BIJLAGE 6

SCOPE DOCUMENT MSP

Nictiz

Betere gezondheid
door betere informatie

Bijlage: scope ICT managed services

Versie 1.0 – maandag 8 december 2025

Inhoudsopgave

1. Hardware provisioning

Definitie

Dit bevat het leveren van laptops voor de werkplek. De Opdrachtnemer zorgt voor de beschikbaarheid, registratie en lifecycle van de hardware, zodat Nictiz altijd kan beschikken over passende en up-to-date voorzieningen.

De levering en het beheer van overige werkplekapparatuur (telefoons, beeldschermen, toetsenborden, muizen en headsets) worden momenteel door een derde partij gerealiseerd. Als optie kan de levering van deze hardware worden overgenomen door de nieuwe opdrachtnemer.

Wat doet Nictiz zelf

De werkplek beheerders van Nictiz verzorgen de uitgifte en inname van alle werkplek apparatuur. Zij bieden eveneens de eerste lijn ondersteuning richting medewerkers.

Alle overige diensten rond hardware provisioning worden uitgevoerd door de opdrachtnemer.

Gevraagde dienst

De Opdrachtnemer zorgt ervoor dat alle hardware geconfigureerd en gebruiksklaar wordt aangeleverd aan Nictiz en na afschrijving weer wordt ingenomen, waarbij een professionele dataverwijdering wordt uitgevoerd. Nictiz ontvangt een certificaat van de dataverwijdering als ‘proof of compliance’. Nictiz streeft naar hergebruik van de hardware door maatschappelijke organisaties.

Nieuwe client devices, zoals laptops, worden door de Opdrachtnemer geregistreerd voor zero-touch deployment (Windows Autopilot). Dit betekent dat het apparaat direct door de Nictiz servicedesk kan worden uitgegeven aan de medewerker en na het inloggen automatisch wordt voorzien van de juiste configuraties, applicaties en beveiligingsinstellingen.

De opdrachtnemer biedt tweede en derde lijn support rond de hardware voor de werkplekbeheerders van Nictiz.

De Opdrachtnemer geeft proactief advies over welke hardware het beste aansluit op de dienstverlening en rapporteert jaarlijks over verbruik, vervangingen en lifecycleplanning.

2. Werkplek beheer

Definitie

Betreft de diensten die noodzakelijk zijn voor het ontwerpen en leveren van de eindgebruiker IT-werkplek. Hieronder vallen onder andere: softwaredistributie, packaging, virusmanagement, client design en deployment en IMAC/D.

Wat doet Nictiz zelf

De werkplekbeheerders van Nictiz verzorgen de eerstelijns ondersteuning van medewerkers. Zij hebben toegang (leesrechten) tot de diverse beheeromgevingen, zoals de telefonie omgeving, de Apple Business omgeving en Samsung Knox.

Alle overige werkzaamheden in het werkplekbeheer (inclusief tweede- en derdelijns support) worden uitgevoerd door de Opdrachtnemer.

Gevraagde dienst

De Opdrachtnemer levert, beheert en ondersteunt de cloudwerkplek. De werkplek stelt medewerkers in staat veilig en plaats onafhankelijk te werken met toegang tot bestanden en applicaties. De Opdrachtnemer verzorgt het volledige beheer, de beveiliging en de continue doorontwikkeling van deze werkplek inclusief benodigde licenties.

De hybride werkplek wordt geleverd vanuit de cloud, met zero- of light-touch provisioning zoals Windows Autopilot of een gelijkwaardige oplossing. De Opdrachtnemer beheert de configuraties en policies van endpoints, voert lifecyclemanagement uit en verzorgt distributie en packaging van applicaties. Besturingssystemen en applicaties worden tijdig geüpdatet en gepatcht volgens de overeengekomen patchpolicy.

