1e Nota van Inlichtingen
Europese aanbesteding Kantoorautomatisering

Datum: 26 februari 2026
Kenmerk: NIPV2026-EA-04009

In deze Nota van Inlichtingen geeft de Aanbestedende Dienst antwoord op de gestelde vragen en wijzigingsvoorstellen die in het kader van de Aanbesteding Kantoorautomatisering zijn geplaatst. De Nota van Inlichtingen maakt integraal onderdeel uit van het Beschrijvend Document d.d. 6 februari 2026.

Vraag nr.	Document	Vraag	Antwoord
1.	Selectiedocument Kantoorautomatisering, paragraaf 3.10, pagina 22	Gezien de omvang en complexiteit van de gevraagde scope lijkt het genoemde budget beperkt in verhouding tot marktconforme uitvoering. Kunt u toelichten welke uitgangspunten en aannames aan het budget ten grondslag liggen?	Het budget is voortgekomen uit de marktverkenning en marktconsultatie.
2.		Bij het invullen van de Excel sheet programma van eisen krijgen wij foutmeldingen. Het is voor ons niet mogelijk om hem in te vullen. Is dit een juiste bevinding of doen wij iets verkeerd?	De aanbestedende dienst verwacht in deze fase van de aanbesteding geen reactie op het programma van eisen; dit Excel hoeft niet te worden ingevuld. U kunt uw vragen stellen voor de nota van inlichtingen via bijlage 2 'Standaardformulier vragen'.

3.		In paragraaf 3.13 worden een aantal normen opgesomd waar NIPV rekening mee houdt. In hoeverre dient Opdrachtnemer te beschikken over deze certificaten?	Waar een specifieke certificering als eis is gesteld, is dit expliciet opgenomen in het PvE – Security & Compliance (KO-eisen) of in de geschiktheidseisen in het Selectiedocument. Ter verduidelijking: het 'aantoonbaar handelen in lijn met' zoals genoemd in het antwoord, wordt gedurende de looptijd getoetst via onder meer de volgende verplichte onderdelen uit het PvE: • De jaarlijkse assurance-verklaring over cloudbeveiliging (ALG-028). • De maandelijkse security-rapportage inclusief root-cause analyses (SRV-008). • Het recht van NIPV op een jaarlijkse audit op de gehele dienstverlening (SEC-024). • Het naleven van logging- en monitoringprotocollen conform SEC-023 t/m SEC-028. In overige gevallen volstaat het dat Opdrachtnemer aantoonbaar handelt in lijn met deze normen, bijvoorbeeld door middel van beleid, processen, maatregelen, audits en assurance-rapportages zoals gevraagd in het PvE (bijv. jaarlijkse assurance-verklaring, logging, audits).
4.	Selectiedocument, 3.4.1., Blz. 15 –4	In paragraaf 3.4.1 (onderdeel 4 'Serverbeheer') wordt de verantwoordelijkheid beschreven voor het beheer, de monitoring en de uiteindelijke uitfasering van de resterende on-premises servers. Om de logistieke impact van de benodigde on-site werkzaamheden (zoals fysiek onderhoud en vervanging conform paragraaf 3.4.1 onderdeel 5) en de risico's tijdens de transitie naar de 'n-state' correct te kunnen mitigeren, vragen wij u te verduidelijken of deze serverinfrastructuur fysiek is ondergebracht op de NIPV-locaties in Arnhem en/of Zoetermeer, of dat deze in een extern datacenter is gehuisvest.	De resterende on-premises servers bevinden zich op de NIPV-locatie Arnhem. Alle bedrijfskritische applicaties die voorheen op deze omgeving draaiden, zijn inmiddels uitgefaseerd. Er zijn op dit moment nog vier applicaties die worden gemigreerd naar Azure of andere cloudoplossingen. De verwachting is dat dit migratieproces rond de zomer van 2026 grotendeels zal zijn afgerond en daarmee vóór de start van de dienstverlening onder deze aanbesteding. Zodra de laatste vier applicaties zijn overgezet, waarvoor momenten acties zijn uitgezet, blijft uitsluitend een beperkte set infrastructuurcomponenten over, die vervolgens kan worden uitgezet.

			De impact voor en inspanning van de nieuwe dienstverlener op het gebied van serverbeheer is daardoor zeer beperkt. De werkzaamheden bestaan voornamelijk uit: • Technische en functionele ondersteuning bij eventuele resterende vraagstukken • Uitvoeren van de laatste uitfaseringstaken van de overgebleven infrastructuurcomponenten. Hiermee past de scope volledig binnen de in het Selectiedocument beschreven gefaseerde uitfasering van de on-premises omgeving richting een cloud IT landschap.
5.	Selectiedocument, paragraaf 3.10	In paragraaf 3.10 wordt de totale maximale waarde van de overeenkomst voor de gehele duur (inclusief optiejaren) vastgesteld op € 7.000.000,-. Dit bedrag wijkt af van de jaarlijkse raming voor de basisdienstverlening en projecturen (maximaal € 350.000,- per jaar), wat over 10 jaar een cumulatief bedrag van € 3.500.000,- zou betekenen. Kunt u bevestigen dat het resterende deel van de maximale contractwaarde (€ 3.500.000,-) gereserveerd is voor de in paragraaf 3.6 beschreven herzieningsclausules (inkoop Azure-consumptie, WAN-beheer en Teams-telefonie) en eventuele substantiële groei in het gebruikersaantal? Dit inzicht is cruciaal voor een realistische raming van de benodigde schaalbaarheid in onze oplossing.	Gegadigde dient uit te gaan van een geraamde totaalwaarde van €350.000,- per jaar. Wanneer een raamovereenkomst wordt gesloten, dient er een maximale waarde gekoppeld te worden aan de Raamovereenkomst. In dat geval wordt de maximale waarde ruim ingezet op €7.000.000,- (€350.000,- per jaar x 10 jaren x 50%). De 50% is een verhoging voor het geval de inkoopbehoefte van de Aanbestedende dienst hoger mocht zijn dan verwacht. Die 50% hoeft niet evenredig over de afzonderlijke jaren van de looptijd te worden ingezet. De omvang van de onderdelen zoals opgenomen in de herzieningsclausule (paragraaf 3.6 van het selectiedocument) zijn hier geen onderdeel van en vallen boven deze genoemde waarde.
[redacted] 6.	Selectiedocument, paragraaf 3.5	Het document stelt dat bepaalde onderdelen buiten scope vallen, zoals netwerkbeheer en SOC-diensten. Tegelijkertijd worden MSP's wel verantwoordelijk gehouden voor incidenten, beveiligingsmaatregelen en samenwerking met deze externe partijen. Dit kan leiden tot operationele risico's voor een MSP, omdat het moeilijk is verantwoordelijk te zijn zonder controle. Is het mogelijk om	Het is niet mogelijk om de onderdelen die momenteel buiten scope vallen alsnog binnen de scope van deze aanbesteding te brengen. De reden hiervoor is dat voor deze diensten reeds lopende contracten bestaan met andere gespecialiseerde dienstverleners, zoals beschreven in het Selectiedocument. Hierdoor kunnen deze onderdelen op dit moment geen onderdeel zijn van de scope.

		deze onderdelen wel onderdeel van de scope te maken? Zo niet, waarom niet?	De aanbesteding bevat echter een herzieningsclausule, waarmee het NIPV de mogelijkheid heeft om bepaalde diensten op een later moment, alsnog onder het contract met de te selecteren dienstverlener te brengen. Dit geldt onder meer voor bijvoorbeeld connectiviteit en SOC-diensten, zoals toegelicht het selectiedocument. Het NIPV kiest bewust voor een SPOC-constructie. Dit betekent dat de nieuwe dienstverlener zich constructief en proactief dient op te stellen in de samenwerking met de reeds gecontracteerde netwerk- en SOC-leveranciers. Hierbij wordt verwacht dat de opdrachtnemer tekortkomingen niet afschuift, maar de samenwerking in de keten stimuleert en bewaakt binnen de eigen verantwoordelijkheid en scope. De netwerk infrastructuur op de NIPV-locaties draait stabiel en is bovendien recent vervangen, waardoor de benodigde inzet vanuit de nieuwe dienstverlener voor on-site netwerkondersteuning naar verwachting beperkt is. De rol van de nieuwe dienstverlener bestaat met name uit proactieve ondersteuning en het oppakken van concrete verzoeken of incidenten op locatie, binnen de kaders van de externe netwerkdienstverlener. Ten aanzien van SOC-diensten kiest NIPV er in deze fase nadrukkelijk voor om deze extern te beleggen. Dit voorkomt een situatie waarin “de slager zijn eigen vlees keurt” en waarborgt objectieve monitoring en analyse van beveiligingsincidenten. Wanneer zich echter security-incidenten voordoen binnen de onderdelen van de IT-omgeving die onder beheer van de nieuwe dienstverlener vallen, heeft deze wél een belangrijke operationele rol en verantwoordelijkheid in de afhandeling en coördinatie van de oplossing, in nauwe samenwerking met de SOC-partner.

7.	Selectiedocument, paragraaf 8.2	Ervaring leert dat het beantwoorden van vragen op maximaal 2 pagina's ervoor zorgt dat belangrijke details missen omdat ze moeten worden weggelaten. Er dient te veel gesneden te worden in de kwaliteit van de beantwoording. Bent u bereid de beantwoording van uw selectiecriteria met 2 pagina's te verhogen?	Nee, het aantal pagina's wordt niet aangepast.
8.	Bijlage 10 Programma van Eisen	Er worden hoge eisen gesteld aan responsetijden en SLA's zonder dat er duidelijk verband wordt gelegd met afhankelijkheden. De MSP is in de huidige opzet afhankelijk van de externe partijen zoals SOC- en netwerkdienstverlener. Kunt u aangeven wat de verwachtingen zijn als er externe partijen zijn betrokken?	De in Bijlage 10 Programma van Eisen beschreven SLA's, responstijden en beschikbaarheidseisen zijn van toepassing op de diensten binnen de scope van Opdrachtnemer (werkplek, M365, Azure, back-up, service- en changemanagement). Waar de afhandeling van incidenten mede afhankelijk is van: • De netwerk dienstverlener • De SOC dienstverlener • Cloud dienstverleners (zoals Microsoft) • Andere betrokken dienstverleners • Geldt dat: Opdrachtnemer als SPOC optreedt richting eindgebruikers van het NIPV • Opdrachtnemer verantwoordelijk is voor tijdige coördinatie en escalatie in de keten • In de uiteindelijk haalbare doorlooptijden rekening wordt gehouden met de onderliggende contractuele afspraken met deze derden De exacte afspraken en escalatiepaden tussen de MSP, de netwerkpartner en de SOC dienstverlener worden na gunning definitief vastgelegd in het Dossier Afspraken en Procedures (DAP). In de gunnings- en contractfase worden de SLA's nader geconcretiseerd en, waar nodig, afgestemd op de ketenafhankelijkheden, zonder dat dit de kern van het PvE wijzigt.

