EMVI / Plan van Aanpak

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

Datum: 12/8/2025

EMVI / Plan van Aanpak — Raamovereenkomst ICT-beheer en -beveiliging (referentie GV-IT-2026-001), Gemeente Voorbeeldstad

1. Managementsamenvatting Doel: stabiele, veilige en duurzame ICT-dienstverlening voor Gemeente Voorbeeldstad met aantoonbaar hogere beschikbaarheid en kortere incidentafhandeling dan de minimumeisen, conform EMVI-criteria Kwaliteit (40%), Duurzaamheid (20%), Risicobeheersing (20%) en Prijs (20%).

Onze kernbeloften (SMART):

- Beschikbaarheid kritieke systemen: 99,90% per kalendermaand (≥99,8% vereist) gemeten per dienst en per site, met service credits bij onderprestatie. KPI K-01, W-01, Risico R-01; bewijs E-02/E-09.
- Responstijd P1: ≤15 minuten, 24×7×365, 99% van de meldingen; oplostijd P1: ≤2 uur in 95% van de gevallen (eis ≤4 uur). KPI K-02/K-03, W-02/W-03, Risico R-02; bewijs E-03/E-09.
- Monitoring & patchmanagement: 100% van kritieke assets onder 24/7 monitoring; kritieke beveiligingsupdates binnen 48 uur, hoog binnen 7 dagen, overig binnen 21 dagen. KPI K-04/K-05, W-04, R-03; bewijs E-02/E-09.
- EU-only dataverwerking: 100% data, back-ups en logs binnen EU-regio’s (Azure West/North Europe, M365 EU Data Boundary). KPI K-06, W-05, R-04; bewijs E-07/E-10.
- ITIL-processen: Incident, Problem, Change conform ITIL v4, met maandelijkse PDCA-review en kwartaal-QBR. KPI K-07, W-06, R-05; bewijs E-09.
- Continuïteit: geteste BCP/DR met RTO ≤4 uur en RPO ≤1 uur voor kritieke diensten; jaarlijkse test + halfjaarlijkse tabletop. KPI K-08, W-07, R-06; bewijs E-05/E-09.
- Security: 24/7 detectie en respons via SecureOps NL (SOC), MTTD ≤15 min en MTTR ≤120 min voor high alerts. KPI K-09/K-10, W-08, R-07; bewijs E-03/E-09.
- M365 beheer en adoptie support: incidentoplossing binnen SLO’s; baselines (CIS/Microsoft) binnen 90 dagen geïmplementeerd. KPI K-11, W-09, R-08; bewijs E-09.
- Personeel & integriteit: VOG op verzoek binnen 5 werkdagen aangeleverd; 100% medewerkers met security awareness- en privacytraining jaarlijks. KPI K-12, W-10, R-09; bewijs E-06/E-08.
- Duurzaamheid: 92% remote-resolutie, 40% minder autokilometers jaar-op-jaar, 100% EU-datacenters op hernieuwbare stroom, 100% e-facturatie. KPI K-13–K-15, W-11–W-13, R-10; bewijs E-09.

Knock-outs geborgd: ISO 27001 en ISO 9001 aanwezig; 24/7 bereikbaarheidsdienst ingericht. Extra: NEN 7510, Microsoft Solutions Partner – Modern Work, Fortinet NSE4.

2. Begrip van de opdracht Context en scope:

- Opdracht: raamovereenkomst voor beheer, onderhoud en beveiliging van cloud- en infrastructuuroplossingen van Gemeente Voorbeeldstad, inclusief servicedesk, monitoring, patching, endpoint- en netwerkbeheer, back-up en restore, Microsoft 365, en beveiligingsmonitoring (SOC).
- Doelgroep: ambtenaren, ketenpartners en eventuele burgerportalen; prioriteit op continuïteit van publieksdiensten.
- Binnen scope: 24/7 P1-support; ITIL-servicedesk; proactieve monitoring; patch- en vulnerabilitymanagement; M365 beheer; back-up/restore EU; change & release management; rapportages en governance.
- Buiten scope (exclusies reeds afgestemd): levering/beheer van onsite hardware tenzij overeengekomen; third-party applicatiesupport buiten technische laag; projectmatig meerwerk buiten vast maandtarief; end-user adoptietraining op verzoek; zie ook Exclusions.
- Eisen: responstijd P1 ≤30 min (wij ≤15 min); beschikbaarheid ≥99,8% (wij ≥99,9%); EU-dataverwerking; BCP; escalatieprocedure; ITIL; monitoring en patching; VOG indien vereist; M365-

ondersteuning.
- Aannames (conform tender): tijdige toegang en informatie; kantoortoegankelijkheid; tijdige besluitvorming; adequate netwerkverbindingen; rechtmatige licenties.