Samenwerken vindt plaats binnen de Microsoft 365 omgeving, waarbij ook externen (mensen zonder een Nictiz account) veilig kunnen deelnemen (Zoals bijvoorbeeld Microsoft Sharepoint Online). Tweede en derdelijns support wordt geleverd conform SLA en DAP. Nictiz verzorgt zelf de eerstelijns ondersteuning voor de medewerkers.

Adoptie wordt ondersteund met trainingen, instructies en periodieke verbetervoorstellen op basis van gebruiksdata.

Beveiliging wordt ingericht volgens het principe van security-by-design, met centraal remote beheer, certificaatbeheer, multi-factor authenticatie, encryptie van data, next-gen endpointbeveiliging (EDR/XDR) en beleidshandhaving via conditional access en compliance. De omgeving is beschermd tegen ransomware en overige dreigingen.

Continuïteit wordt geborgd met back-up en herstel van Microsoft 365-data (of gelijkwaardig), inclusief: bewaartermijnen, point-in-time restore en hersteltests. Voor grootschalige incidenten zijn noodprocedures beschikbaar.

De prestaties van de werkplek zijn gericht op een uitstekende gebruikerservaring, met snelle inlogtijden, stabiele performance en minimale verstoringen.

3. Servicedesk en support

Definitie

De servicedesk en support is erop gericht de medewerkers van Nictiz optimaal te ondersteunen bij het gebruik van de diverse ICT middelen. De ondersteuning is beschikbaar tijdens kantoor uren (van 09:00 tot 17:30 uur).

Wat doet Nictiz zelf

De rol van service desk wordt bij Nictiz uitgevoerd door de beheerders van Team IM. Deze eerstelijns ondersteuning betreft de call intake, registratie, routering en afmelding van meldingen in Topdesk (1e lijn), het bieden van ondersteuning (op locatie en op afstand) en het beantwoorden van gebruikersvragen.

De beheerders van Nictiz kunnen met hun vragen terecht bij de tweede lijn support van Opdrachtnemer.

Gevraagde dienst

De tweede lijn support van Opdrachtnemer is het Single Point of Contact (SPOC) voor de servicedesk van Nictiz omtrent alle afgenomen diensten in deze aanbesteding. Dit omvat de intake, registratie, routering en afhandeling van service requests, incidenten en problems.

De tweede lijn van Opdrachtnemer kan zoveel mogelijk zelfstandig oplossen en verzorgt de verdere communicatie en afstemming met de 3e lijn van Opdrachtnemer, volgens overeengekomen SLA's/DAP's. Er wordt daarbij gewerkt met een service managementsysteem.

De Opdrachtnemer rapporteert maandelijks over de kwaliteit van dienstverlening volgens de afgesproken KPI's, SLA's en DAP's. Elk kwartaal worden de resultaten besproken tussen Opdrachtnemer en Nictiz.

In geval van calamiteiten waarbij Nictiz tijdelijk niet zelf in staat is de servicedesk te bemensen (bijvoorbeeld door ongeval, ziekte of anderszins uitval van personeel) moet het mogelijk zijn dat Opdrachtnemer de eerste lijn serivcedesk tijdelijk overneemt.

4. Beheer Microsoft 365 en Azure

Definitie

Betreft het technisch beheer van Microsoft 365 en Azure. Het beheer omvat het oplossen van incidenten en verstoringen, het monitoren van de prestaties en beschikbaarheid van de applicaties, het doorvoeren van standaardwijzigingen, het uitvoeren van bugfixes.

Wat doet Nictiz zelf

De Microsoft 365 beheerder van Nictiz verzorgt de eerstelijns ondersteuning rond de Microsoft 365 omgeving. De beheerder voert zelfstandig standaard wijzigingen uit en kan kleine problemen oplossen. Daartoe heeft hij de volgende rechten in de Microsoft 365 omgeving:

- Intune beheerder
- Exchange admin
- Authenticatie admin
- Groups admin
- Teams admin
- SharePoint admin
- Helpdesk admin
- Global reader
- Yammer admin
- Device admin

Gevraagde dienst

De Opdrachtnemer levert het beheer en tweedelijns/derdelijns ondersteuning voor Microsoft 365 (o.a. Exchange Online, Teams, OneDrive en SharePoint Online), waarbij wordt gezorgd voor stabiele werking, optimale configuratie en veilige toegang.