9.	Bijlage 10 Programma van Eisen	Het PvE stelt dat er geen downtime mag zijn tijdens gepland onderhoud. Dit is een hoge eis, waarbij wij inderdaad dit altijd minimaliseren, maar de strekking geen downtime is feitelijk onuitvoerbaar op bepaalde componenten. Bent u bereid de beschikbaarheid in een percentage uit te drukken van bijvoorbeeld 99,8%?	Het PvE stelt hoge eisen aan continuïteit en minimalisatie van downtime. Dit sluit aan bij de doelstelling van het NIPV om een stabiele en moderne cloud-first werkomgeving te bieden. De formulering “geen downtime tijdens gepland onderhoud” moet worden gelezen als: gericht op het voorkomen van merkbare verstoring voor gebruikers, door bijvoorbeeld: • Onderhoud buiten kantoortijd, • Gefaseerde uitrol, • Redundantie. Het NIPV zal de beschikbaarheidseisen in de contractfase concretiseren in percentages per dienst (bijvoorbeeld 99,8% of hoger, afhankelijk van het type dienst) en in lijn brengen met het totale risicoprofiel en de ketenafhankelijkheid. Een generieke aanpassing van de tekst in het PvE wordt in deze Nota van Inlichtingen niet doorgevoerd; de strekking "zeer hoge beschikbaarheid" blijft van kracht. Downtime veroorzaakt door externe factoren buiten de macht van de MSP (zoals een wereldwijde Azure-storing) valt buiten de SLA-meting.
10.	Bijlage 10 Programma van Eisen	In het selectiedocument wordt benoemd dat het netwerk en daarbij behorende beheer buiten scope zijn en reeds in beheer bij een derde partij. In het PVE wordt er op meerdere punten toch iets verwacht vanuit de opdrachtnemer. Kunt u aangeven wat wel en wat niet binnen scope is?	Daar waar het PvE verwijst naar netwerkactiviteiten door Opdrachtnemer (bijv. WPL-010, WPL-011), betreft het concreet uit te voeren taken op locatie binnen de door NIPV en de netwerkdienstverlener gestelde kaders, niet het overnemen van de volledige netwerkdienstverlening of verantwoordelijkheid.
11.	Selectiedocument paragraaf 3.8	In paragraaf 3.8 van het Selectiedocument geeft u aan dat Opdrachtgever de mogelijkheid de Overeenkomst maximaal tien jaar te laten doorlopen onder ongewijzigde voorwaarden. Voor de Opdrachtnemer kan dit bezwaarlijk zijn, omdat technologische ontwikkelingen, markt- en	Het NIPV heeft begrip voor de standpunten hieromtrent. Het NIPV heeft voor een langere looptijd gekozen om Opdrachtnemer in staat te stellen investeringen terug te verdienen. Die terugverdientijd zit ook verdisconteerd in de verlengingen.

		prijsontwikkelingen en overige ontwikkelingen over een termijn van tien jaar niet te overzien zijn. Een verplichting om een verlenging altijd onder gelijke voorwaarden te accepteren kan daardoor tot disproportionele risico's leiden. Wij verzoeken daarom om opname van de volgende aanvullende bepaling: "Indien Opdrachtnemer van mening is dat een (verdere) verlenging onder ongewijzigde voorwaarden voor hem ernstige nadelige gevolgen heeft, kan hij dit - voor het eerst na verloop van 7 jaren - tot uiterlijk twaalf (12) maanden vóór afloop van de (verlengde) contractperiode schriftelijk en gemotiveerd kenbaar maken, in welk geval geen (verdere) verlenging zal plaatsvinden."	Daarnaast heeft Opdrachtgever belang bij een stabiele dienstverlening. Opdrachtgever gaat om die reden niet akkoord met het voorstel. De Opdrachtgever geeft de mening van Opdrachtnemer bij de verlenging wel een uitdrukkelijke plaats. Daartoe zal het volgende worden opgenomen de Overeenkomst: "*Na het verloop van zeven (7) jaren, zal de Opdrachtnemer de gelegenheid hebben om diens mening over het gebruik van de opvolgende verlengingen te geven. Opdrachtgever bericht de Opdrachtnemer uiterlijk 12 maanden voor het verloop van de verlengde duur of de Opdrachtgever voornemens is om de looptijd te verlengen. De Opdrachtnemer heeft gelegenheid om naar aanleiding van dat bericht kenbaar te maken of hij het daarmee eens is of niet. Als Opdrachtnemer meent dat verlenging onder toepassing van de Overeenkomst voor haar niet wenselijk is, dan kan de Opdrachtnemer haar mening binnen een (1) week na ontvangst van het voornemen van Opdrachtgever schriftelijk, onderbouwd kenbaar maken aan de Opdrachtgever. De Opdrachtgever zal de mening van de Opdrachtnemer meenemen bij haar definitieve beslissing over de verlenging.*"
12.	Selectiedocument paragraaf 8.2	In Selectiecriterium S2 vraagt Opdrachtgever bij de eerste bullit over een samengevoegd overzicht van de behaalde SLA prestaties over een periode van 12 maanden. Dit betekent een zeer grote inspanning voor Inschrijver om alle SLA's voor de verschillende diensten te beschouwen. Het halen van de SLA zegt nog niets over de tevredenheid van de opdrachtgevers. Wij achten de tevredenheid van de opdrachtgevers en gebruikers een betere indicatie. Kan Inschrijver tevredenheidscijfers overleggen om de eerste bullit te beantwoorden? Of kan Opdrachtgever de eerste bullit aanpassen?	Het NIPV kan niet geheel akkoord gaan met het voorstel. Het meten van klanttevredenheid is inherent willekeurig en ondoorzichtig. Het kan simpelweg niet objectief worden gemeten. Dat is bij het halen van SLA afspraken anders. Een verplichting binnen een SLA is immers behaald of niet. Het criterium wordt daarom gehandhaafd, net als de informatie die moet worden aangeleverd. Het NIPV is evenwel bereid om het aantal bewijsmiddelen te beperken, om de inschrijflast te beperken. Gegadigde kan volstaan met het aanleveren van ten minste 5 representatieve SLA's van het afgelopen jaar, mits die

			SLA's betrekking hebben op opdrachtgevers met 300 – 800 gebruikers (dezelfde bandbreedte als bij geschiktheidseis 5).
13.	Selectiedocument paragraaf 3.3	Welke risico's beschouwt NIPV zelf als de grootste aandachtspunten bij deze aanbesteding en de daaropvolgende transitie?	Het NIPV ziet de volgende vier belangrijkste risico's voor deze aanbesteding en de daaropvolgende transitie: • Verlies van kwaliteit, beschikbaarheid en bereikbaarheid van de IT-dienstverlening wanneer de opdrachtnemer de SPOC-rol niet effectief en proactief invult. • Een dienstverlener die onvoldoende proactief handelt, waardoor verbeteringen, optimalisaties en tijdige signalering uitblijven. • Een niet-optimale samenwerking tussen het NIPV-regieteam en de dienstverlener, wat kan leiden tot vertragingen, misverstanden en onduidelijkheid over verantwoordelijkheden. • Onvoldoende begrip van de NIPV-context door medewerkers van de dienstverlener, waardoor keuzes en adviezen niet aansluiten bij de behoeften van de organisatie.
14.	Selectiedocument paragraaf 3.11	Zijn er specifieke privacy- of datagevoeligheden binnen NIPV (bijv. crisisdata, oefendata) die extra aandacht vragen bovenop de generieke AVG-eisen?	Het NIPV verwerkt data die gerelateerd is aan brandweerzorg en crisisbeheersing, wat een verhoogd integriteits- en vertrouwelijkheidsrisico met zich mee kan brengen. Specifieke eisen rondom dataclassificatie, labels en retentiebeleid voor deze datastromen worden in de gunningsfase nader gespecificeerd conform de Baseline Informatiebeveiliging Overheid (BIO2.0). Veel van deze data wordt opgeslagen en beheerd in systemen en platformen die buiten de scope van deze aanbesteding vallen. Daarnaast bevatten de werkplekken en Microsoft-omgevingen binnen deze aanbesteding wel diverse typen gevoelige gegevens, zoals onder meer: • opleidings- en oefendata, • gegevens rondom crisisbeheersing en incidenten,

			• persoonsgegevens van medewerkers, docenten, studenten en ketenpartners, • operationele informatie die verband houdt met de uitvoering van NIPV-taken. Hoewel de meest kritieke data elders is ondergebracht, blijft de informatie die via werkplekken, Microsoft 365 en Azure wordt verwerkt privacy- en veiligheidsgevoelig. Daarom is het essentieel dat deze omgeving hoogwaardig wordt beveiligd, conform de eisen voor security, compliance en governance zoals opgenomen in de aanbestedingsstukken.
15.	Selectiedocument, pg 15 (On site netwerkbeheer)	Kan u toelichten waarom de huidige netwerkleverancier deze werkzaamheden niet zelf uitvoert?	De huidige netwerkleverancier levert uitsluitend remote beheer en monitoring (NOC/SOC) en beschikt niet over een on-site serviceapparaat voor fysieke interventies op de NIPV-locaties. NIPV heeft hier niet zelf de kennis/capaciteit voor in huis. Om de continuïteit bij hardware-incidenten of fysieke wijzigingen op locatie te borgen, is deze on-site ondersteuning noodzakelijkerwijs opgenomen in de scope van de kantoorautomatiseringsopdracht.
16.	Selectiedocument, pg 15 (On site netwerkbeheer)	Bent u bereid deze activiteiten bij uw huidige netwerkleverancier neer te leggen en deze te schrappen uit de scope van deze uitvraag?	Nee, de Aanbestedende Dienst handhaaft de huidige scope. Zoals toegelicht in het antwoord op vraag 15, maken fysieke on-site werkzaamheden geen deel uit van de dienstverlening van de remote netwerkbeheerder en heeft het NIPV hier niet zelf de kennis/capaciteit voor in huis. De impact en frequentie van deze taken zijn naar verwachting, op basis van de ervaringen tot nu toe, zeer beperkt. De Opdrachtnemer heeft de vrijheid om deze on-site activiteiten zelf uit te voeren of hiervoor een gespecialiseerde partner of onderaannemer in te zetten.
17.	Selectiedocument, pg 15 (On site netwerkbeheer)	Hoe is deze on site dienstverlening momenteel ingevuld en door wie wordt dit uitgevoerd; wat loopt hierbij goed en wat loopt niet goed?	Momenteel wordt dit ingevuld door een netwerkpartner die partner is van de netwerkleverancier. Dit loopt goed maar de wens is om

			dit bij de MSP onder te brengen. Zie ook de antwoorden bij vraag 15 & 16.
18.	Selectiedocument, pg 15 (On site netwerkbeheer)	Wie stuurt de genoemde activiteiten aan (ondersteuning bij netwerkproblemen, connectiviteitsissues en projecten). NIPV of de derde partij waarbij het netwerkbeheer is ondergebracht?	De regieorganisatie van NIPV coördineert de samenwerking tussen de verschillende ketenpartners en voert de regie op escalaties. De feitelijke uitvoering van on-site werkzaamheden door de IT-partner vindt plaats in nauwe afstemming met zowel NIPV-regie als de remote netwerkbeheerder.
19.	Selectiedocument, pg 15 (On site netwerkbeheer)	Wat is de verwachting hoe vaak er een beroep gedaan wordt op de Opdrachtnemer? En op welke momenten (overdag, avond, weekend)?	Eind 2025 en begin 2026 is het grootste deel van de netwerk-infrastructuur van NIPV vernieuwd, waaronder alle access points, een aantal switches en de firewalls. Deze moderne infrastructuur wordt volledig remote beheerd en bewaakt door de netwerkleverancier. De dekking, capaciteit en stabiliteit van het netwerk zijn daarmee zodanig op orde dat de verwachting is dat de benodigde on-site inzet de komende jaren nihil zal zijn. Alleen in het uitzonderlijke geval dat zich een verstoring voordoet waarbij fysieke interventie op locatie noodzakelijk is, zal de netwerkleverancier dit signaleren en de benodigde stappen en acties specificeren. Het uitgangspunt is dat de leverancier alle beheertaken en incidenten remote kan oppakken en oplossen, waardoor, bij het uitblijven van incidenten, geen tot zeer beperkte on-site inzet wordt verwacht gedurende de eerste jaren van de contractperiode.
20.	Selectiedocument, pg 15 (On site netwerkbeheer)	Wat zijn de reactietijden voor on site netwerksupport, binnen welke tijd moet Opdrachtnemer op locatie zijn?	Reactietijd on site: binnen een werkdag.
21.	Selectiedocument, pg 15 (On site netwerkbeheer)	Er wordt gesproken over uitvoeren van fysieke werkzaamheden aan de infrastructuur. Kunt u aangeven wat voor werkzaamheden dit mogelijk betreft, of specifieker zijn over wat voor infrastructuur?	Het betreft fysieke werkzaamheden aan de netwerkinfrastructuur op de locaties van het NIPV die de bestaande netwerkdienstverlener niet op afstand kan uitvoeren, zoals het op locatie uitvoeren van wijzigingen, checks of interventies aan netwerkcomponenten en bijbehorende infrastructuur. De exacte