Value-for-money: hogere SLA's zonder meerprijs (pricing locked), lagere risico's door SOC + gestandaardiseerde ITIL-processen, en duurzame inzet (minder kilometers, EU hernieuwbare energie).

3. Aanpak (Plan-Do-Check-Act) 3.1 Transitie (8 weken, nul-uitval) Doel: risicoloze overgang met volledige zichtbaarheid en borging.

- Week 1–2 (Plan): kick-off; inventarisatie CMDB (100% kritieke assets geregistreerd); contractkaders en DPA; meten nul-situatie SLA's; risico-workshop; communicatie- en escalatieplan afgerond. Deliverables: CMDB v1.0, DAP/DPA, Transitieplan.
- Week 3–5 (Do): implementatie monitoring (agents/sensors), logverzameling (EU), back-upbeleid, patchkalender; ITIL-workflows in service management-tool (incident/problem/change); integratie SOC; test restores; M365-baseline review.
- Week 6 (Check): proefdraaien (shadow support); P1/P2 simulaties; toets op SLA-metingen; security tabletop oefening (BCP).
- Week 7–8 (Act): bevindingen doorvoeren; go-live; live-stand-by van senior engineers gedurende 2 weken post go-live; overdracht naar beheer.

3.2 Beheerfase (operationeel, 24/7)

- Incidentmanagement: P1 24/7; P2–P4 binnen kantoortijden 08:00–18:00, optioneel verlengd. Prioritering op impact/urgentie; major incident procedure met hourly updates.
- Problemmanagement: root cause analyses binnen 5 werkdagen na P1; trendanalyses maandelijks; bekend probleemregister.
- Changemanagement: CAB wekelijks; standaard changes binnen 2 werkdagen; normal changes risico-gebaseerd; emergency change <2 uur doorlooptijd.
- Monitoring: 24/7 NOC/SOC; MTTD ≤15 min; synthetische testen op kritieke diensten; drempelwaarden per KPI.
- Patch- & vulnerabilitymanagement: kritieke patches ≤48 uur; high ≤7 dagen; CVE-scans wekelijks; compliance-rapport maandelijks; maintenance windows in overleg.
- Back-up & restore: dagelijkse back-ups (kritiek 4× per dag); retentie 30/180/365 dagen (operational/legal); restoretest maandelijks (steekproef).
- M365 beheer: baseline-hardening binnen 90 dagen; Conditional Access; MFA 100%; audit-logging 365 dagen; Secure Score ≥75 binnen 6 maanden.

3.3 Security & privacy

- Frameworks: ISO 27001, NEN 7510; beleid voor access, cryptografie, logging, leveranciersmanagement.
- SOC: 24/7 monitoring op endpoint, netwerk, identiteit; playbooks voor ransomware, BEC, data exfiltratie.
- DPIA-ondersteuning op verzoek; dataminimalisatie; EU-only verwerking; DPA annex met subverwerkers.
- Awareness: jaarlijkse training 100% dekking; phishing-simulaties per kwartaal (≥4/jaar).
- VOG: op verzoek, binnen 5 werkdagen; register bijhouden.

3.4 Escalatie en Major Incident

- P1-bridges binnen 10 minuten; Incident Manager toegewezen; statusupdates elk uur; stakeholderberichtgeving conform sjabloon; post-incident review binnen 3 werkdagen; verbeteracties binnen 10 werkdagen door CAB beoordeeld.

3.5 Continuïteit (BCP/DR)

- RTO ≤4 uur, RPO ≤1 uur voor kritieke diensten; failover-scenario's gedocumenteerd; jaarlijkse DR-test + halfjaarlijkse tabletop; verbetercyclus PDCA.