De Opdrachtnemer denkt proactief mee over verbetering, toepassing en adoptie van deze diensten. De Opdrachtnemer ondersteunt gebruikersadoptie met trainingen, handleidingen en inspiratiesessies.

5. Netwerk beheer

Definitie

Dit betreft de voorzieningen die nodig zijn om het netwerk beschikbaar, veilig en schaalbaar te houden. Dit domein omvat WAN, LAN en internetverbindingen, aangevuld met firewall- en DMZ-functionaliteit voor gecontroleerde toegang. Ook netwerkzonering, monitoring en carrier management maken standaard deel uit van deze dienstverlening, zodat dataverkeer betrouwbaar wordt afgehandeld en beveiligingsrisico's tot een minimum worden beperkt.

Wat doet Nictiz zelf

Het beheer van alle netwerk componenten is geheel belegd bij de Opdrachtnemer.

De 1e lijn ondersteuning is belegd bij de servicedesk van Nictiz. Ter ondersteuning van die rol is toegang tot de netwerkomgeving (raadplegen) wenselijk.

Gevraagde dienst

De Opdrachtnemer levert en beheert het volledige Office (W)LAN-netwerk, inclusief access points, switches, routers en firewallvoorzieningen. Het netwerk voldoet aan actuele veiligheidsnormen, wordt preventief onderhouden en voorzien van tijdige updates en patchmanagement. Bij stroomuitval wordt de apparatuur gecontroleerd afgesloten via een getest noodmechanisme. De coreswitch levert een gesegmenteerd en betrouwbaar netwerk, terwijl firewallvoorzieningen ongeautoriseerde toegang blokkeren. De Opdrachtnemer borgt de schaalbaarheid, veiligheid en continuïteit van het netwerk. Daarnaast rapporteert de Opdrachtnemer periodiek over prestaties en beveiliging.

6. Beveiliging en continuïteit

Definitie

Deze diensten zijn erop gericht om de werkplek en digitale samenwerkingsomgeving van Nictiz veilig en beschikbaar te houden. De dienstverlening rond veiligheid en continuïteit is van toepassing op alle onderdelen van deze aanbesteding.

Wat doet Nictiz zelf

Nictiz heeft de regie, geeft de kaders aan en bewaakt architectuur en compliance op het gebied van beveiliging en continuïteit. Daarnaast werkt Nictiz aan veilig gedrag door medewerkers, met onder meer bewustwordingscampagnes.

Gevraagde dienst

De Opdrachtnemer levert operationeel beheer, monitoring en rapportage rond beveiliging en continuïteit, evenals gevraagd en ongevraagd advies op dit terrein.

De Opdrachtnemer hanteert een security-by-design-benadering bij de inrichting van alle werkplekken, cloud-omgevingen en infrastructuren. Dit betekent:

- Integratie van multi-factor authenticatie (MFA), conditional access, en encryptie van data (in rust en tijdens transport).
- Toepassing van Zero Trust-architectuur en Identity & Access Management (IAM), inclusief periodieke review van toegangsrechten.
- Naleving van NEN 7510, ISO/IEC 27001 en AVG richtlijnen.

De Opdrachtnemer verzorgt 24/7 beveiligingsmonitoring, proactieve detectie van kwetsbaarheden via vulnerability scanning, patchmanagement en periodieke PEN-tests.

Er zijn duidelijke afspraken over incidentrespons, root cause analysis (RCA) en rapportage van beveiligingsincidenten binnen vastgestelde responstijden.

Beveiliging van Microsoft 365, Azure en hybride omgevingen verloopt via next-gen endpointbeveiliging (EDR/XDR) en Data Loss Prevention (DLP).

