

Bijlage F - Programma van Eisen IT-Beheer 2025

versie 1.0

Nr.	Relatie met Bijlage E	Beschrijving
1	4.2. Digitale werkplek	Maximale tijdsduur voor enrollen van een werkstation in de MDM-omgeving: De maximale tijdsduur voor het succesvol enrollen van een werkstation in de Mobile Device Management (MDM) omgeving is niet langer dan 45 minuten. Dit omvat alle noodzakelijke configuraties en beveiligingsinstellingen die benodigd zijn voor een correct werkende integratie van het apparaat binnen de MDM-omgeving. Maximale tijdsduur voor volledige inzetbaarheid van het apparaat na eerste inloggen: Na het eerste inloggen met een persoonlijk gebruikersaccount dient het apparaat volledig operationeel te zijn, inclusief de benodigde applicaties en toegang tot systemen, binnen een maximale tijdsduur van 15 minuten. Gedurende deze tijd moet de gebruiker toegang kunnen krijgen tot alle voor hen benodigde resources en applicaties, zodat zij hun werkzaamheden kunnen aanvangen dan wel voortzetten zonder verdere vertraging. Maximale opstarttijd van het apparaat: Binnen 40 seconden na het indrukken van de aan/uit-knop dient een werkstation volledig te zijn opgestart en dient het inlogscherf te worden weergegeven. Dit omvat het opstarten van het besturingssysteem, het laden van de noodzakelijke systeeminstellingen en het gereedmaken van het apparaat voor gebruik. Gedurende deze tijd mag er geen merkbare vertraging optreden, zodat de gebruiker tijdens dagelijks gebruik snel toegang kan verkrijgen tot inlogscherf en bureaublad zonder onnodige wachttijden.
2	4.5. Informatieveiligheid	Alle data en verwerking van persoonsgegevens dienen binnen de Europese Economische Ruimte (EER) te blijven en zijn encrypted opgeslagen.
3	4.5. Informatieveiligheid	Medewerkers van Opdrachtnemer hebben alleen toegang onder geheimhoudingsverplichting. Een geheimhoudingsverplichting als onderdeel van de arbeidsovereenkomst tussen werknemer en Opdrachtnemer volstaat hiertoe.
4	4.5. Informatieveiligheid	De Opdrachtnemer heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht. De VOG heeft in ieder gevalbetrekking op: risicogebied 01: functiaspecten 11, 12, 13; risicogebied 03: functiaspecten 36, 37; risicogebied 04: functiaspect 41; risicogebied 06: functiaspect 61; risicogebied 07: functiaspect 71.
5	4.5. Informatieveiligheid	Opdrachtnemer zal de toegang en de autorisaties die zijn verleend ten behoeve van de uitvoering van de dienst(en) enkel voor die doeleinden gebruiken en niet voor enig ander doeleinde.
6	4.5. Informatieveiligheid	De verwerking van data en persoonsgegevens behoort op werkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke data en persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
7	4.5. Informatieveiligheid	Opdrachtnemer draagt er zorg voor dat bij de uitvoering van de werkzaamheden niet meer data of persoonsgegevens worden ingezien of anderszins verwerkt dan werkelijk noodzakelijk voor het correct uitvoeren van de opdracht. Medewerkers van Opdrachtnemer zijn alleen geautoriseerd voor de taken en onderdelen die passen bij hun rol.
8	4.5. Informatieveiligheid	De Opdrachtnemer behoort werkers gescheiden en beperkt toegang te verlenen tot data en persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
9	4.5. Informatieveiligheid	Opdrachtnemer dient aan te tonen dat hij passende technische en organisatorische beveiligingsmaatregelen heeft geïmplementeerd om data, persoonsgegevens en andere gevoelige gegevens van (medewerkers, klanten of andere relaties van) Opdrachtgever te kunnen verwerken.
10	4.5. Informatieveiligheid	Opdrachtnemer meldt datalekken/incidenten onverwijld, maar binnen maximaal 24 uur na ontdekken aan Opdrachtgever, dat er een datalek/incident heeft plaatsgevonden waarbij persoonsgegevens van Opdrachtgever betrokken zijn.
11	4.5. Informatieveiligheid	Uit dienst tredende medewerkers van Opdrachtnemer wordt de toegang tot de IT-omgeving uiterlijk op de laatste werkdag ontzegd.
12	4.5. Informatieveiligheid	Opdrachtnemer zal geen handelingen verrichten die de vertrouwelijkheid, integriteit en/of beschikbaarheid van de systemen van Opdrachtgever(s) en/of de daarop verwerkte gegevens in gevaar kan brengen.
13	4.5. Informatieveiligheid	Opdrachtgever krijgt vaste contactpersonen bij Opdrachtnemer voor technische- en informatiebeveiligingsvraagstukken (respectievelijk CISO en ISO) en voor privacyvraagstukken (Functionaris Gegevensbescherming (FG) en Privacy Officer (PO)). De contactgegevens worden opgenomen in het document SLA.
14	4.5. Informatieveiligheid	Opdrachtnemer betracht alle noodzakelijke zorg om te vermijden dat (nader) forensisch onderzoek niet goed meer kan worden uitgevoerd of de resultaten daarvan niet goed (meer) zouden kunnen worden vertrouwd voor een periode van minimaal een jaar.

15	4.5. Informatieveiligheid	In geval van forensisch (digitaal) onderzoek, zorgt Opdrachtnemer voor het aantoonbaar maken van de bevindingen, voor een periode van minimaal een jaar, om als bewijsmateriaal te kunnen dienen in strafrechtelijke of civielrechtelijke rechtszaken en op een voor dat doeleinde deugdelijke en betrouwbare wijze bijhouden wie op ieder moment toegang had tot of beschikking had over het bewijsmateriaal ('chain of custody').
16	4.5. Informatieveiligheid	De Opdrachtnemer heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.
17	4.5. Informatieveiligheid	De Opdrachtnemer heeft een privacyverklaring waarin is beschreven op welke wijze persoonsgegevens worden verwerkt en hoe een betrokkene, zijn of haar rechten kan uitoefenen.
18	4.5. Informatieveiligheid	De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de Opdrachtnemer vastgelegd en vastgesteld, inclusief die bij uitwisseling van persoonsgegevens tussen Opdrachtnemer en Opdrachtgever, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.
19	4.5. Informatieveiligheid	De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.
20	4.5. Informatieveiligheid	De Opdrachtnemer waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
21	4.5. Informatieveiligheid	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
22	4.5. Informatieveiligheid	Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacy-risico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.
23	4.5. Informatieveiligheid	De Opdrachtnemer past anonimiseren of pseudonimisering toe waar dit de dienstverlening niet belemmert.
24	4.7. De dienstverlening	Het beheerteam van Opdrachtnemer is op werkdagen van 08:00 tot 18:00 uur (kantoortijden) en gedurende gepland onderhoud buiten kantoortijden beschikbaar voor het beheerteam van Opdrachtgever.
25	4.7. De dienstverlening	Indien Opdrachtgever telefonisch contact zoekt, dient de telefoon te worden opgenomen door een medewerker van het beheerteam van Opdrachtnemer. Toegang tot een medewerker via een geautomatiseerd systeem, keuzemenu of andere tussenstappen is niet toegestaan.
26	4.7. De dienstverlening	Opdrachtnemer zorgt dat continuïteit en beschikbaarheid van de IT-omgeving voor de gebruikers is gewaarborgd. Voor zover voor die continuïteit en beschikbaarheid vereist, dient gepland onderhoud te gebeuren buiten kantoortijden. Deze onderhoudsmomenten dienen in overleg met de Opdrachtgever te worden vastgesteld. De vaststelling dient minimaal 14 dagen voor het onderhoud plaats te vinden.
27	4.7. De dienstverlening	Opdrachtgever begrijpt dat oplossingen niet altijd direct beschikbaar zijn, afhankelijk van de complexiteit van het probleem. Dat laat onverlet dat Opdrachtnemer dient te zorgen dat er direct contact is tussen Opdrachtgever en de persoon die het probleem daadwerkelijk oplost en over de juiste expertise beschikt, om onnodige wisselingen van contactpersonen te voorkomen en direct inhoudelijk het probleem te kunnen bespreken.
28	4.7. De dienstverlening	De behoefte aan direct contact met specialisten en korte communicatielijnen is groot, voor alle aspecten binnen de dienstverlening. De Opdrachtnemer dient hierin een goede balans te bieden tussen fysieke samenwerking op locatie en digitale afstemming, met actieve deelname aan reguliere overleggen. Dit alles moet gebeuren binnen een structuur van korte lijnen, met vertrouwde gezichten die beschikken over relevante kennis van de IT-omgeving, trends en ontwikkelingen.
29	4.7. De dienstverlening	Opdrachtnemer zorgt dat minimaal een dag per week of zoveel meer als Opdrachtgever noodzakelijk acht, een engineer van Opdrachtnemer (met kennis van de IT omgeving van Opdrachtgever bij Opdrachtgever op locatie is. De weekdag wordt in goed onderling overleg vastgesteld. Daarnaast sluit Opdrachtnemer aan bij alle reguliere overleggen van Opdrachtgever in het kader van de dienstverlening. Het is toegestaan voor Opdrachtnemer om bij reguliere overleggen digitaal aanwezig te zijn.
30	4.7. De dienstverlening	Opdrachtnemer zet ter zake kundig Personeel in en zorgt dat alle in te zetten Personeel ingewerkt is in en kennis heeft van de IT-omgeving van Opdrachtgever.
31	4.7. De dienstverlening	Opdrachtnemer draagt zorg voor de uitvoering van het capacity management. Opdrachtnemer dient hiervoor resources te managen: A) Monitoren en bewaken van de IT-omgeving. B) Analyseren van de meetgegevens om proactief uitspraken te kunnen doen over het toekomstige gebruik van resources. C) Implementeren van aangepaste of nieuwe capaciteit, conform Beleid Change Management.

32	4.7. De dienstverlening	Opdrachtnemer maakt dagelijks back-ups van de IT-omgeving conform het back-up beleid van Opdrachtgever in Bijlage H - Beleid Backup en herstel. Opdrachtnemer toont aan door middel van testen en rapportage dat backups succesvol zijn gemaakt en herstelbaar zijn. Bij een niet succesvolle back-up dient Opdrachtnemer deze alsnog een nieuwe succesvolle back-up gemaakt te worden. De herstelbaarheid van back-ups dient minimaal eenmaal per kwartaal getest te worden dat back-ups werken naar behoren.
33	4.7. De dienstverlening	Opdrachtnemer is verantwoordelijk voor het transparant en effectief beheren van alle kosten die verband houden met IT-omgeving, waaronder Azure Cost Management en committeert zich aan proactieve kostenoptimalisatie gedurende de contractduur.
34	4.7. De dienstverlening	Opdrachtnemer is verantwoordelijk voor het realiseren van een minimale beschikbaarheid van de IT-omgeving van 99,5% tijdens reguliere kantoor tijden (maandag t/m vrijdag van 08:00 tot 18:00 uur, exclusief nationale feestdagen). Beschikbaarheid wordt gemeten over de meest recente twaalf maanden en omvat de ongeplande downtime. De KPI wordt per kwartaal berekend, waarbij de kantoor tijd omgezet wordt naar aantal minuten. Kantoor tijd zijn alle reguliere werkdagen met een werkvenster van 08:00 tot 18:00, concreet 10 uur ofwel 600 minuten. De storingstijd is het aantal minuten dat een dienst binnen de IT-omgeving niet beschikbaar is in een kwartaal. Tijdens de operationele fase wordt de gerealiseerde KPI uitgedrukt in een percentage en als volgt berekend. (a) Onbeschikbaarheid van die delen van de omgeving die buiten verantwoordelijkheid van Opdrachtnemer vallen worden niet in de berekening van de beschikbaarheid meegenomen. (b) Buiten kantoor tijden heeft Opdrachtnemer een zwaarwegende inspanningsverplichting met betrekking tot beschikbaarheid. (c) In het kader van het hostingplatform kunnen in de toekomst er per subscriptie voor een derde partij andere (hogere) servicelevels gelden. In dat geval zullen partijen in overleg bepalen wat de impact daarvan is op de dienstverlening en kosten. Gerealiseerde KPI = $(1 - \text{storingstijd in minuten} / \text{kantoor tijd in minuten}) * 100\%$ Rekenvoorbeeld In het derde kwartaal bestond het kwartaal uit 12 werkweken van vijf werkdagen. De totale kantoor tijd is in deze situatie $12 * 5 * 600 \text{ minuten} = 36.000 \text{ minuten}$. De storingstijd in dezelfde periode bedroeg drie uur, 180 minuten. De gerealiseerde KPI wordt als volgt berekend: KPI 2 derde kwartaal: $(1 - 180 / 36000) * 100 = 99,5\%$
35	4.7. De dienstverlening	Na ontvangst van een schriftelijk of mondeling verzoek van Opdrachtgever om specialistisch advies, zorgt Opdrachtnemer dat een specialist binnen één werkdag beschikbaar is voor overleg. Dit overleg kan plaatsvinden via een digitale sessie of fysiek op locatie, afhankelijk van wat Opdrachtgever verzoekt. De KPI wordt berekend per kwartaal en kent een minimale prestatienorm van 99%. Dit betekent dat in minimaal 99% van de gevallen een specialist van Opdrachtnemer binnen één werkdag beschikbaar moet zijn na een ontvangen verzoek. Tijdens de operationele fase wordt de gerealiseerde KPI uitgedrukt in een percentage en als volgt berekend. Gerealiseerde KPI = $(1 - \text{aantal verzoeken niet binnen één werkdag behandeld} / \text{totaal aantal verzoeken}) * 100\%$ (a) Opdrachtnemer houdt een logboek bij waarin tijdstempels van het verzoek en de start van het overleg worden geregistreerd. Deze worden periodiek gedeeld met Opdrachtgever ter verificatie. (b) De KPI is van toepassing op verzoeken die gedaan zijn binnen de reguliere kantoor tijden.
36	4.9 Governance	Voor alle genoemde KPI's geldt het volgende: (a) Opdrachtnemer rapporteert per 2 maanden aan Opdrachtgever de gerealiseerde KPI's en de beheersmaatregelen die getroffen zijn ter borging van de KPI-normen. Bij het niet behalen van de KPI-norm stelt Opdrachtnemer een analyse op van de oorzaken en stelt verbetermaatregelen voor. Deze dienen binnen een maand na afloop van het laatste 2 maanden waar de KPI betrekking had op en implementeert deze na na goedkeuring door Opdrachtgever. Het verbeterplan dient in het opvolgende 2 maanden te leiden tot een gerealiseerd KPI volgens de norm. (b) Indien de prestatienorm twee keer achtereenvolgens niet wordt gehaald, volgt een escalatiegesprek. Bij structurele afwijkingen kan Opdrachtgever betalingen voor het deel van de dienstverlening waarop de afwijking betrekking heeft opschorten. Wanneer de Opdrachtnemer later alsnog aan de prestatienorm voldoet, wordt de opgeschorte betaling alsnog uitgevoerd.
37	4.9 Governance	Alle communicatie, overleggen, documentatie en rapportages zullen in het Nederlands (taalniveau C1) gevoerd en aangeleverd worden. Dit geldt ook voor het uitvoeren van de dienstverlening. Specialistische communicatie met software- en hardware leveranciers in het Engels (taalniveau C1) is toegestaan.

38	4.9 Governance	In aanvulling op artikel 8.1 van de AWBIT-2023 worden alle in het kader van de Overeenkomst gemaakte of opgeleverde Documentatie, scripts en rapportages eigendom van Opdrachtgever. Alle Documentatie, scripts en rapportages in het kader van de dienstverlening door Opdrachtnemer worden opgesteld in de huisstijl van Opdrachtgever. Opdrachtnemer is verantwoordelijk voor het opstellen van Documentatie van de IT-omgevingen borgt dat deze altijd up-to-date en beschikbaar is voor Opdrachtgever. De Documentatie dient van zodanig niveau te zijn dat het overdragen van bepaalde activiteiten en/of onderdelen, bijvoorbeeld naar derden, eenvoudig kan plaatsvinden.
39	4.9 Governance	Opdrachtnemer rapporteert maandelijks over in ieder geval de volgende onderwerpen: (A) alle KPI's (tenzij anders overeengekomen) en eventueel zelf gehanteerde kengetallen. (B) Incidenten. De invulling van deze rapportage wordt in overleg met Opdrachtgever samengesteld, maar in elk geval: doorlooptijd van incidenten, first-time-right fixes). (C) Kostenrapportages over Azure-omgeving. De verdere invulling van de rapportages en de onderwerpen die opgenomen moeten worden, worden na gunning tijdens de transitiefase in overleg vastgesteld.
40	4.9 Governance	In aanvulling op artikel 8.1 van de AWBIT-2023 zijn alle data in het kader van de uitvoering van de Overeenkomst eigendom van Opdrachtgever. Alle data dienen uitsluitend binnen de omgeving van de Opdrachtgever opgeslagen te worden. Opdrachtnemer is niet toegestaan om data lokaal of in de eigen omgeving op te slaan.