3.6 Rapportage & overleg (Check & Act)

- Maandelijks service review (MSR): SLA/KPI-rapport, incidenten, changes, security, duurzaamheid, verbeterplan (max. 5 acties).
- Kwartaal QBR: trendanalyses, roadmap, risicoherijking, auditresultaten.
- Realtime dashboards: beschikbaarheid, incidentstatus, patchcompliance, SOC-alerts.

3.7 Eenvoudige Gantt transitieplanning

Fase | Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 | Week 8 Inventarisatie & DPA | ████ | ████ | | | | | Monitoring & Back-up implementatie | | | ████ | ████ | ████ | | | ITIL-workflows & SOC-integratie | | | ███ | ███ | ███ | ▉ | | Testen (restore, simulaties) | | | | | ▉ | ███ | | Go-live & Hypercare | | | | | | | ████ | ████

4. Borging van kwaliteit (ISO/ITIL/PDCA)

- ISO 9001: kwaliteitsmanagement, documentcontrole, interne audits (2× per jaar), corrigerende maatregelen, managementreview (jaarlijks).
- ISO 27001/NEN 7510: ISMS met risicoanalyse jaarlijks; leveranciersbeoordelingen; toegangsbeheer; logging; continuïteit.
- ITIL v4: processen ingericht in servicetooling; KPI's aan processen gekoppeld; eigenaarschap per proceshouder.
- PDCA: maandelijkse Check (rapportages) en Act (verbeterplan); kwartaal QBR; lessons learned uit PIR's in backlog; max. 60 dagen doorlooptijd voor major verbeteringen.

5. Duurzaamheid en maatschappelijke waarde Doelstellingen (SMART):

- Energie & datacenters: 100% EU-regio's met hernieuwbare stroom (Azure West/North Europe, M365 EU Data Boundary). KPI K-14: 100% green-region usage; bewijs: leveranciersverklaringen (E-09).
- Mobiliteit: 92% remote-resolutie; autokilometers –40% YoY; elektrische poolauto's voor onsite; bundeling van bezoeken. KPI K-13; bewijs: mobiliteitsoverzicht (E-09).
- Digitale sobriety: retentielimieten, lifecycle policies; optimalisatie back-ups (deduplicatie/compressie) → doel 20% opslagreductie in 12 maanden. KPI K-15; bewijs: back-uprapport (E-09).
- Maatschappelijk: stageplaatsen (2 FTE/jaar), inclusieve werving (neutraal), e-facturatie 100%. KPI K-16; bewijs: HR-rapportage (E-09).

6. Risico's en beheersmaatregelen (samenvatting) Code | Risico | Kans/Impact | Beheersing (SMART) | Koppeling R-01 | Onvoldoende beschikbaarheid | M/H | Redundantie, synthetische checks, runbooks; 99,9%/mnd; service credits. KPI K-01; W-01; bewijs E-02/E-09 R-02 | Langzame P1-respons | L/H | 24/7 warmlijn, MI-procedure ≤10 min, on-call schema; responstijd ≤15 min 99%. K-02/K-03; W-02/W-03; E-03/E-09 R-03 | Patchachterstand | M/M | Kritiek ≤48u, high ≤7d, maandelijkse compliance ≥95%. K-05; W-04; E-02/E-09 R-04 | Data buiten EU | L/H | Contractueel EU-only, geofence, DPA; 100% EU-log/back-up. K-06; W-05; E-07/E-10 R-05 | Procesafwijking | M/M | ITIL-audits 2×/jaar, CAB weekly, CSI-backlog ≤60d. K-07; W-06; E-09 R-06 | Onvoldoende continuïteit | L/H | RTO ≤4u, RPO

≤1u, 1×/jaar DR-test, 2×/jaar tabletop. K-08; W-07; E-05/E-09 R-07 | Security-incident (ransomware) | M/H | SOC 24/7, MTTD ≤15 min, MTTR ≤120 min, EDR op 100% endpoints. K-09/K-10; W-08; E-03/E-09 R-08 | M365 misconfiguratie | M/M | Baselines binnen 90 dagen; Secure Score ≥75/6m; maandelijkse config-drift check. K-11; W-09; E-09 R-09 | Integriteit personeel | L/H | VOG binnen 5 werkdagen; jaarlijkse awareness 100%. K-12; W-10; E-06/E-08 R-10 | CO2-doel niet gehaald | M/M | Remote ≥92%, bundeling bezoeken, EV inzet, rapportage. K-13–K-15; W-11–W-13; E-09

7. Organisatie en governance Rollen en bezetting (24/7 voor P1):

- Service Manager (eindverantwoordelijk KPI's/rapportages): 1 FTE, bereikbaar 08:00–18:00; escalatie 24/7 bij P1.
- Technisch Lead (architectuur/changes): 0,6 FTE.
- Security Officer (ISMS/SOC coördinatie): 0,4 FTE.
- Change Manager/CAB-voorzitter: 0,2 FTE.
- Servicedesk (ITIL): 5 FTE (08:00–18:00), door Digital Ease B.V.
- NOC/SOC: 24/7 via SecureOps NL (contractueel geborgd).
- Onsite field services: via IT Infra Group (SLA 4 uur on-site bij nood in regio's).
- Vervanging/continuïteit: buddy-systeem; kennisartikelen in KMS; inwerkprotocol ≤10 werkdagen.

RASCI-overzicht (verkort) Activiteit | Service Manager | Technisch Lead | Security Officer | NOC/SOC | Field (IT Infra) | Gemeente Incident P1 | A | R | C | R | S | I Problem | A | R | C | C | S | I Change (CAB) | A | R | C | C | S | I Patch mgmt | A | R | C | C | S | I Back-up/DR | A | R | C | C | S | I M365 baseline | A | R | C | C | S | I Rapportages | A | C | C | C | I | I/A Security alerts | C | C | A/R | R | S | I Escalaties | A | C | C | C | S | I

8. Programma van Wensen (W-xx) met kruiskoppelingen W-xx | SMART-beschrijving | KPI | Risico | Bewijs W-01 | Beschikbaarheid kritieke systemen ≥99,90% per maand; service credits bij <99,90%. | K-01 | R-01 | E-02 (monitoring), E-09 (rapport) W-02 | P1-responstijd ≤15 min, 24/7/365, in 99% van de gevallen. | K-02 | R-02 | E-03 (on-call), E-09 W-03 | P1-oplostijd ≤2 uur, 95% gehaald per maand. | K-03 | R-02 | E-09 (SLA-rapport) W-04 | Patchbeleid: kritiek ≤48u, high ≤7d, compliance ≥95%/mnd. | K-05 | R-03 | E-02, E-09 W-05 | 100% EU-only data, back-up en logs; geen offshoring. | K-06 | R-04 | E-07 (DPA), E-10 (DPO-verklaring) W-06 | ITIL v4-processen actief; 2×/jaar procesaudit; CSI acties ≤60d. | K-07 | R-05 | E-09 (auditverslag) W-07 | BCP/DR getest: RTO ≤4u, RPO ≤1u; 1×/jaar DR-test, 2× tabletop. | K-08 | R-06 | E-05 (BCP/DR), E-09 W-08 | SOC 24/7: MTTD ≤15min, MTTR ≤120min voor high; EDR op 100% endpoints. | K-09/K-10 | R-07 | E-03, E-09 W-09 | M365 baseline binnen 90 dagen; Secure Score ≥75 binnen 6 maanden. | K-11 | R-08 | E-09 (configrapport) W-10 | VOG op verzoek binnen 5 werkdagen; 100% jaarlijkse awareness. | K-12 | R-09 | E-06 (VOG-register), E-08 (trainingslog) W-11 | Remote-resolutie ≥92% per kwartaal; visits gebundeld. | K-13 | R-10 | E-09 (mobiliteitslog) W-12 | Autokilometers –40% YoY; EV inzet 100% bij onsite. | K-13 | R-10 | E-09 W-13 | 100% EU datacenters op hernieuwbare stroom. | K-14 | R-10 | E-09 (leveranciersverklaring) W-14 | Back-upopslagreductie 20% binnen 12 maanden via optimalisatie. | K-15 | R-10 | E-09 (back-uprapport) W-15 | Maandelijkse MSR en kwartaal-QBR met actieplan (max. 5 acties). | K-07 | R-05 | E-09 (verslagen) W-16 | Escalatieprocedure gepubliceerd; MI-bridge binnen 10 min; hourly updates. | K-02/K-03 | R-02 | E-09 (PIR's) W-17 | EU-loggingretentie 365 dagen; audit-trails compleet. | K-06 | R-04/R-07 | E-02/E-09 W-18 | CAB wekelijks; standaard changes ≤2 werkdagen; emergency ≤2 uur. | K-07 | R-05 | E-09 (CAB-notulen) W-19 | Maandelijkse vulnerability scan; kritieke findings ≤48u opgelost. | K-05 | R-03/R-07 | E-09 (scanrapport) W-20 | Servicecontinuïteit bij piek: capaciteit opschalen binnen 48 uur. | K-01/K-02 | R-01 | E-09 (capaciteitsplan)

Bewijsdefinities:

- E-02 Monitoring dashboards en uptime logs (NOC)

- E-03 On-call roosters, SOC playbooks en alertlogs
- E-05 BCP/DR-documentatie en testverslagen
- E-06 VOG-register (geanonimiseerde bevestigingen)
- E-07 Verwerkersovereenkomst en subverwerkerslijst
- E-08 Trainingsregister security/privacy
- E-09 Maand-/kwartaalrapporten en auditnotulen
- E-10 DPO-verklaring EU-dataverwerking

9. KPI/SLA-samenvatting KPI | Definitie | Target | Meting | Frequentie | Koppeling K-01 Beschikbaarheid | Uptime kritieke systemen | ≥99,90%/mnd | Synthetische en real-user monitoring | Maandelijks | W-01, R-01 K-02 P1-responstijd | Tijd tot acceptatie | ≤15 min, 99% | Servicedesk/NOC logs | Maandelijks | W-02, R-02 K-03 P1-oplostijd | Tijd tot herstel | ≤2 uur, 95% | Ticketing/PIR | Maandelijks | W-03, R-02 K-04 Monitoring coverage | % kritieke assets gemonitord | 100% | CMDB vs sensors | Maandelijks | W-04, R-03 K-05 Patchcompliance | Kritiek ≤48u; high ≤7d; ≥95% | 95%+ | Patchrapport | Maandelijks | W-04, R-03 K-06 EU-only verwerking | % data/logs/back-ups in EU | 100% | Config-audits | Kwartaal | W-05/W-17, R-04 K-07 ITIL-proceskwaliteit | Audit-score en doorlooptijd changes | 90%+ score; std ≤2d | Procesaudit/CAB | Halfjaar/maand | W-06/W-18, R-05 K-08 Continuïteit | RTO/RPO gehaald in tests | 100% | DR-testverslag | Jaarlijks | W-07, R-06 K-09 MTTD | Time-to-detect high alerts | ≤15 min | SIEM/SOC logs | Maandelijks | W-08, R-07 K-10 MTTR security | Time-to-respond high alerts | ≤120 min | SIEM/SOC logs | Maandelijks | W-08, R-07 K-11 M365 posture | Secure Score | ≥75/6 mnd | M365 rapport | Maandelijks | W-09, R-08 K-12 Integriteit & awareness | VOG en training | 100% dekking | HR/training logs | Jaarlijks | W-10, R-09 K-13 Remote-resolutie & mobiliteit | % remote; km reductie | ≥92%; −40% YoY | Tickets/mobiliteit | Maandelijks/jaar | W-11/W-12, R-10 K-14 Groene regio’s | % workloads in groene EU-regio’s | 100% | Cloud rapport | Kwartaal | W-13, R-10 K-15 Opslagoptimalisatie | Back-upreductie | ≥20%/12 mnd | Back-uprapport | Kwartaal | W-14, R-10 K-16 Maatschappelijk | Stageplaatsen/e-facturatie | 2 FTE/jaar; 100% e-factuur | HR/fin. rapport | Jaarlijks | W-15 (governance uitbreiding)

SLA’s en service credits:

- Bij onderprestatie K-01: creditering 5–10% maandfee van betreffende dienst (bandbreedte per 0,1%-punt onder target), onverminderd overige rechten.
- Voor K-02/K-03 structurele afwijking (>2 maanden per jaar): verbeterplan binnen 10 werkdagen; bij aanhoudende afwijking recht op beëindiging specifieke servicecomponent zonder boete.
- Rapportage: binnen 5 werkdagen na maandafsluiting.