Beveiliging van het netwerk verloopt middels netwerksegmentatie, firewallbeheer en DMZ-structuren voor gecontroleerde toegang.

De Opdrachtnemer voert regelmatige audits uit en levert nalevingsrapportages over beveiligingsmaatregelen.

Voor het borgen van de beschikbaarheid (continuïteit) verzorgt de Opdrachtnemer dienstverlening rond back-up en herstel, disaster recovery en capaciteits- en performance management.

Nadere invulling van de vereisten op het terrein van beveiliging en continuïteit volgt in de volgende fase van de aanbesteding.

7. Licentie beheer

Definitie

Het systematisch beheren van de hardware en software licenties in de context van de werkplek en de Microsoft 365 samenwerkingsomgeving, gedurende hun hele levenscyclus van aanschaf tot verwijdering. Het doel is optimaal gebruik, kostenbeheersing en risicoreductie.

Wat doet Nictiz zelf

Werkplekbeheerders van Nictiz hebben een rol in het toekennen van licenties aan medewerkers en daarmee ook een rol in beheer van de CMDB database.

Gevraagde dienst

Registreren, controleren en beheren van softwarelicenties van Nictiz in de context van de werkplek en de M365 omgeving. Het doel is te zorgen dat alle gebruikte software legaal is, dat er niet te veel of te weinig licenties zijn aangeschaft, en dat de organisatie voldoet aan de licentievoorwaarden van leveranciers.

8. Hosting overige applicaties

Definitie

Naast de genoemde werkplek en M365 omgeving beschikt Nictiz over een aantal bedrijfsspecifieke applicaties en websites, die deels gehost worden op de Azure omgeving. Het gaat om software die gebruikt wordt bij de ontwikkeling en het beheer van informatie standaarden en enkele websites voor publicatie van informatiestandaarden en aanverwante content.

Wat doet Nictiz zelf

Nictiz voert het functioneel beheer op deze applicaties zelf uit. Het technisch applicatiebeheer is belegd bij een derde partij, welke hiervoor toegang heeft tot de betreffende onderdelen van de Azure omgeving van Nictiz.

Gevraagde dienst

Opdrachtnemer geeft toegang aan derde partij voor het applicatiebeheer aan de applicaties die gehost worden op de Azure omgeving van Nictiz.

De door Opdrachtnemer verzorgde 24/7 beveiligingsmonitoring en proactieve detectie van kwetsbaarheden (zie hierboven) geldt ook voor deze applicaties.

9. Overige Scope

9.1 Transitie

Definitie

De transitie betreft de projectmatige overgang van de huidige ICT-dienstverlener naar de Opdrachtnemer. Met als doelstelling een soepele en gecontroleerde overgang, waarbij continuïteit wordt gewaarborgd, risico's worden geminimaliseerd en de impact op medewerkers en organisatie tot een minimum wordt beperkt.

De Opdrachtnemer is eindverantwoordelijk voor de voorbereiding, coördinatie en uitvoering van alle transitieactiviteiten. Dit gebeurt in nauwe samenwerking met Nictiz en de huidige leverancier(s), op basis van het transitieplan dat als onderdeel van de gunning is ingediend. De transitie wordt afgerond met een gezamenlijke acceptatie, waarna de reguliere beheerfase formeel start.

Gevraagde dienst

De Opdrachtnemer voert de feitelijke transitie uit op basis van het goedgekeurde transitieplan. Deze dienstverlening omvat ten minste:

1) Inventarisatie en overdracht: in kaart brengen en overnemen van alle relevante contracten, systemen, documentatie, accounts en afhankelijkheden.

2) Technische migratie: gecontroleerde overdracht van infrastructuur, werkplekken, applicaties, data en koppelingen, inclusief validatie en testmomenten.

3) Communicatie en adoptie: informeren en begeleiden van gebruikers en stakeholders over de wijzigingen en planning, inclusief trainingen waar nodig.

4) Continuïteit en risicobeheersing: toepassen van mitigerende maatregelen om de beschikbaarheid en beveiliging van diensten tijdens de transitie te waarborgen.

5) Rapportage en voortgang: periodiek rapporteren aan Nictiz over status, risico's, issues en behaalde mijlpalen.

De Opdrachtnemer borgt dat de transitie efficiënt, veilig en transparant verloopt, met minimale impact op de bedrijfsvoering van Nictiz.

9.2 Levering van kennis, kunde, ervaring en expertise

Definitie

Dit betreft de tijdelijke inzet van expertise ter ondersteuning van Nictiz. Het gaat om IT-experts die op uurbasis of projectbasis worden ingezet voor specifieke vraagstukken of advies welke buiten de Scope van de vaste, Managed Services, vergoeding vallen.

Gevraagde dienst

De Opdrachtnemer stelt op verzoek van Nictiz gekwalificeerde IT-experts beschikbaar voor de uitvoering van werkzaamheden die buiten de vaste dienstverlening vallen maar wel gerelateerd zijn aan de Scope van de aanbesteding. De procedure is daarbij (volgordelijk):

1) Nictiz dient een aanvraag in met een omschrijving van de gewenste werkzaamheden of het te behalen resultaat.

2) De Opdrachtnemer reageert hierop met een beknopte offerte of plan van aanpak dan wel het voorstellen van een kandidaat IT-expert middels een cv. de offerte c.q. het plan van aanpak bevat minimaal een duidelijke inschatting van de benodigde uren, de beoogde resultaten (deliverables), een globale planning en de profielen van de in te zetten experts.

3) De werkzaamheden starten uitsluitend na expliciete schriftelijke goedkeuring van Nictiz.

Nictiz heeft geen afnameverplichting voor de inhuur van IT-expertise. Deze dienstverlening dient uitsluitend om de flexibiliteit te bieden wanneer de behoefte zich voordoet.

9.3 Exit-plan

Definitie

Het exit-plan betreft de georganiseerde afbouw en overdracht van de dienstverlening aan het einde van de contractperiode of bij voortijdige beëindiging. Het doel van het exit-plan is het waarborgen van de continuïteit van de bedrijfsvoering van Nictiz door een gecontroleerde, veilige en volledige overdracht van alle relevante diensten, data, configuraties, licenties, documentatie en verantwoordelijkheden naar een nieuwe leverancier of terug naar Nictiz. Het plan voorziet in heldere procedures, afspraken en tijdslijnen die vendor lock-in voorkomen en zorgen voor een soepele overgang met minimale impact voor eindgebruikers.

Gevraagde dienst

De Opdrachtnemer stelt binnen zes maanden na de start van het contract een exit-plan op, dat jaarlijks wordt geactualiseerd en afgestemd met Nictiz. Dit plan bevat minimaal:

1) een inventarisatie van alle diensten, systemen, configuraties en documentatie die binnen de Scope vallen;

2) procedures voor overdracht van kennis, documentatie, configuraties, licenties en data;

3) afspraken over de wijze waarop data veilig en volledig wordt overgedragen in open en gangbare formaten, zonder vendor lock-in;

4) een plan voor de afbouw of beëindiging van infrastructuurcomponenten en accounts;

5) afspraken over medewerking van personeel, zoals kennisoverdracht en begeleiding van de nieuwe leverancier;

6) een tijdslijn met activiteiten, verantwoordelijkheden en communicatiemomenten.

Tijdens de exit-fase werkt de Opdrachtnemer constructief samen met Nictiz en de nieuwe leverancier, waarbij continuïteit van de dienstverlening voor de eindgebruikers prioriteit heeft. De Opdrachtnemer levert voortgangsrapportages en neemt deel aan coördinatie-overleggen totdat de overdracht formeel is afgerond en door Nictiz is geaccepteerd. Werk in het kader van de exit wordt verrekend op basis van nacalculatie.