			aard en omvang van deze werkzaamheden worden per incident of wijziging bepaald, in afstemming met het NIPV en de netwerkdienstverlener.
22.	Selectiedocument, pg 15 (On site netwerkbeheer)	Kunt u aangeven hoe u de demarcatie in verantwoordelijkheden ziet tussen de externe netwerkleverancier en on site netwerkbeheer bij de Opdrachtnemer (Hoe voorkomt u een grijs gebied?)	De demarcatie is als volgt te lezen: • De externe netwerkleverancier is verantwoordelijk voor ontwerp, configuratie, centrale monitoring en beheer van de netwerk-infrastructuur. • De opdrachtnemer kantoorautomatisering voert op verzoek van NIPV en in afstemming met de netwerkleverancier on-site werkzaamheden uit (uitvoering op locatie, “hands-on” support). • Het NIPV voert de regie en bewaakt de afspraken, zodat er geen grijs gebied ontstaat en taken expliciet worden belegd.
23.	Selectiedocument, pg 12 (Werkplekbeheer)	Op pg 12 wordt vermeld dat voor on site support de Opdrachtnemer nauw samenwerkt met NIPV. Betekent dit dat er op het vlak van on site support werkplekbeheer geen invulling wordt verwacht van de Opdrachtnemer (m.u.v. on site support t.b.v. netwerk?)?	Nee, deze veronderstelling is niet juist. De opdrachtnemer levert wél on-site ondersteuning binnen het domein van werkplekbeheer en eindgebruikersondersteuning. Dit is nadrukkelijk onderdeel van de scope, zoals beschreven in paragraaf 3.4.1 van het Selectiedocument.
24.	Bijlage 10, Tab Diensten, WPL-004	U vraagt om rapportage: "Kwaliteit van de dienstverlening (SLA&CSAT), inclusief de te verwachten ontwikkeling (1 kwartaal vooruitkijkend". Kunt u 2 voorbeelden geven van wat voor informatie u hier zoekt?	Bij deze rapportage denken we bijvoorbeeld aan: Terugblik afgelopen periode • Overzicht van gerealiseerde SLA’s (bijv. oplostijden, beschikbaarheid, aantal incidenten per prioriteit) en • De bijbehorende klant en gebruikers- tevredenheidscores (CSAT), inclusief korte toelichting op oorzaken van afwijkingen en trends. Vooruitblik komende periode • Verwachte ontwikkeling van de kwaliteit, zoals geplande verbetermaatregelen, bekende risico’s, verwachte

			piekbelasting (bijv. examens, migraties) en de impact hiervan op SLA/CSAT. Het doel is om zowel de huidige prestaties als de verwachte ontwikkeling concreet en inzichtelijk te hebben om te beoordelen of de dienstverlener de kwaliteit en verwachtingen kan waarmaken. Een aantal voorbeelden: Voor de aanbesteding is het voorstel drie kern-KPI's te hanteren die de kwaliteit en betrouwbaarheid van de dienstverlening borgen. Continuïteit & Servicekwaliteit wordt gestuurd via KPI's zoals snelle respons en hersteltijden bij P1-incidenten om downtime tot een minimum te beperken. Security & Compliance wordt gegarandeerd door tijdige installatie van kritieke patches, een voortdurend op peil gehouden Secure Score en periodieke hersteltests van back-ups om digitale weerbaarheid aantoonbaar te houden. Tot slot stimuleert Innovatie, Adoptie & Regie de proactieve waarde van de leverancier door het organiseren van innovatie-sessies, actief cloudkostenmanagement en het structureel actueel houden van documentatie, zodat de regieorganisatie altijd grip houdt en de IT-omgeving blijvend ontwikkelt.
25.	Bijlage 10, Tab Diensten, WPL-012	Bedoelt u hiermee dat de Opdrachtnemer buiten de kantoortijden remote standby heeft ter ondersteuning van P1 incidenten? Indien u dit niet bedoelt, kunt u dan nader specificeren wat hier bedoeld wordt en wat de verwachting is hoe vaak dit voorkomt?	Ja, dat is correct. Met WPL-012 wordt bedoeld dat de opdrachtnemer buiten kantoortijden beschikbaar en oproepbaar is voor de afhandeling van P1-incidenten en andere ernstige verstoringen, primair op remote basis.
26.	Bijlage 10, Tab Diensten, WPL-023	Kunt u aangeven welke certificeringen u hier bedoelt?	WPL-023 gaat niet over certificeringen, dus op deze vraag kunnen we geen antwoord geven.

27.	Bijlage 10, Tab Diensten, WPL-031	Bedoelt u hiermee dat incidenten/ verzoeken via de Servicedesk schriftelijk worden gelogd in service management tooling? Zo niet, kunt u dan aangeven wat wel bedoeld wordt?	Ja. Met WPL-031 wordt bedoeld dat alle meldingen via de Servicedesk, inclusief telefonisch gemelde incidenten en verzoeken, schriftelijk worden vastgelegd in de gebruikte service-managementtool(ing).
28.	Bijlage 10, Tab Diensten, SRV-006	U geeft aan dat een ticket wordt geregistreerd in het ticketsysteem van de Opdrachtgever, en via een koppeling wordt uitgewisseld met de Opdrachtnemer. Wij stellen voor, aansluitend bij onze standaard werkwijze, een ticket te registeren in ons eigen ticketsysteem (Opdrachtnemer) en deze door te zetten naar uw ticketsysteem. Is dit akkoord?	Ja, dat is een constructie waar wij ons in kunnen vinden. Daarbij is het wel van belang dat de betreffende medewerkers vanuit het NIPV service management systeem een registratie melding/mail ontvangt en in dit systeem ook updates kan zien/plaatsen. Voor de NIPV medewerkers moet het NIPV service management systeem altijd primair en leidend zijn.
29.	Bijlage 10, Tab Diensten, SRV-017	U geeft aan dat opdrachtnemer bij einde contract kosteloos aantoonbaar data moet vernietigen. Kunt u specifieker zijn rondom wat u verstaat onder aantoonbare vernietiging? Eventueel aan de hand van voorbeelden?	Onder "aantoonbare vernietiging" verstaat NIPV een proces waarbij de Opdrachtnemer middels een certificaat van datavernietiging of een formeel logboek aantoont dat alle (back-up)data permanent en onomkeerbaar is verwijderd uit alle systemen van de Opdrachtnemer. Dit moet voldoen aan de standaarden gesteld in de ISO 27001 en de verwerkersovereenkomst.
30.	Bijlage 10	Bijlage 10 is beveiligd. Dient deelnemer bijlage 10 in te vullen? Kunt u een versie publiceren die ingevuld kan worden?	Nee, bijlage 10 hoeft niet ingevuld te worden. Zie bijlage 1 Checklist aanmelding.
31.	PVE WPL035	Verwacht u ketenmonitoring voor monitoring van performance. Oftewel, dient de performance monitoring van end (werkplek) to end (bijvoorbeeld een database op een VM) te zijn?	Ja, NIPV verwacht dat de Opdrachtnemer de performance van de gehele keten monitort (end-to-end), van de eindgebruikerservaring op de werkplek tot de beschikbaarheid van de workloads in Azure. Dit is essentieel om proactief knelpunten te signaleren voordat de eindgebruiker hinder ondervindt.
32.	Selectiedocument pg 22, hoofdstuk 3.10 Waarde van de opdracht	Inschrijver constateert dat de rekensom van maximaal €300.000 aan diensten per jaar inclusief de eventuele projecten van €50.000 per jaar samen geen €7.000.000 aan totale waarde is zoals genoemd. Inschrijver ziet wel	Zie het antwoord op vraag 5.

		eventuele toevoegingen met een totale waarde van €2.480.000 staan maar dit maakt de rekensom niet kloppend. Dient inschrijver uit te gaan van €7.000.000 contractwaarde of de som van diensten voor €300.000 per jaar plus eventuele projecten van €50.000 per jaar plus de optionele waarde van €2.480.000? Hoe verhoudt deze som (€5.280.000) zicht tot de opgenomen totale waarde van €7.000.000?	
33.	Selectiedocument pg 12 (SPOC)	Zijn er externe partijen die gebruik maken van de SPOC diensten van inschrijver en zo ja, hoeveel.	Ja. Zoals in het Selectiedocument Kantoorautomatisering.pdf is beschreven, vallen onder meer het beheer van de netwerkomgeving en SOC-diensten buiten de scope van deze opdracht en worden deze geleverd door externe partijen. • Deze partijen zullen, voor zover relevant, via de SPOC-functie (servicedesk / regie) met Opdrachtnemer samenwerken bij incidenten, changes en projecten. • Het exacte aantal externe partijen kan in de tijd wijzigen (bijvoorbeeld bij contractwisselingen of uitbreiding van diensten). In elk geval gaat het ten minste om de netwerkleverancier en één of meer SOC-leveranciers, zoals ook in het Programma van Eisen wordt verondersteld (bijv. PVE SRV023). Een actueel overzicht van de betrokken externe leveranciers wordt in de transitiefase gedeeld, zodat Opdrachtnemer de SPOC-rol en ketensamenwerking kan inrichten.
34.	Geschiktheidseis 5: Referenties (relevante ervaring en competenties)	In "geschiktheidseis 5: Referenties" verzoekt u om aantoonbare ervaring in "IT dienstverlening" aan een organisatie van 300-800 gebruikers (niet groter of kleiner), waarbij IT Dienstverlening bestaat uit "de volledige scope van de onderhavige opdracht, zoals verwoord in paragraaf 3.4.1." Deze geschiktheidseis is zo geformuleerd dat uitsluitend	Het NIPV deelt de mening van de vraagsteller niet dat er sprake is van gelijke ervaring. De geraamde omvang van de opdracht op basis van het aantal medewerkers is genoemd in paragraaf 3.9 van het Selectiedocument. Dit aantal ligt op ongeveer het midden van de bandbreedte genoemd in kerncompetentie 1.

		gelijke referenties worden geaccepteerd, oftewel referenties die volledig voldoen aan de scope van de aanbesteding. Volgens artikel 2.93 lid 3 van de Aanbestedingswet 2012 mogen uitsluitend vergelijkbare referenties worden gevraagd. Deze geschiktheidseis is daarom niet proportioneel en u sluit hiermee erg veel partijen in de markt uit. Allereerst verzoeken wij u het aantal gebruikers niet te maximeren, maar uitsluitend de ondergrens aan te geven, dus: een organisatie met minimaal 300 gebruikers. Indien u hiertoe niet bereid bent, kunt u dit dan motiveren?	Kerncompetentie 1 laat het toe referenties in te dienen van een opdrachtgever met een aantal gebruikers binnen een ruime bandbreedte. Het aantal gebruikers kan zowel groter als kleiner zijn als dat van het NIPV zoals benoemd in paragraaf 3.9. Het aantal gebruikers hoeft dus niet gelijk te zijn aan dat van het NIPV. De omvang van de kerncompetentie is als zodanig opgenomen om het belang te onderstrepen dat het NIPV hecht aan de kwaliteit van dienstverlening die past bij een opdrachtgever van vergelijkbare omvang als het NIPV. Als de omvang van de opdrachtgever uit de referentie een omvang heeft die substantieel afwijkt van die van het NIPV, dus buiten de bandbreedte uit kerncompetentie 1 ligt, dan is het NIPV van oordeel dat dat invloed heeft op de dienstverlening en dat er dus geen sprake is van gelijkwaardige ervaring. Het NIPV zal de bandbreedte van de gebruikers in de kerncompetentie niet aanpassen.
35.	Geschiktheidseis 5: Referenties (relevante ervaring en competenties)	In "geschiktheidseis 5: Referenties" verzoekt u om aantoonbare ervaring in "IT dienstverlening" aan een organisatie van 300-800 gebruikers (niet groter of kleiner), waarbij IT Dienstverlening bestaat uit "de volledige scope van de onderhavige opdracht, zoals verwoord in paragraaf 3.4.1." Deze geschiktheidseis is zo geformuleerd dat uitsluitend gelijke referenties worden geaccepteerd, oftewel referenties die volledig voldoen aan de scope van de aanbesteding. Volgens artikel 2.93 lid 3 van de Aanbestedingswet 2012 mogen uitsluitend vergelijkbare referenties worden gevraagd. Deze geschiktheidseis is daarom niet proportioneel en u sluit hiermee erg veel partijen in de markt uit. Wij verzoeken u de kerncompetenties voor de opdracht	De Aanbestedende Dienst heeft de geschiktheidseis met betrekking tot de referenties (Eis 5) heroverwogen en past deze als volgt aan om de proportionaliteit te vergroten en de marktwerking te bevorderen: In plaats van de 'volledige scope' vraagt Aanbestedende Dienst om ervaring op de volgende drie geclusterde kerncompetenties: Cluster A: Werkplekbeheer & eindgebruikersondersteuning. Inclusief het technisch beheer van een Microsoft 365-tenant en een (skilled) servicedeskfunctie. Cluster B: Cloud-infrastructuur & Security. Inclusief het operationeel beheer van Microsoft Azure (landingszones),

		helder te bepalen, zie Voorschrift 3.5 F van de Gids Proportionaliteit. "er moet worden gezocht naar ervaring op punten die van essentieel belang zijn". 'De volledige scope van de dienstverlening' kan dan ook geen kerncompetentie zijn. De kerncompetenties zouden kunnen zijn: 1. Werkplekbeheer en eindgebruikersondersteuning, Microsoft 365-beheer 2. Microsoft Azure-beheer, Server beheer, Back-up en herstel, Beveiliging van de IT omgeving 3. Databeheer 4. Service management en governance Dit zou inhouden dat partijen ook maximaal 4 referenten mogen indienen (1 per kerncompetentie). Stemt u hiermee in en kunt u de geschiktheidseisen hierop aanpassen? Als u niet akkoord gaat, kunt u dit dan motiveren?	serverbeheer, back-up/herstel en integrale beveiligingsmaatregelen. Cluster C: Service Management, regie & transitie. Inclusief ervaring met het opereren in een SIAM-model (ketenregie met derden), het voeren van tactische regie voor een opdrachtgever en het succesvol uitvoeren van een transitietraject. Gegadigden mogen ter bewijsvoering van deze clusters maximaal twee (2) referentieopdrachten indienen. De clusters mogen over deze twee referenties verdeeld worden, mits de gecombineerde referenties alle drie de bovenstaande clusters afdekken.
36.	Geschiktheidseis 5: Referenties (relevante ervaring en competenties)	U verzoekt zowel in Referentie eis 1 als in referentie eis 2 om Adoptie. Wij verzoeken u om punt 10. Training en adoptie te laten vallen in Referentie eis 1 aangezien u deze al uitvraagt als tweede kerncompetentie.	Adoptie is een specifieke kerncompetentie, dit blijft onderdeel van de referentievraag. Deze is noodzakelijk om de ervaring met het totaalconcept te toetsen. De eis blijft gehandhaafd.
37.	PVE SEC044 -	Mean Time to Repair voor dienstverlening maximaal 2 uur bij hoogste prioriteit. In uw verslag marktverkenning bij vraag 33 geeft u als antwoord een oplostijd van maximaal 4 uur te verwachten voor een P1 verstoring. Vraag: Hoe verhoudt dit zich tot de gestelde 2 uur in deze eis. Inschrijver ziet dat deze eis is genoemd als indicatief maar vroegen ons toch af hoe u dit ziet. Of is dit van toepassing op alleen security incidenten en/of RPO/RTO?	De MTTR-eis van maximaal 2 uur voor P1-incidenten is een gewenste norm vanuit ons continuïteitsbeleid en sluit aan bij ons perspectief van BIO richtlijn 1.04 – hoofdstuk 17, waarin wordt benadrukt dat organisaties passende maatregelen moeten treffen om de continuïteit van vitale diensten te waarborgen. De in de marktconsultatie genoemde 4 uur betreft een indicatieve marktschatting en is niet kaderstelling voor deze aanbesteding. De 2-uurs MTTR is voor nu opgesteld als richtlijn waaraan inschrijvers moeten voldoen. Deze norm is indicatief opgenomen en kan in de definitieve versie nog worden bijgesteld, mede op basis van verdere verfijning van eisen en proportionaliteit. De eis geldt voor alle P1-incidenten, niet uitsluitend voor security-incidenten of RPO/RTO-situaties.

38.	PVE SEC081	De organisatie heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren. Met name de uitval van diensten van derden en onze getroffen maatregelen is naar ons idee een eenzijdige maatregel. Vraag: Het netwerk wordt beheerd door een derde partij (u vraagt hierbij wel onsite ondersteuning voor netwerk), mag inschrijver ervan uitgaan dat dergelijke derde partijen ook zijn voorzien van heldere processen en afspraken voor de gevraagde getroffen maatregelen zodat we gezamenlijk voorkomen dat een dienst uitvalt en hier dan ook een gezamenlijke verantwoordelijkheid ligt? Netwerk is bijvoorbeeld een belangrijke schakel in de keten voor de dienstverlening.	Ja, inschrijver mag ervan uitgaan dat ook de door het NIPV gecontracteerde netwerkleverancier beschikt over heldere processen, afspraken en beveiligings- en continuïteitsmaatregelen. Deze partij is verantwoordelijk voor het beheer van de netwerk-infrastructuur, zoals firewalls, routers, switches en internetverbindingen, en werkt binnen duidelijke scope- en kwaliteitsafspraken die de continuïteit waarborgen.
39.	PVE SRV023	De Opdrachtnemer werkt actief samen met SOC-leveranciers voor detectie en respons op beveiligingsincidenten. U geeft aan SOC-leveranciers aan in meervoud. Vraag: Hoeveel leveranciers zijn dit?	Dit gaat bij start van de dienstverlening om 2 leveranciers; • De netwerkdienstverlener die ook bewaking doet vanuit een NOC; • De SOC leverancier die de IT-omgeving bewaakt.
40.	PVE TRX002	Op eerste aangeven stelt Opdrachtnemer, binnen 3 maanden, een Exit-plan op. Het Exit-plan dient ter goedkeuring aan het NIPV te worden voorgelegd. In dit plan wordt o.m. opgenomen hoe ALLE documentatie en configuraties wordt overgedragen aan het NIPV danwel een evt nieuwe Opdrachtnemer. Ook wordt aangegeven hoe na de overdracht de bestaande data definitief en onomkeerbaar wordt gewist. Vraag: is er een huidig exitplan aanwezig?	Er is op dit moment geen exitplan aanwezig.

41.	PVE WPL008	Opdrachtnemer richt back-up en herstel in voor Microsoft 365 en Azure workloads met afgesproken RPO/RTO en testfrequentie. Vraag: zijn deze waarden al bekend of volgen deze in de volgende fase?	RPO en RTO waarden worden in de volgende fase meegenomen.
42.	PVE WPL016	Alle internetgebruikersinterfaces moeten worden beveiligd met Multi-Factor Authentication. Vraag: Wat verstaat u onder alle internetgebruikersinterfaces? Het kan zijn dat er internetgebruikersinterfaces buiten onze diensten worden gebruikt die niet geschikt zijn voor Multifactor Authentication (MFA).	Met “alle internetgebruikersinterfaces” wordt bedoeld: Alle door Opdrachtnemer aangeboden en/of beheerde web- of cloud-gebaseerde toegangspunten waarmee gebruikers bij NIPV-data en NIPV-diensten komen. Voor systemen buiten de scope van Opdrachtnemer (bijvoorbeeld specifieke externe SaaS-oplossingen die NIPV zelf afneemt) geldt: • Opdrachtnemer is niet verantwoordelijk voor het technisch realiseren van MFA op die diensten; • Waar mogelijk wordt geadviseerd om SSO toe te passen, zodat MFA centraal via de IdP kan worden afgedwongen. Indien een specifieke interface technisch niet geschikt is voor MFA, wordt in overleg een passend alternatief beveiligingsniveau bepaald en vastgelegd.
43.	PVE WPL017	De dienst en gebruikte oplossing dient aan te sluiten bij de NIPV Architectuur en aansluitvoorwaarden. Vraag: welke architectuur (principes) en aansluitvoorwaarden zijn dit? Wordt er bijvoorbeeld gebruik gemaakt van een architectuurraamwerk zoals de NORA, CAF, etc.	Aanbestedende Dienst werkt zoveel mogelijk ‘onder architectuur’ en op basis van TOGAF als architectuurraamwerk. Er worden o.a. 10 architectuurprincipes gehanteerd. Deze zijn deels afgeleid van NORA en de VeRA (Veiligheidsregio’s Referentie Architectuur): • Standaardiseer waar mogelijk • Tijdig voldoen aan de wet • Security en Privacy by design • Gezamenlijk, tenzij • Informeer bij de bron • Hergebruik vóór kopen vóór maken

			• Data als strategische asset • Ethisch en transparant • Voorkom onnodige complexiteit • Verplaats je in de gebruiker Daarnaast hanteert Aanbestedende Dienst ook het Cloud Adoption Framework (CAF) van Microsoft.
44.	PVE WPL026	Opdrachtnemer levert een servicedesk voor eindgebruikers tijdens kantooruren en optioneel buiten kantooruren (beschrijf openingstijden en doorlooptijden). Vraag: betreft dit een eerste lijn servicedesk? Met andere woorden, is de eerste lijn servicedesk naast tweede/derde lijn in scope en hoe ziet u het proces bij een eerste lijn servicedesk met de koppeling tussen onze SMT (service management tool) en uw Jira SMT? Omdat u in de scope van de selectieleidraad geen servicedesk benoemt, nemen we aan dat de eerste lijn door u wordt ingevuld? Is deze aanname juist?	In het Selectiedocument Kantoorautomatisering is beschreven dat Opdrachtnemer verantwoordelijk is voor werkplekbeheer en eindgebruikersondersteuning, inclusief servicedeskfunctionaliteit. WPL026 ziet primair op de door Opdrachtnemer geleverde servicedesk voor eindgebruikers. Deze omvat naast eerste lijn service ook minimaal tweede- en derdelijns ondersteuning.
45.	PVE WPL031	Meldingen via de telefoon moeten ook schriftelijk worden vastgelegd. Vraag: voor snelle afhandeling en borging van een incident stellen wij voor dat het self-service portaal het primaire middel is voor het melden van een incident. Of heeft u de verwachting dat de servicedesk vooral gebeld wordt?	Het NIPV stimuleert het gebruik van digitale kanalen (self-service portaal en e-mail) als primaire meldkanalen, in lijn met de gewenste standaardisatie en rapportagemogelijkheden. Tegelijk geldt: • Telefonische meldingen blijven noodzakelijk voor incidenten met prioriteit en voor gebruikers die (tijdelijk) geen toegang hebben tot digitale middelen; • Ongeacht het kanaal geldt dat iedere melding altijd in het ITSM-systeem wordt vastgelegd (dit is de strekking van WPL031).
46.	Selectiedocument pg 51, H8.3	Wat wordt bedoeld met "Actieve SLA's"? (in het geval wij een dienst leveren aan een klant, is deze actief; wij kennen geen inactieve SLA's)	Met “actieve SLA’s” worden bedoeld: Alle op het moment van de gestelde periode van 12 maanden lopende SLA-afspraken tussen Gegadigde en zijn klanten,

			waarmee de prestaties van de door Gegadigde geleverde diensten worden gemeten. Dit ter onderscheid van bijvoorbeeld: • beëindigde SLA's (historisch); • SLA-voorstellen/offertes die nog niet zijn ingegaan. In het overzicht dat bij selectiecriterium S2 wordt gevraagd, gaat het dus om SLA's die gedurende de betreffende 12 maanden periode daadwerkelijk van kracht waren.
47.	Selectiedocument pg 51, H8.3	Wat wordt bedoeld met "het onderwerp van de SLA"? Bedoelt u hiermee: werkplekdienst, netwerkdienst, etc, namelijk het type dienstverlening?	Ja, hiermee wordt het type dienstverlening bedoeld.
48.	Selectiedocument pg 51, H8.3 – S2	U vraagt gegadigde om een samengevoegd overzicht van de behaalde SLA-prestaties over een periode van 12 maanden, teruggerekend vanaf het moment van Aanmelden, inclusief: o het totaal aantal actieve SLA's, inclusief het onderwerp waarvoor een SLA is afgesproken; o het percentage behaalde SLA's, onderverdeeld naar de onderwerpen waarvoor SLA's worden afgesproken; Hoe beoordeelt u de informatie die wordt opgeleverd: gaat het er om dat de gegadigde deze informatie registreert en dus kan opleveren? Of beoordeelt u hier de prestatie van de Gegadigde? Interpretatie van de gevraagde data zonder context (diensten en de bijbehorende afspraken, KPI's etc) kan een verkeerd beeld geven.	De beoordelingsgrond is de mate waarin de dienstverlening en klantgerichtheid wordt nageleefd. Naast het samengevoegde overzicht van de SLA-prestaties (1e bullet) vraagt de Aanbestendende dienst ook een toelichting (bullet 2-4). Deze toelichting voorziet het beoordelingsteam van de juiste interpretatie op het samengevoegde overzicht. Zie tevens het antwoord op vraag 12.
49.	Selectiedocument pg 51, H8.3 – S2	Bedoelt u met het percentage behaalde SLA's, het percentage op organisatieniveau?	Het gaat om zowel een percentage op dienstniveau als ook een overkoepelend percentage op organisatieniveau.

50.	Selectiedocument pg 51, H8.3	Kunt u een format leveren waarin de gevraagde informatie moet worden aangeleverd zodat de beoordeling transparant is op basis van dezelfde indicatoren onder alle gegadigden.	Aanmelders mogen hiervoor een eigen format gebruiken. Zie tevens het antwoord op vraag 48.
51.	PVE SRV012	U geeft aan dat zowel updates als upgrades binnen de prijzen van het Prijsmodel dienen te vallen. Wij zien hierin echter een wezenlijk verschil. Updates betreffen reguliere activiteiten (bijvoorbeeld maandelijks of per kwartaal) en zijn voorspelbaar in zowel frequentie als tijdsbesteding. De uitvoering vindt plaats via het reguliere changemanagementproces en past daarmee goed binnen het Prijsmodel. Upgrades daarentegen kennen een onregelmatig karakter en vergen doorgaans aanzienlijk meer inspanning, zowel qua omvang als impact, voor zowel Opdrachtnemer als Opdrachtgever. De uitvoering hiervan vindt meestal plaats in projectvorm. Om deze reden stellen wij voor om upgrades niet op te nemen binnen het Prijsmodel, maar deze buiten het Prijsmodel te houden. Is dit akkoord?	Het NIPV houdt vast aan de eis dat reguliere lifecycle-updates (zoals nieuwe Windows- of M365-versies) onderdeel zijn van de vaste beheerprijs. Ingrijpende functionele migraties of architectuurwijzigingen (upgrades) die op verzoek van NIPV plaatsvinden, kunnen als projecturen (€ 50.000,- budget) worden afgehandeld.
52.	PVE SRV-016	Kunt u specifieker aangeven wat bedoeld wordt met 'verzamelde gegevens?	Met ‘verzamelde gegevens’ in SRV-016 wordt bedoeld: alle beheer- en servicemanagementdata die Opdrachtnemer gedurende de opdracht genereert of opslaat ten behoeve van NIPV, zoals: • configuratie- en inventarisgegevens (CMDB / configuratieoverzichten); • monitoring- en performancedata; • incident-, change- en problem-registraties; • use cases voor monitoring/security (incl. versies en wijzigingen); • gegevens die worden gebruikt om afwijkend gedrag in de infrastructuur te detecteren (alerts, correlatieregels, trendinformatie).

			Het gaat niet om willekeurige commerciële of interne data van Opdrachtnemer, maar uitsluitend om gegevens van en over NIPV en de NIPV-omgeving die nodig zijn voor: • overdracht aan NIPV of een nieuwe leverancier (exit); • borging van continuïteit, security en compliance.
53.	PVE SRV022	Kunt u specifieker aangeven wat u bedoelt met logboekbronnen (welke) en log?	Met “logboekbronnen” bedoelen we alle systemen en componenten die relevante logs genereren en binnen de scope van de dienstverlening vallen.
54.	PVE WPL010	"Opdrachtnemer dient bij het uitvoeren van on-site netwerkondersteuning te specificeren met welke interne en externe systemen en netwerken gecommuniceerd moet (kunnen) worden teneinde de juiste wijzigingen in connectiviteit en routering binnen de netwerken van Opdrachtgever (NIPV) te kunnen aanbrengen, aanpassen of valideren." Aangezien een leverancier van NIPV verantwoordelijk is voor het netwerk, verwachten wij dat deze leverancier deze eisen stelt, en de Opdrachtnemer aangeeft of hier aan kan worden voldaan. Kunnen u deze eisen delen?	Opdrachtnemer stemt in overleg met opdrachtgever af welke specificaties nodig zijn ten behoeve van de dienstverlening, waarbij in overleg met de netwerkbeheer de juiste inrichting wordt gerealiseerd.
55.	PVE WPL011	"Opdrachtnemer beheert netwerk- en printerdiensten op locatie op aanvraag van het NIPV" Kunt u aangeven op welke wijze u hier invulling verwacht: vaste inzet op vaste dagen? Of op basis van planning? In het laatste geval, wat is de verwachting hoe snel de Opdrachtnemer ter plaatse kan zijn? Of op basis van incidenten? Hoe vaak verwacht u aanwezigheid?	On-site inzet is niet vast maar op afroep, gestuurd door NIPV-regie, op basis van concrete behoefte (incidente, projecten of changes). Meer informatie over de aanwezigheid is te vinden in het antwoord op vraag 19.
56.	PVE WPL011	Heeft NIPV de beschikking over supportcontracten van printers? Zo ja, wat verwacht u van on site ondersteuning door de Opdrachtnemer? Welke activiteiten? In H3.5 plaatst u de activiteiten rondom printers buiten scope.	In H3.5 wordt expliciet de multifunctionele printers buiten scope geplaatst. Het beheer van deze apparatuur, inclusief onderhoud en eventuele on-site ondersteuning, wordt uitgevoerd door een reeds gecontracteerde dienstverlener.

			De opdrachtnemer is daarentegen wel verantwoordelijk voor de softwarematige componenten binnen de werkplekomgeving, waaronder: • Windows-gerelateerde printproblemen; • driver-issues; • printermapping vanuit de werkplek; • ondersteuning bij printproblemen die voortkomen uit de werkplekinrichting. Op deze manier blijft de scheiding van verantwoordelijkheden voor multifunctionals helder: hardware en fysieke service via de printer partner, werkplekgerelateerde printfunctionaliteit via de opdrachtnemer. Daarnaast beschikt NIPV nog wel over een aparte printserver voor de aansturing van een beperkt aantal werkplek gebonden printers, zoals labelprinters en printers in het magazijn. Het beheer van deze omgeving valt binnen de verantwoordelijkheden van de opdrachtnemer.
57.	PVE WPL025	U bedoelt hier de *"bij de Opdrachtnemer in beheer zijnde"* componenten?	Ja. Met de “componenten” in WPL-025 worden bedoeld: alle IT-componenten binnen de scope en in beheer bij Opdrachtnemer.
58.	PVE WPL029	Over hoeveel IT en SOC leveranciers gaat het? En waarom is de SOC leverancier hier niet leidend in?	De rolverdeling is bewust als volgt ingericht: • de SOC-leverancier levert 24/7 detectie, analyse en specialistische security-expertise (buiten scope van deze aanbesteding); • de Opdrachtnemer is integraal beheerder van de kantoorautomatiseringsomgeving, is verantwoordelijk voor de security configuratie van de IT omgeving, (werkplekken, servers, Azure/M365) en: ○ is primair aanspreekpunt voor NIPV;

			○ bundelt informatie uit SOC, monitoring en eigen beheer; ○ bereidt mitigerende maatregelen en changes voor; ○ neemt volgens WPL-029 een leidende rol in de ketenafstemming. De SOC-partij is dus leidend in detectie & specialistische analyse, terwijl de Opdrachtnemer leidend is in regie, coördinatie en doorvoering van maatregelen binnen de beheerde omgeving.
59.	PVE WPL035	Welke verwachting heeft u van een performance rapportage. Dit is belangrijk om te weten, zodat wij een inschatting kunnen maken of we hiervoor ook tooling in moeten richten.	Het betreft een indicatieve eis; de Aanbestedende Dienst neemt de suggestie mee en past dit indien gewenst aan in de definitieve versie die tijdens de gunningsfase wordt gepubliceerd.
60.	PVE ALG025	Wij werken met vaste contactpersonen; echter een persoon kan wel gedurende de contractperiode vervangen worden (bv bij uitdiensttreding). Kunt u deze eis hierop herformuleren?	De Aanbestedende Dienst zal dit in het definitieve pve wijzigen.
61.	Selectiedocument	In het Selectiedocument wordt gesproken over werken via het ticketsysteem van de Opdrachtnemer, aangevuld met meldingen vanuit NIPV via telefoon, e-mail en een online portaal. Daarnaast wordt specifiek verwezen naar Exact Synergy als voorbeeld bij integraties (§3.2). In het Programma van Eisen (PvE SRV-024) staat echter dat de Aangeboden Oplossing procedureel moet aansluiten op de processen van het NIPV en dat de opdrachtnemer via een geautomatiseerde koppeling dient aan te sluiten op Jira Service Management. Wilt u bevestigen welk ticketsysteem leidend is voor: 1. registratie van incidenten, changes en aanvragen door NIPV (NIPV-tooling),	Momenteel loopt er een project voor de overgang van Exact Synergy naar Jira. De huidige planning is dat bij aanvang van de dienstverlening vanuit deze aanbesteding het Service Management systeem Jira is. Dit project is ongoing en daarom is er zowel over Exact Synergy als Jira gesproken in de documenten.

		2. registratie en afhandeling in de keten (tooling opdrachtnemer), 3. de verplichte geautomatiseerde koppeling zoals opgenomen in PvE SRV-024? Daarnaast verzoeken wij te verduidelijken of Synergy nog een rol speelt in de beoogde dienstverlening of als voorbeeld ter referentie is opgenomen.	
62.	Selectiedocument	Het Selectiedocument benoemt dat on-site netwerkondersteuning (Arnhem en Zoetermeer) onderdeel is van de scope, maar kwantitatieve verwachtingen (frequentie, responstijden, minimale beschikbaarheid) ontbreken. Kunt u aangeven: 1. wat de minimale vereisten zijn voor on-site beschikbaarheid (aantal dagdelen per week/maand), 2. wat de gewenste of verwachte responstijd is voor on-site taken bij storingen of projecten, 3. of er piekmomenten zijn (bijv. examens, evenementen, migraties) die structureel hogere on-site capaciteit vereisen?	Zie het antwoord op vragen 15 t/m 20.
63.	Selectiedocument	Wij beschikken over aantoonbare, langdurige ervaring met volledig vergelijkbare ITdienstverleningstrajecten (werkplekbeheer, Microsoft 365beheer, Azurebeheer, security, service management, adoptie) voor organisaties tot ca. 220 werkplekken. Deze referenties omvatten nagenoeg dezelfde functionele scope, complexiteit, ketensamenwerking en securityeisen als in de onderhavige aanbesteding. Conform de geldende Proportionaliteitsgids geldt als uitgangspunt dat referentie-eisen in redelijke verhouding dienen te staan tot de aard en omvang van de opdracht.	Vraag 1. De bandbreedte is gerelateerd aan het aantal gebruikers genoemd in paragraaf 3.9 van het Selectiedocument. Daarin is benoemd dat de omvang van de opdracht circa 608 gebruikers betreft. De bandbreedte start op 49% van dat aantal. De omvang van de kerncompetentie is opgenomen om het belang te onderstrepen dat het NIPV hecht aan de kwaliteit van dienstverlening die past bij een opdrachtgever van vergelijkbare omvang als het NIPV. Als de omvang van de opdrachtgever uit de referentie een omvang heeft die substantieel afwijkt van die van het NIPV, dus buiten de bandbreedte uit kerncompetentie 1 ligt, dan is het NIPV van oordeel dat dat invloed heeft op de

		Daarbij wordt veelal een richtlijn van circa 60% van de omvang van de opdracht als proportioneel beschouwd voor referenties. Onze vragen zijn daarom: 1. Kunt u toelichten waarom specifiek de bandbreedte van 300–800 gebruikers noodzakelijk wordt geacht om de gevraagde ervaring en complexiteit aan te tonen? 2. Staat de Aanbestedende Dienst open voor het accepteren van referenties met een lager aantal werkplekken (bijvoorbeeld tussen 200–500), mits de inhoudelijke scope, technische complexiteit en governance vergelijkbaar zijn met de gevraagde dienstverlening?	dienstverlening en dat er dus geen sprake is van gelijkwaardige ervaring. Vraag 2. Het NIPV ziet geen reden voor een aanpassing. De gevraagde omvang van de referentie is proportioneel en staat in verhouding tot de omvang van de opdracht. Bovendien valt de door vraagsteller genoemde bandbreedte goeddeels al binnen de omvang van de geschiktheidseis die het NIPV aanhoudt.
64.	Selectiedocument, blz. 46, 7.3 Financiële en economische draagkracht	Aanbestedende dienst vraagt na gunning een goedgekeurde accountantsverklaring. Inschrijver maakt gebruik van de accountantsverklaring uit het geconsolideerde jaarverslag van haar moedermaatschappij en publiceert geen zelfstandige cijfers. Inschrijver voldoet zelfstandig aan de gestelde selectiecriteria en doet geen beroep op de draagkracht van haar moedermaatschappij om te voldoen aan de selectiecriteria. Accepteert Aanbestedende dienst de accountantsverklaring van onze moedermaatschappij in combinatie met de 403 verklaring welke gedeponeerd is bij de Kamer van Koophandel zonder dat er een eigen UEA voor onze moedermaatschappij wordt ingediend?	Ja, dat is akkoord.
65.	Bijlage 10 Programma van Eisen, tab 01 Diensten, regel 2	Wat wordt er bedoeld met on premise omgeving en waar draait deze on premise omgeving?	Zie het antwoord op vraag 4.

66.	Selectieleidraad, blz. 40, 5.5 Beroep op derden	Het is Inschrijver niet duidelijk of zij voor deze uitvraag een Derden / Onderaannemer wil gaan inzetten, aangezien de scope nog niet helder en duidelijk is. Gaat Aanbestedende dienst akkoord met het feit dat in de RFP-fase nog een Derden / Onderaannemer toegevoegd kan worden? Uiteraard zal Inschrijver dan daarvoor een gewijzigde Eigen Verklaring (UEA) aanleveren.	Dat is akkoord. Het NIPV is ermee akkoord dat een Onderaannemer, dus een partij die werkzaam is in opdracht van de Opdrachtnemer, die slechts bedoeld is voor het uitvoeren van (een deel van) de Opdracht en die niet nodig is om te voldoen aan de Geschiktheidseisen en / of de Selectiecriteria, pas in de gunningsfase kenbaar wordt gemaakt. Dat mag er niet toe leiden dat de Aanmelding wijzigt. De Inschrijver moet ook in dat geval de in paragraaf 5.5 Selectiedocument genoemde informatie en documenten van / over de Onderaannemer aanleveren. Het NIPV heeft in die fase nog steeds het recht om inzet van de Onderaannemer te weigeren als blijkt dat op de Onderaannemer een of meerdere Uitsluitingsgronden van toepassing zijn. Als de Onderaannemer om die reden wordt geweigerd, dan kan de Inschrijver ervoor kiezen om toch geen Onderaannemer in te zetten, dan wel een vervangende Onderaannemer in te zetten. De Inschrijver moet diens beslissing, met bijvoeging van de eventueel benodigde informatie / documenten, aan het NIPV kenbaar maken binnen de door het NIPV genoemde termijn.
67.	Selectieleidraad blz. 22, 3.10 Waarde van de Opdracht	Kunt u toelichten hoe u tot het bedrag komt van Euro 7.000.000, - als maximale waarde van de overeenkomst. Welke posten neemt u mee in deze opteling. Kunt u toelichten welke aannames zijn gehanteerd bij het bepalen van de maximale contractwaarde van €7.000.000, en of deze mede ziet op mogelijke uitbreidingen uit paragraaf 3.6?	Zie het antwoord op vraag 5.
68.	Selectieleidraad blz. 12	U beschrijft dat de verantwoordelijkheid van regulier beheer op Windows devices, en indien van toepassing andere	Deze systemen zijn beschreven in hoofdstuk 3.9 Omvang van de opdracht.

		systemen de verantwoordelijkheid is van de opdrachtnemer. Wat bedoelt u met andere systemen?	
69.	Paragraaf 3.4.1 en 3.5	In paragraaf 3.4.1 en 3.5 wordt aangegeven dat connectiviteit, netwerkbeheer en SOC-dienstverlening buiten scope vallen, terwijl de Opdrachtnemer wél verantwoordelijk is voor opvolging van SOC-tickets, security-incidenten en on-site netwerkondersteuning. Kunt u verduidelijken waar exact de grens ligt tussen de verantwoordelijkheden van de Opdrachtnemer en de bestaande netwerk- en SOC-dienstverleners, met name bij security-incidenten en netwerk gerelateerde verstoringen, en hoe aansprakelijkheid is belegd?	Zie het antwoord op vraag 58.
70.	par. 3.4.1	De Opdrachtnemer fungeert als SPOC voor alle meldingen (par. 3.4.1), terwijl meerdere diensten expliciet door derden worden geleverd. Betekent het SPOCprincipe- dat de Opdrachtnemer --verantwoordelijk is voor coördinatie en doorlooptijd, ook als de oorzaak buiten de eigen scope ligt?	De Opdrachtnemer is wel verantwoordelijk voor coördinatie en ook voor de doorlooptijd van de activiteiten en acties aan kant van de Opdrachtnemer. Indien een derde partij niet voldoet aan de SLA's dan dient het NIPV regie team hierover te worden geïnformeerd en zullen ze dit oppakken met de betreffende partij.
71.	paragraaf 3.10	In paragraaf 3.10 wordt uitgegaan van een vast bedrag per reguliere gebruiker per maand, met daarnaast incidentele gebruikers. Kunt u nader specificeren hoe wordt omgegaan met structurele schommelingen in aantallen gebruikers en devices gedurende de looptijd (bijvoorbeeld als gevolg van seizoenspieken, projecten, crisisopschaling)?	Door een vast bedrag per gebruiker/gebruikersgroep per maand te stellen kunnen de kosten maandelijks fluctueren. Het schaalt mee met de groei of krimp van het NIPV.

72.	paragraf 3.10	Projectmatige inzet (500 uur / €50.000 per jaar) “maakt onderdeel uit van de opdracht”, maar is niet verplicht af te nemen (paragraf 3.10 Waarde van de opdracht). Kunt u bevestigen of projectmatige inzet binnen de bestaande SLA-verplichtingen valt, of dat hiervoor afzonderlijke prioritering, planning en acceptatiecriteria gelden?	Voor de projectmatige inzet worden aparte SLA afspraken gemaakt. Dit soort werkzaamheden moeten goed gepland worden en vergen beschikbaarheid van het projectteam van de Opdrachtnemer en het regie team van het NIPV.
73.	Hoog-risico AI is uitgesloten (par. 3.12).	Kunt u bevestigen hoe NIPV omgaat met standaard Microsoft 365-functionaliteiten waarin AI-componenten zijn geïntegreerd (zoals Copilot, Defender AI-features), en hoe wordt bepaald wat als “hoog-risico AI” wordt aangemerkt?	Het gaat hier om de AI die door opdrachtnemer wordt gebruikt. Voor de bepaling of AI onder een hoog risico valt, wordt uitgegaan van de definities zoals die in de AI-act zijn opgenomen. In zijn algemeen kun je stellen dat AI die mogelijk gevolgen heeft voor de fundamentele rechten van mensen een hoog risico vormen. In het algemeen zal gebruik van normale Microsoft functionaliteiten niet tot een hoog risico leiden, maar dat is afhankelijk van de toepassing van die AI door opdrachtnemer. Opdrachtnemer dient dus zelf (zoals ook in de AI-act vereist) te bepalen of haar AI gebruik onder een hoog risico valt.
74.	Paragraaf 3.4.1	De Opdrachtnemer is verantwoordelijk voor transitie, maar de omvang hiervan is niet nader gekwantificeerd (Paragraaf 3.4.1) Kunt u aangeven welke concrete transitieactiviteiten bij start worden verwacht en of hiervoor een afzonderlijk budget of fasering wordt voorzien?	In de gunningsfase wordt van de geselecteerde Inschrijvers gevraagd om een gedetailleerd Implementatieplan en een Transitiebudget (via het prijzenblad) in te dienen. Het NIPV wijst er volledigheidshalve op dat voor de daadwerkelijke invulling ook input van de Opdrachtnemer nodig is. De volgende transitieactiviteiten moet de Opdrachtnemer — in abstracto — uitvoeren om tot een bedrijfsvaardige oplevering te komen: • Nulmeting en baseline: uitvoeren van een technische en functionele inventarisatie om het referentiepunt van de huidige ICT-infrastructuur vast te leggen.

			• Dossier Afspraken en Procedures (DAP): in samenspraak met NIPV uitwerken van de procesafspraken (RASCI), communicatielijnen en de escalatiepaden. • Kennisoverdracht: borgen van de overdracht van technische en functionele documentatie van het huidige team naar de nieuwe beheerorganisatie. • Servicedesk-integratie: realiseren van de geautomatiseerde koppeling tussen de ITSM-tooling van de Opdrachtnemer en de Jira Servicedesk van het NIPV. • Service-inrichting: operationeel maken van de SPOC-functie, inclusief de bereikbaarheid en routering van meldingen.
75.	Selectieleidraad blz. 13	Hier wordt een overzicht van incidenten weergegeven. Kunt u een indicatie geven van welk percentage van deze incidenten en/of wijzigingen on-site ondersteuning vereiste voor de oplossing?	Verreweg de meeste incidenten zijn remote/online te verhelpen. Een percentage van incidenten en/of wijzigingen die on site ondersteuning vereisen is lastig omdat in het huidige systeem niet wordt geregistreerd of het op locaties wordt opgelost. De voornaamste vraagstukken en incidenten die lokaal worden opgelost hebben te maken met het uitleveren apparatuur aan nieuwe medewerkers, het innemen van apparatuur van medewerkers die de organisatie verlaten en het oplossen van problemen met lokale voorzieningen.
76.	Selectieleidraad blz. 7	U geeft aan dat er al intensief gebruik wordt gemaakt van Microsoft 365 voor productiviteit en communicatie. Betekent dit dat alle gebruikers data en bedrijfsdata al lokaal beschikbaar is op de moderne werkplek in Teams, SharePoint, OneDrive en Outlook?	Dit is correct. Alle gebruikers data en bedrijfsdata is beschikbaar in Teams, SharePoint, OneDrive en Outlook. Er wordt geen gebruik meer gemaakt van lokale (on prem) shares.
77.	Selectieleidraad blz. 14	Wat wordt er bedoeld met Teambeheer, en welke partij verantwoordelijk voor het beheer.	Hiermee wordt het beheer van Microsoft Teams verstaan, opdrachtnemer is hiervoor verantwoordelijk.
78.	Selectieleidraad blz. 17	Er wordt ook een adoptieprogramma gevraagd. Kunt u aangeven wat het huidige volwassenheidsniveau is van medewerkers van NIPV in het gebruik van Teams, SharePoint en OneDrive?	Er wordt dagelijks gebruik gemaakt van Teams, SharePoint en Onedrive bij het NIPV. De volwassenheid verschilt per afdeling en per persoon en hierin zijn veel niveaus te onderkennen (van onbekwaam naar volledig bekwaam). Het is voor NIPV van

			belang dat hier nog extra aandacht aan wordt gegeven en vooral om alle waarde te halen uit de mogelijkheden/opties van de Microsoft 365 suite.
79.	Bijlage 03 en 04	Kunt u deze documenten ook in een Word-versie verstrekken?	Ja, de documenten zijn toegevoegd.
80.	Bijlage 10 Programma van Eisen	In het programma van Eisen zijn in meerdere tabbladen witregels te vinden waar in kolom E of F wel een kruis staat. Gegadigde vraagt zich af of deze lijst compleet is hierdoor. Kunt u dit controleren en bij onvolledigheid een nieuwe versie verstrekken?	Dit gaat om SEC-082 t/m SEC-098. Dit zijn in deze fase van de aanbesteding allemaal indicatieve eisen.
81.	7.4 Technische en beroepsbekwaamheid, geschiktheidseis 4.	U schrijft hier dat Gegadigde minimaal een geldige Mircrosoft Solutions Partner Designation in het voor de Opdracht relevante oplossingsgebied te weten: Modern Work, Security Azure infrastructure. Vervolgens schrijft u: Hieronder worden verstaan de door Microsoft vastgestelde Solution partner-oplossings gebieden waaronder in ieder geval: waarna een opsomming volgt. Het is Gegadigde niet duidelijk of alle genoemde Solution Partner in het bezit moeten zijn van Gegadigde of één van de drie. Graag uw toelichting hoe dit te lezen.	Eis is minimaal één van de drie.
82.	3.4.1 Opdracht (scope) omschrijving punt 4 serverbeheer	Kunt u meer informatie verschaffen over welk type en aantallen on-premise servers het hier gaat, deze informatie is voor Gegadigde cruciaal om een inschatting te kunnen maken of deze in beheer te nemen is en de gevraagde continuiteit te waarborgen.	Zie het antwoord op vraag 4.
83.	3.4.1 Opdracht (scope) omschrijving punt 4 serverbeheer	Is het mogelijk om de on-premise servers te verhuizen naar een datacenter van Gegadigde?	Het doel is om alle resterende servers in 2026 uit te faseren. Daarmee is dit niet nodig. Zie aanvullend het antwoord op vraag 4.

84.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Is er een serviceportaal beschikbaar of moet opdrachtnemer die leveren?	Er is momenteel een serviceportaal beschikbaar in Exact Synergy.
85.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Wordt gewerkt met de telefooncentrale/systeem van opdrachtgever?	Ja, dit is mogelijk. Er wordt bij het NIPV gewerkt met Teams bellen.
86.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Wat zijn de gewenste serviceniveaus en openingstijden voor de servicedesk?	Openingstijden zijn tussen 08:00 – 17:30. Serviceniveau's: 1e, 2e en 3e lijns.
87.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Kan opdrachtgever inzicht geven in de verwachte lokale aanwezigheid per locatie?	Het NIPV stelt geen eis voor vaste lokale aanwezigheid (bijvoorbeeld op vaste weekdagen). De inzet van de Opdrachtnemer op de locaties (Arnhem en Zoetermeer) vindt plaats op afroep en basis van noodzakelijkheid, zoals bij: • Incidenten die niet op afstand (remote) oplosbaar zijn. • Geplande projectactiviteiten of fysieke wijzigingen aan de infrastructuur. Voor reguliere, kleine hardware handelingen (zoals het fysiek aanreiken van een leenlaptop of een simpele patch-handeling)

			kan in overleg gebruik worden gemaakt van de interne NIPV-liaison die aanwezig is op de Servicedesk. De exacte procedurele afspraken over de inzet van de NIPV-liaison versus de technici van de partner worden na gunning vastgelegd in de service-uren binnen het Dossier Afspraken en Procedures (DAP).
88.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Staat opdrachtgever open voor een servicedesk op locatie?	Ja, dit zou kunnen bijdragen aan de snelheid van handelen en verbinding met de medewerkers.
89.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Hoe is de verdeling tussen de werkplekken in Arnhem en Zoetermeer?	De verdeling werkplekken op de verschillende locaties is als volgt: Op de (hoofd)locatie Arnhem zijn 210 werkplekken, Zoetermeer Zilverstraat heeft er 60 en de locatie Chroomstraat kent een tiental werkplekken (dit is voornamelijk een logistieke locatie en kent daardoor minder werkplekken).
90.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	De aantallen meldingen worden opgegeven in synergy registraties, maar wordt ook gesproken over een koppeling met Jira Servicedesk en de tool van opdrachtnemer. Hoe verhoudt Jira zicht tot de synergy?	Zie het antwoord op vraag 61.
91.	3.4.1 Opdracht (scope) omschrijving punt	Er zijn situaties denkbaar dat in opdracht van een derde partij werkzaamheden op locatie uitgevoerd moeten	Dit valt onder projectwerk.

	1 Werkplekbeheer en eindgebruikersondersteuning	worden, bijvoorbeeld het vervangen van hardware op locatie. Is dit projectwerk of zit dit in de dienstverlening?	
92.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Wat is de verwachtte responsen of aanrijtijd bij verwachte aanwezigheid op locatie in geval van incidenten? En in welke gevallen is dit nodig?	Er is geen eis voor vaste aanwezigheid (bijv. elke maandag). De inzet is op afroep bij incidenten die niet remote oplosbaar zijn of bij geplande projectactiviteiten. Voor reguliere kleine hardwarehandelingen kan in overleg gebruik worden gemaakt van de aanwezige NIPV-servicedeskmedewerkers. De exacte afspraken hierover worden vastgelegd in de service-uren binnen het Dossier Afspraken en Procedures (DAP)
93.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Er wordt bij m365 beheer gesproken over SIAM, welke rol speelt de servicedesk van opdrachtnemer hierin?	De servicedesk heeft ook een coördinerende rol richting teams binnen het NIPV en ook richting andere dienstverleners zoals genoemd in de aanbesteding.
94.	Programma van eisen 03 Service & Support SRV-006 en SRV-024:	Wordt de servicedesk van opdrachtnemer geacht te werken in de tooling van opdrachtgever? Mocht dat niet zo zijn, wie logt dat de tickets in Jira?	Zie SRV-006 en SRV-024 van het PVE.
95.	Programma van eisen 03 Service & Support SRV-006 en SRV-024:	Wie beheert/is verantwoordelijk voor de koppeling tussen de ITSM systemen?	De Opdrachtnemer

96.	Programma van eisen 03 Service & Support SRV-006 en SRV-024:	Wordt geacht dat opdrachtnemer de het portaal aan laat sluiten op het ITSM systeem van opdrachtnemer?	Ja, als de Opdrachtnemer wenst in hun eigen portaal te werken. De Opdrachtnemer mag ook kiezen om te werken vanuit het portaal van de Opdrachtgever.
97.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Kan er een applicatielijst gedeeld worden?	Dit wordt gedaan in de volgende fase van deze aanbesteding.
98.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Kan er inzicht gegeven worden in het update proces van applicaties incl verantwoordelijkheden?	Alle devices worden beheerd met Intune en via het bedrijfsportaal worden applicaties aangeboden aan de medewerkers. Er wordt gebruik gemaakt van de applicatie genaamd Scappman voor het updaten van applicaties om dit proces te versnellen/automatiseren.
99.	3.4.1 Opdracht (scope) omschrijving punt 6. Beveiliging van de IT-omgeving	Er staat dat de Opdrachtnemer verantwoordelijk is voor het monitoren, oppakken en afhandelen van alle meldingen in de Microsoft 365 en Azure beheer centra. Voor het oplossen van de meldingen is soms een change nodig, zijn die inclusief?	Ja, dat is inclusief. Changes zijn onderdeel van het beheer van de Microsoft 365 en Azure omgeving. Daarbij gaan we ervan uit dat de dienstverlener een baseline voor zijn klanten heeft waardoor de configuratie up-to-date wordt gehouden op basis van de laatste richtlijnen.
100.	3.4.1 Opdracht (scope) omschrijving punt 6. Beveiliging van de IT-omgeving	Wordt met de meldingen Microsoft 365 en Azure beheer centra ook de defender portalen bedoeld? En hoe verhoudt zich dit tot SOC/SIEM dienstverlening?	Ja, hier worden ook de defender portalen mee bedoeld. De SOC dienstverlening richt zich op cybersecurity incidenten, terwijl de defender portalen ook meldingen weergeven over dagelijkse operationele activiteiten die moeten worden opgevolgd. Daarnaast faciliteert het SOC niet in de opvolging, alleen monitoring en detectie.

101.	3.4.1 Opdracht (scope) omschrijving punt 2. Microsoft 365-beheer	Hoe loopt nu het proces voor aanmaken, wijzigen en verwijderen van accounts, inclusief externen en stagiairs?	Gegevens worden opgevoerd in de bronsystemen, vanuit daar landt de informatie in Exact Synergy. Vanuit Exact Synergy worden er scripts gestart die ervoor zorgt dat accounts worden aangemaakt. Bij wijzigingen en/of verwijderen van accounts ligt de basis van de mutatie in de bronsystemen. Er wordt op dit moment geen gebruik gemaakt van tooling, dit is wel de wens van NIPV om dat in de toekomst te gaan doen.
102.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Het ziet de opdrachtgever de verantwoordelijkheid bij het up to date houden van business applicaties?	Standaard applicaties worden up-to-date gehouden door de Opdrachtnemer. Bij grote updates of wijzigingen die impact hebben is daarover vooraf overleg met het NIPV Regie team. Patch my PC is geïmplementeerd om het updaten van business applicaties grotendeels te vereenvoudigen/automatiseren. Business Applicaties worden door up to date gehouden door het functioneel beheer team van het NIPV.
103.	3.4.1 Opdracht (scope) omschrijving punt 1 Werkplekbeheer en eindgebruikersondersteuning	Welke acties wil NIPV eindgebruikers zelf laten uitvoeren (accounts, groepen, licenties, gasten, incidentmeldingen)?	Eindgebruikers kunnen zelf het initiatief nemen voor aanvragen zoals accounts, groepen, licenties, gasttoegang en incidentmeldingen. Voor alle aanvragen die betrekking hebben op rechten of licenties blijft leidinggevende accordering vereist voordat de actie wordt uitgevoerd. Op dit moment worden veel van deze aanvragen door gebruikers zelf ingediend via Synergy; in de toekomst kan dit proces eenvoudiger en/of gebruiksvriendelijker worden ingericht via modernere tooling met meer automatiseringsmogelijkheden. Het uitgangspunt is dat het initiatief bij de eindgebruiker ligt, terwijl het uitvoeren van de actie afhankelijk is van vooraf vastgestelde afspraken over: • welke aanvragen direct uitgevoerd mogen worden, • welke eerst door een leidinggevende moeten worden goedgekeurd, en • in welke gevallen een aanvraag mag worden afgewezen.

			De opdrachtnemer ondersteunt dit proces technisch en procedureel binnen de dienstverlening voor werkplekbeheer en eindgebruikersondersteuning.
104.	Budget	Indien de Aanbestedende Dienst van mening is dat de volledige scope en alle verplichte en indicatieve eisen zoals opgenomen in paragraaf 3.4 en het Programma van Eisen binnen het geraamde prijs- en contractkader realiseerbaar zijn, verzoeken wij de Aanbestedende Dienst concreet aan te geven: a) welke onderdelen van de dienstverlening in de transitie- en initiële uitvoeringsfase als kritisch (must-have) worden aangemerkt; b) welke onderdelen in een latere fase mogen worden gerealiseerd zonder dat dit leidt tot non-compliance met het Programma van Eisen; en c) of bepaalde indicatieve eisen expliciet als optioneel of conditioneel mogen worden beschouwd in de gunnings- en uitvoeringsfase. Deze toelichting is voor Gegadigden noodzakelijk om realistisch, kwalitatief hoogwaardige en conform budget van de opdracht te kunnen ontwerpen.	Het NIPV wijst er volledigheidshalve op dat voor de daadwerkelijke invulling ook input van de Opdrachtnemer nodig is. De volgende transitieactiviteiten moet de Opdrachtnemer — in abstracto — uitvoeren om tot een bedrijfsvaardige oplevering te komen. Kritiek (Must-have bij start, en zo snel als mogelijk na de start van het contract): • Continuïteit Werkplekondersteuning: de dagelijkse ondersteuning voor de circa 500 gebruikers moet vanaf de eerste dag van de operationele overdracht geborgd zijn • 24/7 Security Respons: de bereikbaarheid en het handelingsvermogen voor P1-incidenten en beveiligingsdreigingen zijn direct bij start noodzakelijk. • SPOC-functionaliteit: de centrale ingang voor meldingen en de triage daarvan moet volledig functioneren om "finger-pointing" in de keten te voorkomen. Latere realisatie (binnen de eerste contractfase): • Uitfasering On-premise Servers: de gefaseerde afbouw van de resterende servers in Arnhem naar de gewenste "n-state" kan gedurende de looptijd in 2026/2027 worden uitgevoerd. • Automatisering IDU-proces: hoewel het proces moet werken, mag de verdere optimalisatie en automatisering van het Instroom-, Doorstroom-, en Uitstroomproces als een verbeteractiviteit na de initiële transitie worden gerealiseerd. Zie aanvullend het antwoord bij vraag 74.

105.	Paragraaf 3.4.1 Scope	Waar zit voor u het verschil tussen het uitvoeren van proactieve monitoring, het opvolgen van beveiligingsincidenten en de werkzaamheden die vanuit het SOC van de externe leverancier geleverd worden? Kunt u de verschillen toelichten?	Zie het antwoord op vraag 58.
106.	Paragraaf 3.5 Buiten scope	U stelt op pagina 19 dat 24/7 monitoring en incidentrespons buiten scope valt. Echter op pagina 16 moet inschrijver ook proactief monitoren en beveiligingsincidenten opvolgen. Waar zit het verschil tussen de dienstverlening die u in deze aanbesteding uitvraagt en die de externe SOC-leverancier van aanbestedende dienst op dit moment levert? Daarnaast stelt u in Bijlage 10, tabblad Diensten, dat Opdrachtnemer wél 24x7 bereikbaar moet zijn voor het NIPV en de SOC-dienstverlener als er een P1 beveiligingsincident voordoet. Kunt u verduidelijken hoe dit zit en wat uw wensen zijn op dit gebied? Dient de opdrachtnemer een 24/7 eyes-on-screen dienstverlening te hebben voor het monitoren, of is een standby-dienstverlening afdoende?	Zie de antwoorden op vraag 25 en vraag 58.
107.	Paragraaf 3.5 Buiten scope	Valt het functioneel beheer van M365 binnen- of buiten scope? Het wordt niet als binnen scope genoemd. Het kopje ‘Maatwerksoftwareontwikkeling’, tenzij het gaat om standaardconfiguraties binnen Microsoft 365, Azure of andere platformen die onderdeel zijn van de scope, doet echter anders vermoeden. We verzoeken u dit toe te lichten.	Functioneel beheer van bedrijfsspecifieke applicaties en procesinrichting blijft de verantwoordelijkheid van het functioneel beheer team van het NIPV. De dienstverlener zal vanuit zijn rol wel ondersteuning, strategische sessies en adviezen geven aan het NIPV.
108.	Paragraaf 3.4.1 Scope	Ten aanzien van het netwerk is de opdrachtnemer met name gericht op de uitvoering van on-site werkzaamheden. Een andere dienstverlener levert primair de bewaking van deze netwerkcomponenten. Mag de dienstverlener verwachten dat:	Correct.

		• Met name instructief gewerkt wordt (op basis van info vanuit de andere dienstverlener). • Geen monitoring ingeregeld hoeft te worden t.a.v. de bewaking van de infrastructuur. Input tot het uitvoeren van werkzaamheden geïnitieerd wordt vanuit de andere dienstverlener?	
109.	Bijlage 10	In bijlage 10 vraagt u op regel 13 van het tabblad 01 Diensten 24x7 bemenste dienstverlening bij calamiteiten buiten kantoortijden. Is onze aanname juist dat dit betekent dat opdrachtnemer altijd (24x7) een team stand-by moet hebben staan in het geval van calamiteiten? Zo niet, kunt u dan toelichten wat u hier bedoelt?	Ja, dit is correct. Zie ook het antwoord op vraag 25.
110.	Bijlage 10	Op regel 30 tabblad 01 Diensten stelt u dat opdrachtnemer een leidende rol neemt in het geval van security alerts/events. Is het niet logischer om dit bij de SOC partij te beleggen, aangezien zij 24x7 monitoring doen? Kunt u toelichten hoe u dit ziet?	Zie het antwoord op vraag 58.
111.	Selectiedocument Kantoorautomatisering – 3.7 – pag 20	Kunt u aangeven op welk moment en op welke wijze de gunningscriteria van de gunningsfase (inclusief weging en beoordelingsmethodiek) beschikbaar worden gesteld, zodat voor zowel Aanbestedende Dienst als geselecteerde inschrijvers vooraf duidelijk is waarop het onderscheid zal worden gemaakt en wordt voorkomen dat inschrijvers na selectie alsnog besluiten geen inschrijving te doen omdat de gunningscriteria niet volledig matchen bij de scope van haar dienstverlening?	Zie de planning in paragraaf 4.5 van het Selectiedocument. De gunningscriteria worden op dit moment opgesteld en zullen worden opgenomen in het Beschrijvend Document. Dit zal op 24 april (volgens de nieuwe planning) worden gedeeld via TenderNed aan geselecteerde partijen.
112.	Selectiedocument Kantoorautomatisering – 4.10 – pag 32	In paragraaf 4.10, stap 5 van het Selectiedocument staat dat bij gelijke scores een loting plaatsvindt. Bij vergelijkbare procedures is het gebruikelijk om, vóór loting, een nadere differentiatie aan te brengen door eerst opeenvolgend te beoordelen op één van de selectiecriteria (bijvoorbeeld S1),	Omdat de selectiecriteria gelijk zijn verdeeld (elk 20 punten) heeft Aanbestedende dienst niet één selectiecriterium welke het belangrijkste is qua weging. Aanbestedende dienst heeft daarom gekozen deze werkwijze niet op te nemen.

		vervolgens op het volgende criterium (S2) en daarna op S3, zodat loting pas plaatsvindt als ook deze rangorde volledig gelijk blijft. Kunt u aangeven, gezien het aantal potentieel geïnteresseerden, hoe u tegenover deze werkwijze staat en of u bereid bent te overwegen om deze aanvullende differentiatiestappen toe te passen vóórdat wordt overgegaan tot loting?	
113.	Selectiedocument Kantoorautomatisering – 4.10 – pag 32	Kunt u toelichten hoe de beoordelingscommissie is samengesteld, waaronder het aantal leden en (indien mogelijk) de functieprofielen?	Het beoordelingsteam voor de selectiefase bestaat uit minimaal 5 beoordelaars van verschillende disciplines in de functie van materiedeskundigen.
114.	Selectiedocument Kantoorautomatisering – 4.11 – pag 33	Kunt u bevestigen dat digitaal ondertekenen wordt geaccepteerd als rechtsgeldige ondertekening, mits de ondertekening bevoegdheid blijkt uit het KvK-uittreksel?	Dat is correct.
115.	Selectiedocument Kantoorautomatisering – 4.11. – pag 33	Kunt u bevestigen dat Inschrijver enkel de UEA, Bijlage 06 Formulier referentieopdracht en Bijlage 11 Conformiteitenverklaring rechtsgeldig dient te ondertekenen?	Dat is correct, en tevens indien van toepassing Bijlage 3 Verklaring Samenwerkingsverband, Bijlage 4 Verklaring Onderaanneming en Bijlage 5 Verklaring middelen derde. Zie Bijlage 1 Checklist inschrijving v2 (Bijlage 11 Conformiteitenverklaring is toegevoegd aan de kolom ‘bij Aanmelding indienen’.)
116.	Selectiedocument, §3.4.1 punt 1 Werkplekbeheer en eindgebruikersondersteuning, p.11	Kan de opdrachtgever bevestigen dat on-site inzet door de opdrachtnemer uitsluitend plaatsvindt op verzoek van of in afstemming met de NIPV-regieorganisatie?	Dit is correct.
117.	Selectiedocument, §3.4.1 punt 2	Er wordt aangegeven dat de opdrachtnemer “volledig verantwoordelijk” is voor het technisch beheer van	Dat klopt en is een juiste omschrijving.

	Microsoft 365-beheer, p.13	Microsoft 365, terwijl beleid, governance, admin-rollen en compliance onder de regie van NIPV blijven. Kunt u bevestigen dat met “volledig” bedoeld wordt: volledige operationele uitvoering binnen door NIPV vastgestelde kaders?	
118.	Selectiedocument, §3.4.1 punt 2 Microsoft 365-beheer, p.13	Heeft NIPV op dit moment drift configuration tools in gebruik zoals Inforcer/Simeon Cloud?	Nee, NIPV heeft geen drift configuration tools in gebruik.
119.	Selectiedocument, §3.4.1 punt 2 Microsoft 365-beheer, p.13	Heeft NIPV specifieke eisen met betrekking tot de security en compliancy baselines?	Op het gebied van informatiebeveiliging conformeert NIPV zich aan ISO 27001, BIO 2.0 en de Cyberbeveiligingswet (=NIS2) en de AVG. Daarin is de hoogst gestelde eis steeds leidend.
120.	Selectiedocument, §3.4.1 punt 3 Microsoft Azure-beheer, p.14	Vallen Azure-native netwerkcomponenten zoals Azure Firewall, VNET-peering of Private Endpoints binnen of buiten de scope van de opdracht?	Binnen scope van de opdracht.
121.	Selectiedocument, §3.4.6 punt Beveiliging van de IT-omgeving, p.16	In hoeverre mag Inschrijver configuratiewijzigingen voorstellen of doorvoeren in de back-up- of securityconfiguratie wanneer deze bijdragen aan security of performance? Zijn hiervoor voorafgaande goedkeuringen vereist?	Dit mag na overleg, en goedkeuring, door de NIPV regie organisatie.
122.	Bijlage 10, SEC-094	Wil NIPV deze training afstemmen op het intern gebruik van AI systemen?	Het gaat er in deze eis om dat als opdrachtnemer AI inzet als onderdeel van hun dienstverlening, dat personeel van de opdrachtnemer dan voldoende is opgeleid om veilig met AI te werken. Het NIPV verzorgt zelf de trainingen voor haar eigen personeel.

123.	Bijlage 10, SEC-094	Welke AI systemen heeft NIPV op dit moment in gebruik?	Binnen de scope van deze opdracht is het gebruik van AI op dit moment zeer beperkt. Binnen de scope beperken de gebruikers zich tot verantwoord gebruik van enkele LLM's.
124.	3.4.1 Werkplekbeheer, p. 11–13	Kunt u aangeven of NIPV een bestaande uniforme werkplekstandaard hanteert of dat de leverancier deze moet definiëren?	Hiervoor is een standaard die in de volgende fase van de aanbesteding wordt toegelicht.
125.	3.4.1 Serverbeheer, p. 15	Kunt u inzicht geven in de omvang, rollen en configuratie van de resterende on-prem serveromgeving?	Zie het antwoord op vraag 4.
126.	3.4.1 Serverbeheer, p. 15	Zijn er geplande migraties of uitfaseringsprojecten waarmee de leverancier rekening moet houden?	Zie het antwoord op vraag 4.
127.	3.4.1 Back-up en herstel, p. 16	Gebruikt NIPV uitsluitend Rubrik of zijn er aanvullende storage-oplossingen binnen scope?	NIPV streeft ernaar om uitsluitend Rubrik te gebruiken. NIPV beschikt over een grote hoeveelheid cloud storage en nog een deel on prem storage voorziening (welke steeds minder nodig is). Naast Rubrik is de standaard Microsoft Cloud back-up voorziening actief
128.	3.4.1Beveiliging ITomgeving, p. 16	Welk deel van security monitoring wordt door de SOC-partner uitgevoerd en welk deel door de leverancier?	Zie antwoord op vraag 58
129.	3.13 Informatiebeveiliging, p. 23–24	Hanteert NIPV een vaste securitybaseline (BIO2.0 / NIS2 / M365 Secure Score) die leidend is voor configuratie en compliance?	Op het gebied van informatiebeveilging conformeert NIPV zich aan ISO 27001, BIO 2.0 en de Cyberbeveiligingswet (=NIS2) en de AVG. Daarin is de hoogst gestelde eis steeds leidend.
130.	3.4.1 Service Management, p. 17	Werkt NIPV met vaste SLA/KPI/XLA formats of mogen leveranciers eigen formats aanbieden?	De leverancier mag eigen formats aanleveren voor het monitoren en rapporteren van SLA/KPI/XLA.

131.	3.4.1 Service Management, p. 17	Wat is de gewenste overlegstructuur (operationeel, tactisch, strategisch) en frequentie?	Wanneer de Aanbestedende dienst hier eisen of wensen over heeft, zal dit worden opgenomen in de gunningsfase.
132.	Selectiedocument Kantoorautomatisering, Paragraaf 4.7, pagina 29	Kunt u bevestigen of Gegadigden in een eventuele tweede Nota van Inlichtingen nieuwe vragen mogen indienen?	Ja, dat is akkoord.
133.	Selectiedocument Kantoorautomatisering, Paragraaf 7.4, pagina 47	Kan de Aanbestedende Dienst bevestigen dat een referentie die is uitgevoerd binnen een cloudomgeving die qua architectuur en dienstverlening vergelijkbaar is met Azure, eveneens wordt geaccepteerd, mits deze voldoet aan de inhoudelijke scope van de opdracht?	De Aanbestedende Dienst bevestigt dat een referentie uitgevoerd in een andere cloudomgeving (zoals AWS of Google Cloud) wordt geaccepteerd voor het voldoen aan Geschiktheidseis 5 (Referenties). De Gegadigde moet dan wel gemotiveerd onderbouwen dat en waarom de omgeving vergelijkbaar is qua inhoudelijke scope en technische complexiteit (zoals beschreven in paragraaf 3.4.1) aantoonbaar gelijkwaardig is aan de gevraagde dienstverlening. Aanbestedende Dienst wijst Gegadigden erop dat Geschiktheidseis 4 (Microsoft Solutions Partner Designation) een zelfstandige, verplichte ongewijzigd van kracht blijft. Dit betekent dat een Gegadigde op het moment van Aanmelding — ongeacht de cloudomgeving van de ingediende referentie — op straffe van terzijdelegging moet beschikken over minimaal één geldige Microsoft Solutions Partners Designations (Modern Work, Security of Azure Infrastructure) om de technische bekwaamheid voor de specifieke NIPV-omgeving aan te tonen.