

Bijlage 2 - Programma van eisen

Aanvullend begrip

Melding:

(Storings-) meldingen, wijzigingsverzoeken, restoreverzoeken, gebruikersverzoeken en informatievragen, klachten, incidenten.

Service desk Leverancier:

Dit is de 1e-lijns servicedesk van Leverancier waar meldingen over het netwerkbeheer binnen komen. Deze servicedesk ontvangt via de interne servicedesk van Opdrachtgever, Regiefunctie ICT of de servicedesk Outsourcing ICT meldingen.

Service desk opdrachtgever:

Opdrachtgever heeft een interne servicedesk ingericht. Deze servicedesk ontvangt alle meldingen van eindgebruikers van opdrachtgever en zal deze op basis van de scope van de dienstverlening de melding (warm) doorzetten aan de verantwoordelijke leverancier.

Service desk Outsourcing ICT:

Opdrachtgever heeft bij een externe partij (Nexxt) een 1e-lijns servicedesk belegd waar meldingen over de werkplek en de Azure omgeving binnenkomen. Deze helpdesk is de primaire helpdesk voor ICT gerelateerde zaken en meldingen. Deze servicedesk ontvangt via de interne servicedesk van opdrachtgever meldingen van eindgebruikers.

Regiefunctie ICT:

De ICT adviseurs van Opdrachtgever zijn verantwoordelijk voor de coördinatie en beleid op het gebied van ICT. Dit betreft wijzingen in de ICT-omgeving, bepalen van richtlijnen en beleid op ICT-gebied.

Nr	Algemene eisen
1.	Leverancier levert alle gevraagde diensten zoals beschreven in hoofdstuk 1.1 offerteaanvraag.
2.	Leverancier en zijn dienstverlening dienen in opzet, bestaan en werking, te voldoen aan hoofdstuk 1 van de Baseline Informatiebeveiliging Overheid (BIO2) en toont dat jaarlijks aan, middels onafhankelijke onderzoeken conform eis 60.
3.	Leverancier levert een adequaat beveiligde dienstverlening, waarbij de informatiebeveiliging zodanig ingericht is, zodat opdrachtgever hiermee aan alle huidige en toekomstige relevante wet- en regelgeving (zoals BIO2, NIS2, nieuwe cyberbeveiligingswet etc.) voldoet en blijft voldoen.
4.	De eisen gelden ook voor eventuele onderaannemers in de toeleveringsketen die door Leverancier worden ingezet.
5.	Leverancier geeft inzicht in de keten van toeleveranciers en eventuele risico's daarin.
6.	Gedurende de looptijd van de overeenkomst geeft Leverancier veranderingen in de keten van toeleveranciers door, inclusief risico's. Dit omvat minimaal kwetsbaarheden, en informatiebeveiligingsincidenten die de dienstverlening kunnen raken.
Service desk	
7.	Meldingen aan de servicedesk van Leverancier kunnen op drie verschillende wijzen worden ingediend: 1. Vanuit de servicedesk van opdrachtgever;

	2. Vanuit de Regiefunctie ICT van opdrachtgever; 3. Vanuit de servicedesk Outsourcing ICT. Na binnenkomst van een melding vindt in het kader van efficiënte communicatie en afhandeling van de melding afstemming plaats tussen de eindgebruiker van opdrachtgever en de servicedesk van Leverancier.
8.	Om (proactief) regie te voeren op de meldingen, heeft opdrachtgever via een portaal van leverancier inzicht in de voortgang, status en afhandeling van alle meldingen. De derde leverancier, heeft inzicht in alleen de meldingen die via deze leverancier zijn gemeld.
9.	De Service Desk van Leverancier is een skilled Service Desk, die het eerste contactpunt is voor vragen, (wijzigings-) verzoeken en meldingen voor alle diensten die in scope zijn van deze opdracht. De servicedesk van Leverancier voldoet aan de volgende eisen: a) Nederlandstalige skilled Service Desk; b) Single point of contact; c) Alle meldingen dienen geregistreerd en ter afhandeling gerouteerd te worden. Ook dient de voortgang van de afhandeling van de meldingen bewaakt en teruggekoppeld te worden; d) De Service Desk van Leverancier behandelt (storings-) meldingen, wijzigingsverzoeken en informatievragen met betrekking tot de door Leverancier geleverde dienstverlening; e) Leverancier heeft indien nodig overleg met de Leverancier die de Outsourcing van de ICT verzorgt. Dit betekent afstemming over het registeren, doorzetten en bewaken van verzoeken zoals benoemd onder d; f) De servicedesk is via telefoon en e-mail bereikbaar voor vragen en meldingen; g) Meldingen kunnen middels een selfservice portaal van Leverancier door worden gegeven en is via Single Sign On (SSO) te benaderen en bereikbaar; h) Meldingen worden voorzien van een nummer die teruggekoppeld wordt per email aan de gebruiker.
10.	Naast meldingen van gebruikers, worden ook geautomatiseerde meldingen door bijvoorbeeld Aruba Central, vanuit monitoringssystemen en statusmeldingen door de Servicedesk van Leverancier geregistreerd en afgehandeld.
11.	De service desk van Leverancier lost meldingen zoveel mogelijk direct of na het eerste contactmoment op.
12.	Indien de melding niet direct kan worden opgelost, wordt deze doorgezet naar ondersteunende lijnen van Leverancier.
13.	Leverancier is verantwoordelijk voor het functioneren, beheer en herstel van het netwerk. Indien hardware vervanging noodzakelijk is, wordt deze uitgevoerd onder het hardware contract met de hardware leverancier van Afeer. Leverancier coördineert dit proces, maar de verplichting tot levering/vervanging van hardware ligt bij de hardware leverancier. Leverancier blijft verantwoordelijk voor het volledig herstellen van de netwerkdienst na vervanging. Dit omvat de installatie, configuratie, integratie, testen en oplevering van de vervangende hardware. Dit geldt ook voor eventuele toekomstige uitbreidingen van het netwerk.
14.	De servicedesk van Leverancier is bereikbaar via telefoon en e-mail van maandag tot en met vrijdag van 7:00 uur tot 18:00 uur.
15.	Indien een melding niet direct kan worden opgelost is de maximale reactietijd 3 werkdagen.
16.	De servicedesk van Leverancier is, voor het melden van urgente en kritische incidenten (ernstige verstoring, hack etc.) 24 uur per dag, 7 dagen per week, inclusief feestdagen, telefonisch en per e-mail bereikbaar. Leverancier start direct na de melding met passende herstelwerkzaamheden en zet, indien nodig, escalatieprocedures en/of een workaround in.
Service levels	
17.	Leverancier hanteert voor incidentmanagement minimaal de volgende niveaus van dienstverlening.

	Prio 1 Kritisch incident: Reactietijd <30 minuten, Oplostijd <4 uur. Opdrachtgever verstaat onder een kritiek incident het niet beschikbaar zijn van functionaliteit wat effect heeft op de gehele organisatie of een groot deel hiervan (b.v. één van de twee hoofdlocaties). Het niet kunnen beschikken over deze functionaliteit heeft direct substantiële gevolgen voor de financiële positie van de opdrachtgever of haar medewerkers, het kunnen voldoen aan wet- en regelgeving (b.v. informatiebeveiliging), de te leveren kwaliteit (zoals productieverstoring) door de opdrachtgever en/of de klanttevredenheid van één of meer klanten van de opdrachtgever. De overige niveaus voor incidentmanagement maken onderdeel uit van de gunningscriteria.
18.	Leverancier levert een technische root cause analyse (RCA) voor incidenten die binnen de scope van deze overeenkomst vallen.
19.	Bij incidenten die Aruba Central raken, start Leverancier direct met triage, ongeacht of die in Azure of bij Aruba zelf ligt. Bij conflicten of storingen die vermoedelijk in Azure zitten, levert Leverancier technisch onderbouwde analyses aan ter ondersteuning van triage.
20.	Leverancier blijft eigenaar van het incident zolang dit betrekking heeft op Aruba Central of de netwerkcomponenten, zelfs in het geval er sprake is van afhankelijkheid van derden.
21.	Voor Changes (wijzigingsverzoeken) gelden de volgende doorlooptijden: • Standaard changes: < binnen twee (2) werkdagen; • Niet standaard changes: Binnen twee (2) werkdagen analyse van de impact en doorlooptijd; • Emergency changes: Direct handelen na vaststelling van urgentie door beide partijen.
22.	Voor Standaard, Niet standaard en Emergency changes geldt dat hiervoor een request for change en nadere offerte wordt opgesteld. De offerte is gebaseerd op de uurtarieven in het prijzenblad en wordt P&Q afgerekend.
23.	Firmware-upgrades worden alleen uitgevoerd binnen changevensters die zijn afgestemd met de partij die de Azure omgeving beheert.
Netwerk beheer	
24.	Leverancier onderhoudt de beveiligingsmaatregelen die beschermen tegen ongeautoriseerde toegang, malware, DDoS-aanvallen en overige cyberdreigingen. Dit omvat minimaal: toegangscontrole op beheersinterfaces, minimale rechten, logging, monitoring van security-events en detectie van verdachte activiteiten.
25.	Leverancier werkt binnen de door de derde partij (Outsourcing ICT) beheerde Azure-omgeving uitsluitend via door die partij verstrekte beheeraccounts of API-toegang.
26.	Leverancier is verantwoordelijk voor beheer en configuratie van alle Aruba Central componenten binnen zijn scope, maar niet voor het Azure-platform zelf
27.	Leverancier rapporteert incidenten die afhankelijk zijn van de derde partij direct en registreert die als extern afhankelijk.
28.	Gedurende de looptijd van de overeenkomst dienen de filterfuncties van gateways en firewalls ten alle tijden zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.
29.	Leverancier voert geen wijzigingen door op Azure-componenten (resource groups, policies, networking) zonder schriftelijke toestemming van opdrachtgever. Leverancier stemt wijzigingen altijd vooraf af met de partij die de Azure omgeving beheert (change procedures worden op elkaar afgestemd).
30.	Configuraties van Aruba Central moeten compatibel zijn met de Azure-netwerkarchitectuur (bijv. IP-adressering, subnetting, routing) en voldoen aan de BIO2 richtlijn voor: • Identiteit en toegang; • Logging & monitoring;

	• Configuratiebeheer; • Patchbeheer; • Continuïteit; • Netwerksegmentatie.
31.	Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.
32.	Het netwerk van opdrachtgever en alle Aruba Central componenten worden door Leverancier 24 uur per dag, 7 dagen per week gemonitord op afwijkend gedrag (defect, kwetsbaarheid, externe bedreiging, certificaten, security alerts etc.). Indien er sprake is van afwijkend gedrag neemt Leverancier direct passende en/of mitigerende maatregelen om potentiële informatiebeveiligingsincidenten op te lossen, volgens de afgesproken incident- en escalatieprocedures. De logbestanden worden geregistreerd en bewaard.
33.	Leverancier bewaakt 24 uur per dag, 7 dagen per week de status, beschikbaarheid, performance en capaciteitsbelasting van alle netwerkcomponenten en Aruba Central componenten. Afwijkingen van vooraf vastgestelde drempelwaarden worden automatisch gedetecteerd en gelogd.
34.	Leverancier heeft toereikende logging en monitoring ingericht, om detectie, vastlegging en onderzoek van gebeurtenissen mogelijk te maken, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.
35.	Leverancier onderhoudt alle netwerkcomponenten door beveiligings-, software- en firmware-updates, security patches tijdig te installeren conform de richtlijnen van de fabrikant. Kritieke (security)updates worden zo snel mogelijk, geïnstalleerd, tenzij anders met opdrachtgever overeengekomen. Tevens controleert Leverancier op Aruba Central en Azure compatibiliteit na updates.
36.	Leverancier voert planmatig preventief onderhoud uit om storingen te voorkomen. Onderhoud omvat minimaal: controle van hardwarecomponenten, logreview, analyse van trends in performance/capaciteit en controle van redundantievoorzieningen.
37.	Leverancier zorgt voor dagelijkse back-ups van configuraties, met een minimale retentie van 30 kalenderdagen. Leverancier heeft een herstelplan die minimaal 1x per jaar wordt getest.
38.	Leverancier is verantwoordelijk voor het signaleren van aflopende supportcontracten en te adviseren en ondersteunen bij het verlengen van de contracten dan wel advies te geven om de hardware te vervangen. Leverancier meldt termijnen en expiraties minimaal 3 maanden vooraf aan opdrachtgever.
39.	Leverancier voert minimaal eenmaal per kwartaal een security health check uit op de netwerkarchitectuur, rollen & rechten, certificaatstatus, configuraties en beveiligingsinstellingen. Bevindingen, risico's en adviezen worden schriftelijk gerapporteerd aan opdrachtgever.
Implementatie en beheer overeenkomst	
40.	Leverancier levert na gunning een implementatieplan die voldoet aan de criteria van artikel 6.3 van de GIBIT-voorwaarden.
41.	Bij inschrijving levert Leverancier zijn concept SLA aan. De minimale uitgangspunten waaraan de SLA moet voldoen is opgenomen in bijlage 11 en voorwaarden zoals opgenomen in het PVE. De definitieve inhoud van de SLA wordt na gunning in overleg met opdrachtgever afgestemd.
42.	Bij inschrijving worden de volgende documenten door Leverancier opgeleverd: • Concept Dossier Afspraken en Procedures (DAP); • Concept Producten diensten catalogus (PDC). De definitieve inhoud van deze documenten wordt na gunning in overleg met opdrachtgever afgestemd.
43.	De implementatie van de ICT-prestatie is uiterlijk 25 juni 2026 afgerond. Op deze datum is de ICT-prestatie door opdrachtgever geaccepteerd en kan de ICT-prestatie per 1 juli 2026 in gebruik worden genomen.

44.	Jaarlijks vindt er tussen opdrachtgever en Leverancier een evaluatie over de geleverde dienstverlening plaats. Tijdens het overleg komen o.a. de volgende onderwerpen aan de orde: • Tevredenheid van opdrachtgever en gebruikerservaring; • Evaluatie contractuele afspraken; • Managementrapportages en toelichting; • Klachtenregistratie en behandeling; • Kwaliteit van de geleverde dienstverlening. Leverancier zorgt dat deze gesprekken worden ingepland.
45.	Leverancier zorgt voor één aanspreekpunt voor opdrachtgever in de rol van een Service manager. Deze Service manager is het vaste contactpersoon voor opdrachtgever en draagt zorg voor het up-to-date houden van de dienstverlening, rapporteren over de geleverde prestaties en bewaakt de kwaliteit van de dienstverlening
46.	Als de overeenkomst eindigt wordt van Leverancier verwacht, dat deze bereidwillig en kosteloos meewerkt aan de overdracht van kennis en ervaring en transitie naar een andere externe partij. Leverancier verleent op eerste verzoek van Opdrachtgever tijdige en volledige medewerking aan het overleggen van relevante rapportages en (management)informatie, die opdrachtgever in het kader van de overdracht aan een externe partij en/of voorbereiding van een aanbestedingsprocedure nodig acht.
47.	Uiterlijk 1 maand voor beëindiging van de overeenkomst draagt Leverancier de volgende elementen aan de opdrachtgever over: • De volledig actuele CMDB; • Alle relevante documentatie, configuratiebestanden, architectuur documentatie en back-ups; • Lijst van gebruikte rollen, rechten en API keys; • Aruba Central tenants, keys. Daarnaast verzorgt Leverancier een overdrachtsrapportage met overzicht van lopende incidenten, wijzigingen en afhankelijkheden.
48.	Leverancier zorgt dat Aruba Central volledig overdraagbaar is ingericht. Dit betekent dat de tenant overdraagbaar, configuraties zijn te documenteren, er geen vendor-lock in is op accounts of scripts.
49.	Leverancier zorgt voor configuratiebeheer en houdt een actuele en complete CMDB bij van alle beheerde componenten in het netwerk, waaronder hardware, software, netwerkcomponenten en licenties
50.	Elke wijziging in configuraties, versies en afhankelijkheden wordt onmiddellijk geregistreerd in de CMDB, zodat de CMDB altijd actueel is.
51.	De CMDB is op verzoek van opdrachtgever te allen tijde raadpleegbaar en exporteerbaar.
52.	Leverancier documenteert duidelijk welke onderdelen onder zijn verantwoordelijkheid vallen en welke onder een derde partij vallen.
53.	Leverancier houdt actuele documentatie bij van: • Netwerkdigrammen/Connectieschema's (inclusief IP-adressen, VLAN's to Azure mapping, verbindingen en beveiligingszones); • Routingoverzicht en afhankelijkken (bijv. VPN's, firewall flows) richting Azure; • Configuratiebestanden en systeeminstellingen; • Wijzigingshistorie (inclusief datum, omschrijving en verantwoordelijke); • Gebruikte softwareversies en patchniveaus.
54.	De documentatie in eis 52 moet op elk moment volledig, actueel en controleerbaar zijn en wordt op verzoek van opdrachtgever beschikbaar gesteld in een gangbaar digitaal formaat (bijv. PDF, Visio, Excel)

Rapportages en advies	
55.	Leverancier levert periodieke (kwartaal) rapportages aan opdrachtgever omtrent het gebruik van de ondersteuning en afhandeling van meldingen en de dienstverlening. Leverancier denkt proactief mee om mogelijke structurele incidenten te signaleren en in overleg met opdrachtgever oplossingen te bespreken.
56.	Leverancier levert per kwartaal een schriftelijke compliancy-rapportage aan over de veilige inrichting en het beheer van de netwerkdiensten. Deze rapportage voldoet minimaal aan de volgende eisen: • Toetsing van de feitelijke situatie aan het geldende beveiligingsbeleid van opdrachtgever. • De rapportage bevat een beoordeling van de configuraties en beveiligingsinstellingen van alle netwerkcomponenten (firewalls, routers, switches, gateways). • Een overzicht van incidenten, kwetsbaarheden en afwijkingen van het beveiligingsbeleid. • De rapportage bevat een risico-analyse en concrete aanbevelingen inclusief een actieoverzicht.
57.	Leverancier bespreekt de rapportages in een kwartaaloverleg met opdrachtgever en legt de opvolging van bevindingen vast
58.	Leverancier adviseert de opdrachtgever minimaal eenmaal per jaar proactief over lifecycle management, end-of-life, end-of-support-data, benodigde upgrades en capaciteitsbehoeften. Dit betreft onder andere: • Aruba central configuraties. • Acces points. • Switches. • Gateways.
Informatiebeveiliging & Data	
59.	De data die wordt verwerkt in de ICT-prestatie en in het bijzonder in Aruba Central, zoals configuraties, logs, rapportages) blijven altijd eigendom van opdrachtgever.
60.	Leverancier verleent zekerheid ('assurance') over de kwaliteit van de dienstverlening aan opdrachtgever, bij voorkeur door middel van het jaarlijks aanleveren van een ISAE3402 type II rapportage, ISAE3000 of een SOC2 type II verklaring, waarin de scope is bepaald door de ICT-prestatie die opdrachtgever afneemt. Indien Leverancier niet beschikt over een ISAE3402, ISAE3000 of SOC2 rapportage zal Leverancier de dienstverlening aan opdrachtgever jaarlijks laten auditen door een onafhankelijke auditor en hierover aan opdrachtgever rapporteren. De kosten van de genoemde assurance verklaringen zijn voor rekening van Leverancier.
61.	De effectiviteit van de richtlijnen voor de netwerkbeveiliging kunnen door opdrachtgever, eventueel in samenwerking met een derde partij, periodiek getoetst en geëvalueerd. Leverancier verleent hieraan de benodigde medewerking.
62.	Na gunning wordt er met Leverancier een verwerkersovereenkomst (bijlage 7) afgesloten die integraal onderdeel uitmaakt van de hoofdovereenkomst. Leverancier gaat bij inschrijving akkoord met de inhoud van deze concept verwerkersovereenkomst.
63.	Leverancier rapporteert transparant over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Zowel bij Leverancier als in de toeleveringsketen.
64.	Toegang tot Aruba Central gebeurt uitsluitend via MFA en rolgebaseerde toegang (RBAC).
65.	Leverancier gebruikt strikt gescheiden beheer accounts, met minimaal: • View-only voor rapportages; • Admin voor changebeheer.
66.	Toegang wordt door Leverancier vastgelegd in een Access Control Matrix, die minimaal 1x per jaar wordt beoordeeld.

67.	Alle beheeractiviteiten op Aruba Central moeten worden gelogd, inclusief: • Gebruiker; • Tijdstip; • Wijziging; • Voor/na configuratie.
68.	Logging uit Aruba Central moet geëxporteerd kunnen worden.
69.	Auditlogs moeten minimaal 90 dagen beschikbaar blijven.
70.	Indien API's van Aruba Central gebruikt worden, moeten tokenbeheer en lifecycle management dusdanig zijn ingericht dat de security risico's vanuit de OWASP API Security Top 10 worden gemitigeerd.
Facturatie & Administratie	
71.	Leverancier stuurt maandelijks een factuur voor de geleverde diensten. Facturen dienen te worden gemaïld naar Opdrachtgever.
72.	Op de factuur wordt minimaal de volgende informatie vermeldt: • Naam en adres van de leverancier; • Naam en adres opdrachtgever; • Het btw-nummer van de leverancier; • Het KvK-nummer van de leverancier; • Datum van de factuur; • Een uniek factuurnummer; • Een gespecificeerde omschrijving van diensten, producten of projecten die zijn geleverd; • Het aantal geleverde diensten; • De datum waarop de diensten zijn geleverd, of de datum van een vooruitbetaling; • Bedragen, exclusief btw; • Het geldende btw-tarief; • Het btw-bedrag.
73.	De omschrijving van diensten, producten, projecten zijn dusdanig op de factuur vermeldt dat deze te allen tijde te herleiden zijn naar de in de overeenkomst overeengekomen diensten en prijzen.
74.	De door Leverancier opgegeven prijzen dekken alle in deze uitvraag opgenomen eisen en door inschrijver aangeboden invullingen van de gunningcriteria volledig. Dit betekent dat alle kosten (beheer en ontwikkeling van de producten, diensten-systemen, personele kosten, reiskosten, afleveringskosten, overhead, accountantsverklaring e.d.) in de door Leverancier aangeboden prijzen zijn verwerkt. Facturatie van extra kosten is dus niet mogelijk, tenzij door Opdrachtgever expliciet anders aangegeven.
75.	Aanvullende of variabele kosten zijn alleen te factureren indien deze vooraf zijn afgestemd en schriftelijk goedgekeurd door opdrachtgever.
76.	Het is mogelijk om de dienstverlening op- en af te schalen middels P&Q conform de vereisten zoals vermeldt in het prijzenblad. Verder is het mogelijk dat gedurende de looptijd van de overeenkomst het mogelijk is om aanvullende opdrachten waaraan behoefte is en die nauw verband houden met de scope van deze opdracht aan Leverancier te verstrekken. Deze aanvullende opdrachten hebben uitsluitend betrekking op: • De uitbreiding van het aantal systemen/componenten binnen de bestaande dienstverlening; • Aanverwante beheer- en supportdiensten binnen de bestaande technische en functionele scope; • Doorontwikkeling of optimalisatie van reeds geleverde ICT-diensten.

	De omvang van de aanvullende opdrachten is beperkt tot 20% van de totale maximale geraamde opdrachtwaarde.
77.	In afwijking van de GIBIT-voorwaarden kunnen de tarieven jaarlijks per 1 januari, maar voor het eerst per 1 januari 2028, door Leverancier worden aangepast, mits deze aanpassing minimaal één maand voorafgaand is aangekondigd. Een stijging is gelimiteerd tot maximaal de (eventuele) stijging van het op het moment van aankondiging laatst door het Centraal Bureau voor de Statistiek (CBS) gepubliceerde definitieve prijsindexcijfer dienstenprijzen commerciële dienstverlening en transport (index 2021=100), of de opvolger daarvan, voor groep J62, althans J6202, over het gehele jaar in vergelijking met het prijsindexcijfer van het kwartaal van inschrijving van diezelfde index. Als voorbeeld: het indexcijfer in het kwartaal van inschrijving Q1 2026 is 105. Het jaar dat geïndexeerd gaat worden is 2028. Het indexcijfer van Q1 2027 is 108. De formule is als volgt: $108/105 \times 100\% = 2,85\%$. De prijzen mogen worden geïndexeerd met 2,85%. Leverancier heeft ingeschreven met een prijs van €1000,-. De nieuwe prijs wordt dan € 1028,50. In het jaar 2030 is de index Q1 2029 112. De formule is als volgt $112/105 \times 100\% = 6,67\%$. De nieuwe prijs voor 2030 wordt €1000,- + €66,70 = €1066,70.