10. Borging Compliance en KO-eisen

- KO: ISO 27001 — geldig certificaat aanwezig (Digital Ease B.V.).
- KO: ISO 9001 — geldig certificaat aanwezig.
- KO: 24/7 bereikbaarheidsdienst — ingericht via NOC/SOC en senior on-call.
- Must-haves: responstijd, beschikbaarheid, monitoring/patching, ITIL-servicedesk, EU-dataverwerking, escalatieprocedure, BCP, VOG, proactieve monitoring, M365 — alle meegenomen in W-01 t/m W-20 en KPI K-01 t/m K-16.

11. Prijs, garantie en randvoorwaarden

- Prijs: conform pricing locked; hogere SLA’s zonder meerprijs.
- Garantie: 12 maanden op projectdeliverables (transitie, documentatie, configuratie) met herstel van tekortkomingen binnen redelijke termijn (max. 10 werkdagen na melding, tenzij P1).
- Verwerkersovereenkomst: standaard DPA met subverwerkerslijst; EU-only; auditrechten.

- Aannames/Exclusies: overgenomen uit tender (zie inleiding), afwijkingen vooraf afstemmen.

12. Conclusie Met deze EMVI bieden wij Gemeente Voorbeeldstad aantoonbare meerwaarde: hogere beschikbaarheid (99,9%), snellere incidentafhandeling (P1 ≤15 min, herstel ≤2 uur), bewezen security (24/7 SOC, MTTD ≤15 min), sterke continuïteit (RTO ≤4u/RPO ≤1u), volledig EU-conform en duurzaam ingericht (92% remote, 100% groene EU-regio's). Alle beloften zijn SMART, ITIL-geborgd en PDCA-gestuurd, met transparante KPI-rapportage, duidelijke escalaties en service credits. Risico's zijn in kaart gebracht en gekoppeld aan KPI's, Wensen en bewijslast, zodat sturing, compliance en audittrail op orde zijn vanaf dag 1.

Bijlagen/Deliverables binnen dit plan:

- Plan van Aanpak (secties 3–4),
- Risicodossier (sectie 6),
- KPI-overzicht (sectie 9),
- Escalatieprocedure (sectie 3.4),
- BCP/DR samenvatting (sectie 3.5),
- Programma van Wensen (sectie 8).

Contact en uitvoering:

- Opdrachtnemer: Digital Ease B.V. (KvK 88392011, NL004589230B12), Innovatieplein 12, 1234 AB Amsterdam.
- Partners: SecureOps NL (SOC 24/7), IT Infra Group (onsite field).
- Service Manager (nadere gegevens bij gunning); NEN/ISO-certificaten beschikbaar op verzoek.

Benodigde input:

- Actuele assetlijst/CMDB en netwerkdiagrammen.
- Overzicht kritieke diensten en onderhoudsvensters.
- Toegang tot bestaande monitoring, ticketing en cloud-tenants (M365/Azure) met juiste rollen.
- Lijst van huidige verwerkers en subverwerkers; DPA-contactpersoon/DPO.
- Security policies, compliance-eisen (BIO/AVG) en bestaande DPIA's.
- Contactlijst key stakeholders en escalaties (incl. leveranciers).
- Overzicht back-upjobs, retenties en herstelprioriteiten.
- Huidige SLA's/rapportages laatste 6–12 maanden.
- Beveiligingsincidenthistorie en lessons learned.
- Locaties voor eventuele onsite support en beveiligde toegangsinstructies.

Conclusie / Meerwaarde

Onze aanpak borgt meetbare prestaties via PDCA, een sluitende KPI/SLA-set en aantoonbare risicoreductie. We koppelen ieder W-xx aan KPI's en beheersmaatregelen, leveren bewijslast per bijlage en rapporteren transparant op frequenties die aansluiten bij de opdrachtgever. Daarmee maximaliseren we BPKV-scores, reduceren faalkosten en versnellen oplevering.

Benodigde input: