% kritieke endpoints en servers onder monitoring/EDR en patching (D: agent-deploy binnen 15 werkdagen; C: dekkingrapport; A: wave-2 deploy + onsite indien nodig).
- VOG (P): VOG verplicht voor onsite engineers op verzoek (D: registratie HR; C: steekproef; A: inzet enkel geverifieerd personeel).

3. Juridische uitsluitingen en randvoorwaarden

- Compliance: ISO 27001, ISO 9001, NEN 7510 geborgd. Indien eisen conflicteren, geldt hoogste norm.
- AVG/DPA: verwerkersovereenkomst en subverwerkerslijst (Digital Ease, IT Infra Group, SecureOps NL) voorafgaand aan start. Geen doorgifte buiten EER.
- Aansprakelijkheid: conform aanbestedingsvoorwaarden; bij ontbreken daarvan: directe schade max. 100% jaarvergoeding, geen gevolgschade, overmacht uitgesloten van aansprakelijkheid.
- Intellectuele eigendom: eigen scripts/tooling blijven eigendom Digital Ease; configuraties en documentatie m.b.t. klantomgeving blijven eigendom opdrachtgever.
- Penetratietesten: uitsluitend na schriftelijke toestemming en afgestemd venster.
- Security-by-design: standaard least privilege, MFA verplicht voor beheerdersaccounts.
- Exit/retourdata: bij einde overeenkomst overdracht in gangbare formaten; datawiping conform NIST 800-88 op verzoek.

4. Financiële consequenties en tarieven

- Prijzen: tarieven vast (pricing locked) gedurende eerste 12 maanden; jaarlijkse indexatie per 1-1 op CBS CPI Alle Huishoudens (negatief uitgesloten, cap 5% p.j.).
- Out-of-scope/meerwerk: vooraf geaccordeerd, urencalculatie tegen afgesproken uurtarieven; changes buiten onderhoudsvenster: +25% toeslag; storingen veroorzaakt door derde partijen: doorbelasting.
- Onsite interventies: reistijd/–kosten conform staffel NL; spoed onsite binnen 4 uur: +35% toeslag.
- Service credits (voorstel, indien niet strijdig met aanbestedingsvoorwaarden):
    - Beschikbaarheid: bij <99,8%: 5% maandfee per 0,1% tekort, max. 20%.
    - P1-responstijd: 2% per incident >30 min, max. 10% per maand.
    - P1-oplostijd: 2% per incident >4 uur, max. 10% per maand.
- Warranty: 12 maanden op project-deliverables (documentatie, configuraties). Niet van toepassing op door derden geleverde hardware/software.

5. Uitsluitingen (expliciet)

- Levering en beheer van onsite hardware buiten scope, tenzij separaat vastgelegd.
- Functionele applicatiesupport van third-party SaaS/applicaties buiten directe verantwoordelijkheid.
- Projecten/adoptie/gebruikerstraining buiten regulier beheer; op aanvraag/offerte.
- Onvoorziene werkzaamheden door oorzaak buiten invloedssfeer (stroomuitval, ISP-fouten, DDoS op ISP, force majeure) vallen buiten SLA-credits.
- Security-incidenten voortkomend uit niet-naleving klantbeleid (geen MFA, verouderde OS) na aantoonbare advisering vallen buiten aansprakelijkheid.

6. W-xx ↔ KPI ↔ Risico ↔ Bewijs (SMART-koppelingen)

- W-01 KO ISO 27001 → KPI: 0 major non-conformities per auditjaar → Risico: datalek/boete → Bewijs: geldig certificaat + SoA + auditrapport.
- W-02 KO ISO 9001 → KPI: ≤3 minor non-conformities/jaar → Risico: procesfouten → Bewijs: certificaat + interne auditlog.
- W-03 KO 24/7 bereikbaar → KPI: P1-responstijd ≤30 min (24/7) → Risico: impactcontinuïteit → Bewijs: wachtdienstroosters, ACD-rapport.
- W-04 Must P1 responstijd 30 min → KPI: ≥98% binnen target/maand → Risico: escalaties → Bewijs: tickets met tijdstempels.
- W-05 Must beschikbaarheid 99,8% → KPI: ≥99,8%/maand → Risico: productie-uitval → Bewijs: monitoring-export (uptime).
- W-06 Must monitoring/patch → KPI: ≥95% kritieke patches ≤14 dagen, ≥99% AV/EDR coverage → Risico: kwetsbaarheden → Bewijs: patch/EDR-dashboards.
- W-07 Must ITIL servicedesk → KPI: FCR ≥60%, CSAT ≥8,0/10 → Risico: doorlooptijd → Bewijs: ITIL-procesbeschrijvingen, KPI-rapportages.
- W-08 Must data EU → KPI: 100% datalokaties EU → Risico: AVG-schending → Bewijs: DPA’s, hostinglocaties.
- W-09 Must escalatieprocedure → KPI: 100% escalaties binnen matrix doorgevoerd → Risico: vertraging herstel → Bewijs: procedure + casuslogs.
- W-10 Must BCP → KPI: 1x per jaar getest, RTO/RPO gehaald → Risico: lange uitval → Bewijs: BCP + testverslag.
- W-11 Must VOG → KPI: 100% VOG bij onsite → Risico: integriteitsincident → Bewijs: VOG-register (intern).
- W-12 Must proactieve monitoring → KPI: 24/7 alerting, MTTD <15 min → Risico: late detectie → Bewijs: SIEM/EDR-alertlogs.

- W-13 Must M365 support → KPI: P1 M365 opgelost <4 uur; ≥95% binnen target → Risico: productiviteitsverlies → Bewijs: tickets, change-logs.

7. PDCA-borging (governance en audittrail)

- Plan: kwartaalroadmap (patching, upgrades), risico-register, change-kalender afgestemd met opdrachtgever.
- Do: uitvoering via ITIL (Incident/Problem/Change), 24/7 monitoring, wekelijkse patch-runs.
- Check: maandrapportage SLA/KPI, security-rapport (EDR, kwetsbaarheden), CSAT-samenvatting.
- Act: service review (maandelijks), verbetermaatregelen met eigenaar/deadline, her-test van maatregelen in volgende cyclus.

8. Partners en subverwerkers

- IT Infra Group: netwerk- en datacenterexpertise binnen EU; DPA en verwerking binnen EER.
- SecureOps NL: SOC-monitoring/EDR-tuning; verwerking binnen NL/EU.
- Regie: Digital Ease is hoofdaannemer en single point of contact; subverwerkers conform DPA-lijst.

9. Escalatie en continuïteit

- Escalatiematrix: 3 niveaus (operatie, management, directie) met reactietijden 2u/8u/24u.
- Continuïteit: BCP met RTO 4 uur (kritieke services), RPO 15 min (log/EDR); jaarlijkse test en rapportage.
- Major Incident-procedure: war room binnen 30 min, updates elke 60 min, post-incident review binnen 5 werkdagen.

10. Geldigheid en termijnen

- Ingangsdatering: na gunning en ondertekening raamovereenkomst.
- Aanbiedingsgeldigheid: 90 dagen vanaf indiening (2026-01-20).
- Voorwaardenconflict: aanbestedingsvoorwaarden prevaleren; dit document werkt aanvullend/clarificerend.

Benodigde input:

- Overzicht huidige omgeving: aantallen servers/endpoints, locaties, kritieke systemen, supportvensters.
- CMDB en netwerkdiagrammen; lijst met integraties/koppelingen.
- Huidige leverancierslijst + contractuele beperkingen; contactpunten per leverancier.
- Beheeraccounts en toegangsprocedures; gewenste autorisaties.
- Datalocaties en compliance-eisen per dataset; bestaande DPA’s.
- Escalatiematrix opdrachtgever (namen, bereikbaarheid).
- Change freeze periodes en businesskalender (kritieke data/peaks).
- Microsoft 365 tenant-instellingen en licentieoverzicht.
- Securitybeleid (MFA, wachtwoord, device compliance) en gewenste uitzonderingen.

Benodigde input: