VAN OOSTEN ADVIES B.V.

Dienstverleningsovereenkomst IT-beheer

Inclusief Service Level Agreement, dienstbeschrijving, prijzen, beveiligingsbaseline, noodtoegang en exit-regeling

Document	Gegevens
Versie	Versie 1.0 (2026)
Documentcode	VOA-DVO-1.0-2026
Status	Geldig vanaf 1 oktober 2026; vaste template voor alle IT-beheerklanten, aangegaan door ondertekening van het Opdrachtformulier
Datum	1 oktober 2026
Eigenaar	Van Oosten Advies B.V., KvK 42077708, btw NL869603504B01
Adres	Wilgestraat 40, 4431 CH ’s-Gravenpolder, Nederland

Dienstverleningsovereenkomst IT-beheer

Partijen en totstandkoming

Deze Dienstverleningsovereenkomst (hierna: de **Overeenkomst**) wordt gesloten tussen **Van Oosten Advies B.V.**, gevestigd aan de Wilgestraat 40, 4431 CH 's-Gravenpolder, KvK 42077708 (hierna: **Opdrachtnemer**), en de onderneming die in het Opdrachtformulier IT-beheer als opdrachtgever is vermeld (hierna: **Opdrachtgever**), samen: **Partijen**.

De Overeenkomst komt tot stand door ondertekening van het Opdrachtformulier door beide Partijen. Het Opdrachtformulier bevat alle klantspecifieke gegevens en keuzes: partijgegevens, pakket, aantal Gebruikers en Apparaten, ingangsdatum, prijzen, Microsoft-abonnementen, contactpersonen, noodcontacten, activeringsdata, bewaartermijnen en afwijkende afspraken. Deze template wordt niet per klant aangepast.

Overwegingen

a) Opdrachtnemer levert IT-beheerdiensten aan ondernemingen zonder eigen IT-afdeling, met een vaste prijs per maand en vooraf vastgelegde reactietijden.

b) Opdrachtgever wenst het beheer, de ondersteuning en de beveiliging van zijn Microsoft 365-omgeving en werkplekken aan Opdrachtnemer uit te besteden.

c) Partijen leggen hun afspraken vast in deze Overeenkomst met bijlagen en in het Opdrachtformulier.

Artikel 1. Definities en documenten

1.1 Begrippen met een hoofdletter hebben de betekenis die daaraan is gegeven in de Algemene Voorwaarden van Opdrachtnemer, versie 1.0 (2026), hierna: de **Algemene Voorwaarden**, tenzij hieronder anders gedefinieerd.

1.2 De volgende documenten maken deel uit van de Overeenkomst:

- Het Opdrachtformulier IT-beheer, versie 1.0 (2026), met de klantspecifieke keuzes (hierna: het **Opdrachtformulier**)
- Bijlage 1: Dienstbeschrijving en pakketten
- Bijlage 2: Service Level Agreement (SLA)
- Bijlage 3: Prijzen en tarieven
- Bijlage 4: Beveiligingsbaseline, noodtoegang, toegang van Opdrachtnemer en afspraken voor de toeleveringsketen
- Bijlage 5: Exit-regeling
- De Algemene Voorwaarden, versie 1.0 (2026)
- De Verwerkersovereenkomst, versie 1.0 (2026)
- De Microsoft 365-licentiebijlage (CSP), versie 1.0 (2026), voor zover Opdrachtgever Microsoft-abonnementen via Opdrachtnemer afneemt

1.3 Bij strijd tussen documenten geldt de rangorde van artikel 2.4 van de Algemene Voorwaarden. Het Opdrachtformulier gaat voor op deze Overeenkomst en de

bijlagen voor zover het klantspecifieke keuzes bevat; een afwijking van een bepaling van deze Overeenkomst geldt alleen als het Opdrachtformulier die bepaling noemt.

1.4 **Gebruiker**: iedere unieke natuurlijke persoon voor wie Opdrachtnemer op grond van de Overeenkomst een werkplek of account beheert, ongeacht het aantal aan die persoon toegewezen licenties of Apparaten. Gedeelde mailboxen, technische serviceaccounts en gastaccounts tellen niet mee, tenzij in het Opdrachtformulier anders is overeengekomen. **Apparaat**: een laptop, desktop of ander eindapparaat dat in de goedgekeurde inventarisatie van Bijlage 1 is opgenomen en waarop de beheersoftware van Opdrachtnemer is geïnstalleerd; per Gebruiker zijn maximaal twee (2) Apparaten inbegrepen, tenzij het Opdrachtformulier anders vermeldt. **Omgeving**: de Microsoft 365-tenant van Opdrachtgever (aangeduid met de tenant-ID in het Opdrachtformulier) met de daarin opgenomen gebruikers, gegevens, instellingen en de daaraan gekoppelde Apparaten. **Contactpersoon**: een in het Opdrachtformulier aangewezen persoon met de daar vermelde bevoegdheid (bestellen, wijzigingen goedkeuren, privacy, noodcontact).

Artikel 2. Onderwerp

2.1 Opdrachtnemer levert aan Opdrachtgever de Beheerde Diensten volgens het in het Opdrachtformulier gekozen pakket, zoals omschreven in Bijlage 1, met de serviceniveaus van Bijlage 2 en tegen de vergoeding van Bijlage 3 en het Opdrachtformulier.

2.2 Opdrachtnemer levert daarnaast, als Opdrachtgever daarvoor in het Opdrachtformulier kiest, Microsoft 365-abonnementen en andere Producten. Daarop is de Microsoft 365-licentiebijlage van toepassing.

2.3 Alle Beheerde Diensten worden geleverd op basis van een inspanningsverplichting, met dien verstande dat Opdrachtnemer de in Bijlage 1 en Bijlage 4 concreet omschreven maatregelen, controles en handelingen uitvoert en dat aantoonbaar vastlegt (artikel 4.1 van de Algemene Voorwaarden). Opdrachtnemer garandeert geen ononderbroken beschikbaarheid van de Omgeving en niet dat beveiligingsincidenten uitblijven.

Artikel 3. Duur, proefperiode en opzegging

3.1 De Overeenkomst gaat in op de in het Opdrachtformulier vermelde ingangsdatum en wordt aangegaan voor een initiële termijn van twaalf (12) maanden. Ieder van Partijen kan de Overeenkomst schriftelijk opzeggen tegen het einde van de initiële termijn met een opzegtermijn van één (1) kalendermaand. Voorbeeld: bij een ingangsdatum van 1 november 2026 eindigt de initiële termijn op 31 oktober 2027; een opzegging die uiterlijk op 30 september 2027 is ontvangen, beëindigt de Overeenkomst per 31 oktober 2027.

3.2 Bij gebreke van opzegging tegen het einde van de initiële termijn wordt de Overeenkomst voortgezet voor onbepaalde tijd. Daarna kan ieder van Partijen de Overeenkomst schriftelijk opzeggen met een opzegtermijn van één (1) kalendermaand, tegen het einde van een kalendermaand. Voorbeeld: een opzegging ontvangen op 10 maart beëindigt de Overeenkomst per 30 april.

3.3 **Proefperiode.** Gedurende de eerste negentig (90) dagen na de ingangsdatum mag Opdrachtgever de Overeenkomst schriftelijk opzeggen met onmiddellijke ingang of tegen een door hem opgegeven datum binnen die termijn. Er is dan geen beëindigingsvergoeding verschuldigd. Wel verschuldigd blijven: (a) de vergoeding voor de Beheerde Diensten tot en met de opzegdatum, naar rato per dag; vooruitbetaalde vergoeding over de periode na de opzegdatum wordt binnen dertig (30) dagen terugbetaald; (b) de in het Opdrachtformulier overeengekomen opstartvergoeding; (c) de vergoeding voor Microsoft-abonnementen en andere Producten met een vaste looptijd die op verzoek van Opdrachtgever zijn besteld (Microsoft 365-licentiebijlage). Opdrachtnemer wijst Opdrachtgever in het Opdrachtformulier op de keuze tussen maand- en jaarabonnementen tijdens de proefperiode.

3.4 Opdrachtnemer informeert Opdrachtgever ten minste zestig (60) dagen vóór het einde van de initiële termijn schriftelijk over de voortzetting voor onbepaalde tijd en de opzegmogelijkheid.

3.5 Beëindiging van de Overeenkomst laat de looptijd en betalingsverplichting van Microsoft-abonnementen en andere Producten onverlet, behoudens overdracht aan een andere leverancier; daarvoor gelden de Microsoft 365-licentiebijlage en module D van de Algemene Voorwaarden. Bij het einde van de Overeenkomst worden vooruitbetaalde vergoedingen voor Beheerde Diensten over de periode na de einddatum terugbetaald of verrekend.

3.6 Voor ontbinding en beëindiging bij insolventie gelden de artikelen 15.2 en 15.3 van de Algemene Voorwaarden.

Artikel 4. Vergoeding, gebruikers en indexatie

4.1 Opdrachtgever betaalt de maandelijkse vergoeding voor de Beheerde Diensten volgens Bijlage 3 en het Opdrachtformulier, vermeerderd met de vergoeding voor de afgenomen Producten. De maandelijkse vergoeding wordt maandelijks vooraf gefactureerd; werkzaamheden buiten het pakket en Producten met verbruiksafhankelijke kosten worden maandelijks achteraf gefactureerd. Het Opdrachtformulier vermeldt de beheervergoeding per maand, de licentiekosten per gekozen periode en de eenmalige kosten afzonderlijk.

4.2 De maandelijkse vergoeding is gebaseerd op het aantal Gebruikers op de eerste dag van de kalendermaand en geldt voor diezelfde maand. In het Opdrachtformulier is gekozen voor óf de staffelprijs van Bijlage 3, onderdeel A, óf een prijs per Gebruiker (Bijlage 3, onderdeel C); beide gelden niet naast elkaar. Bij een staffelprijs geldt bij wisseling van staffel de nieuwe staffelprijs vanaf de eerstvolgende kalendermaand. Bij een prijs per Gebruiker is de vergoeding het aantal Gebruikers op de eerste dag van de maand maal de prijs per Gebruiker; rekenvoorbeeld: drie Gebruikers maal € 84,75 is € 254,25 per maand exclusief btw, uitsluitend voor de Beheerde Diensten. Artikel C.4 van de Algemene Voorwaarden regelt nul Gebruikers en overschrijding van de hoogste staffel.

4.3 Indexatie vindt plaats volgens artikel 7.2 van de Algemene Voorwaarden; andere prijswijzigingen volgens artikel 7.3 daarvan, met het daar beschreven opzegrecht. Prijswijzigingen van Microsoft en andere leveranciers worden doorberekend volgens de Microsoft 365-licentiebijlage.

4.4 Betaling vindt plaats per overboeking binnen veertien (14) dagen na factuurdatum.

Artikel 5. Verplichtingen van Opdrachtnemer en activering

5.1 Opdrachtnemer:

a) levert de Beheerde Diensten volgens Bijlage 1 en de SLA van Bijlage 2, met vakbekwaam personeel en met gebruik van professionele beheer- en beveiligingstooling;

b) richt de Omgeving in volgens de beveiligingsbaseline van Bijlage 4 en het activeringsplan van lid 2, in overleg met Opdrachtgever en na inventarisatie van afhankelijkheden;

c) documenteert de Omgeving (inventarisatie, configuratie, contactpersonen, procedures) en houdt die documentatie bij;

d) informeert Opdrachtgever over beveiligingsincidenten volgens artikel 8 en over storingen van leveranciers die de Omgeving raken;

e) rapporteert volgens het gekozen pakket (Bijlage 1);

f) houdt zich aan de Verwerkersovereenkomst en de geheimhoudingsverplichtingen van de Algemene Voorwaarden.

5.2 **Activering.** Opdrachtnemer legt per onderdeel van het pakket in een activeringsverslag vast op welke datum het is geactiveerd, welke controle is uitgevoerd en welke afhankelijkheden of tijdelijke risico's er zijn. Daarbij gelden de volgende termijnen, te rekenen vanaf de dag waarop Opdrachtgever de in artikel 6.1 onder b bedoelde toegang heeft verleend: (a) kritieke onderdelen (meervoudige verificatie, noodtoegang, back-up voor zover in het pakket, en de bewaking van accounts voor zover in het pakket) binnen tien (10) Werkdagen; (b) de overige onderdelen van de beveiligingsbaseline en het werkplekbeheer binnen negentig (90) dagen. Opdrachtgever ontvangt het activeringsverslag na afronding van (a) en na afronding van (b).

5.3 Als een kritiek onderdeel niet binnen de termijn van lid 2 onder (a) is geactiveerd, meldt Opdrachtnemer dat direct aan de Contactpersoon met de oorzaak, de tijdelijke risico's en de nieuwe datum; de overige rechten van Opdrachtgever blijven onverlet. Onderdelen waarvan het Opdrachtformulier een latere activeringsdatum vermeldt (bijvoorbeeld omdat een leverancier nog niet is gecontracteerd), gelden als geleverd vanaf die datum en worden tot die datum niet als actief gepresenteerd.

5.4 Opdrachtnemer maakt gebruik van de leveranciers en tooling die in Bijlage 4 en in de Verwerkersovereenkomst zijn genoemd. Opdrachtnemer mag deze vervangen door gelijkwaardige of betere oplossingen en informeert Opdrachtgever daarover vooraf via de procedure voor subverwerkers in de Verwerkersovereenkomst.

Artikel 6. Verplichtingen van Opdrachtgever

6.1 Opdrachtgever:

a) wijst in het Opdrachtformulier de Contactpersonen aan met hun bevoegdheden: wie meldingen mag doen, wie wijzigingen en bestellingen tot welk bedrag mag goedkeuren, wie het aanspreekpunt voor privacy en

incidenten is, en wie buiten Kantoortijden bereikbaar is voor spoedbeslissingen (noodcontact), telkens met een vervanger;

b) verleent Opdrachtnemer de toegang en machtigingen die voor het beheer nodig zijn, waaronder de goedkeuring van de beheerrelatie bij Microsoft (GDAP) en van de in Bijlage 4, onderdeel C vermelde app-machtigingen, en het toestaan van de installatie van beheersoftware op de Apparaten;

c) meldt in- en uitdiensttreding van medewerkers, wijzigingen in apparatuur en gewenste wijzigingen tijdig via de supportkanalen van Bijlage 2, voor reguliere mutaties uiterlijk twee (2) Werkdagen voor de gewenste ingangsdatum; voor spoedmutaties (zoals het direct blokkeren van een account) geldt de spoedroute van artikel 8.5;

d) zorgt dat zijn medewerkers de beveiligingsmaatregelen gebruiken (waaronder meervoudige verificatie) en de instructies van Opdrachtnemer opvolgen;

e) gebruikt uitsluitend apparatuur en software binnen de door de leverancier ondersteunde versies, of aanvaardt dat niet-ondersteunde onderdelen buiten de Beheerde Diensten vallen;

f) bewaart de bij oplevering ontvangen noodtoegang (Bijlage 4, onderdeel B) veilig en meldt Opdrachtnemer direct als die mogelijk is gecompromitteerd;

g) brengt zelf geen wijzigingen aan in de beveiligings- en beheerconfiguratie die door Opdrachtnemer wordt beheerd, en laat dat ook geen derden doen, zonder overleg met Opdrachtnemer;

h) informeert Opdrachtnemer schriftelijk als Opdrachtgever onder de Cyberbeveiligingswet, de Belgische NIS2-wet of andere sectorale beveiligingsverplichtingen valt of gaat vallen, zodat de ketenafspraken van Bijlage 4, onderdeel D, worden toegepast;

i) informeert Opdrachtnemer als in de Omgeving structureel bijzondere categorieën persoonsgegevens, strafrechtelijke gegevens of nationale identificatienummers worden verwerkt (Verwerkersovereenkomst, artikel 4.2).

6.2 Als Opdrachtgever een verplichting uit dit artikel niet nakomt, mag Opdrachtnemer, na Opdrachtgever daarop te hebben gewezen, de daardoor ontstane extra werkzaamheden tegen de uurtarieven van Bijlage 3 in rekening brengen en is Opdrachtnemer niet aansprakelijk voor schade die daarvan het gevolg is, met inachtneming van artikel 9.7 van de Algemene Voorwaarden.

Artikel 7. Wijzigingen

7.1 Wijzigingen in het pakket, het aantal Gebruikers of Apparaten of de overige klantspecifieke keuzes worden vastgelegd in een aanvulling op het Opdrachtformulier of per e-mail bevestigd door een bevoegde Contactpersoon en Opdrachtnemer. Een wijziging naar een hoger pakket gaat in op de eerste dag van de volgende kalendermaand. Een wijziging naar een lager pakket gaat in op de eerste dag van de kalendermaand na afloop van de initiële termijn of, daarna, na een aankondigingstermijn van één (1) kalendermaand.

7.2 Opdrachtnemer mag de inhoud van de Beheerde Diensten en de gebruikte tooling aanpassen aan technische ontwikkelingen en gewijzigde Derdenvoorwaarden, mits het overeengekomen serviceniveau en de overeengekomen dekking niet

verminderen. Andere wijzigingen kondigt Opdrachtnemer ten minste dertig (30) dagen vooraf aan; is de wijziging voor Opdrachtgever nadelig, dan mag Opdrachtgever de Overeenkomst opzeggen tegen de ingangsdatum van de wijziging (artikel 17.2 van de Algemene Voorwaarden).

Artikel 8. Beveiliging, incidenten, meldingen en spoedroute

8.1 Opdrachtnemer treft de maatregelen van Bijlage 4 en van de Verwerkersovereenkomst. Opdrachtgever blijft verantwoordelijk voor het beveiligingsbeleid van zijn organisatie, voor het gedrag van zijn medewerkers en voor beveiligingsmaatregelen die hij, na schriftelijk advies van Opdrachtnemer met vermelding van de risico's, niet heeft laten toepassen.

8.2 Opdrachtnemer meldt een beveiligingsincident dat de Omgeving raakt en dat Opdrachtnemer bekend wordt, zonder onredelijke vertraging en uiterlijk binnen vierentwintig (24) uur na ontdekking aan de Contactpersoon voor incidenten, met de op dat moment bekende feiten; bij een incident met mogelijk grote gevolgen volgt een eerste waarschuwing zo snel mogelijk, ook als de feiten nog onvolledig zijn. Aanvullende informatie volgt zodra beschikbaar. Een inbreuk in verband met persoonsgegevens wordt daarnaast gemeld volgens de Verwerkersovereenkomst. Buiten Kantoortijden vindt de melding plaats via e-mail en, bij een P1-incident, telefonisch aan het noodcontact.

8.3 **Bevoegdheden bij een incident.** Opdrachtnemer mag bij een acuut beveiligingsincident zonder voorafgaand overleg de maatregelen nemen die redelijkerwijs nodig en proportioneel zijn om schade te voorkomen of te beperken, waaronder het isoleren van Apparaten, het blokkeren van accounts en het intrekken van sessies en tokens. Maatregelen met onomkeerbaar effect (zoals het wissen van Apparaten of gegevens) en herstelwerkzaamheden die buiten het pakket vallen en meer dan vier (4) uur vergen, voert Opdrachtnemer alleen uit na akkoord van een bevoegde Contactpersoon of het noodcontact, tenzij een concreet omschreven noodsituatie (bijvoorbeeld actieve versleuteling door ransomware) dat onmogelijk maakt; Opdrachtnemer documenteert dan de noodzaak en meldt de maatregel direct.

8.4 **Herstel na een incident.** Inbegrepen in Compleet en Premium zijn: het beheersen van het incident (containment), het onderzoek naar de oorzaak binnen de mogelijkheden van de gebruikte tooling, het terugzetten van gegevens en configuraties uit de back-up en het opnieuw beveiligen van accounts en Apparaten. Niet inbegrepen, tenzij het incident aan Opdrachtnemer toerekenbaar is: forensisch onderzoek door een externe partij, het volledig opnieuw opbouwen van de Omgeving of van Apparaten na een aan Opdrachtgever of derden toerekenbare oorzaak, en ondersteuning bij aangifte, verzekeringsclaims en meldingen aan autoriteiten buiten de bijstand van de Verwerkersovereenkomst. Voor Essentieel is herstel na een incident meerwerk, met uitzondering van het opnieuw beveiligen van gecompromitteerde accounts.

8.5 **Spoedroute.** Voor het met spoed blokkeren van een account, het intrekken van sessies of het op afstand vergrendelen of wissen van een Apparaat (bijvoorbeeld bij ontslag op staande voet, verlies of diefstal) geldt: (a) een bevoegde Contactpersoon of het noodcontact meldt het verzoek telefonisch via het supportnummer, gevolgd

door een bevestiging per e-mail of portaal; (b) Opdrachtnemer verifieert de identiteit van de melder aan de hand van de in het Opdrachtformulier vastgelegde gegevens; (c) binnen Kantoortijden voert Opdrachtnemer de blokkering uit binnen één (1) uur na verificatie; buiten Kantoortijden geldt dit alleen voor Premium via de noodlijn, voor zover die volgens het Opdrachtformulier actief is; voor andere pakketten geldt de eerstvolgende Kantoortijd, met de mogelijkheid dat Opdrachtgever de blokkering zelf uitvoert met zijn eigen beheerderstoegang; (d) het wissen van een Apparaat vindt alleen plaats na schriftelijk akkoord van een bevoegde Contactpersoon.

8.6 Opdrachtgever meldt vermoede beveiligingsincidenten, verloren of gestolen Apparaten en verdachte berichten onmiddellijk via het supportnummer van Bijlage 2.

Artikel 9. Aansprakelijkheid en verzekering

9.1 Op de aansprakelijkheid van Partijen is artikel 9 van de Algemene Voorwaarden van toepassing, en voor Belgische Opdrachtgevers mede artikel 20 daarvan.

9.2 Opdrachtnemer houdt gedurende de Overeenkomst een beroeps- en bedrijfsaansprakelijkheidsverzekering in stand met een dekking die past bij de aard en omvang van de Diensten, met inbegrip van IT-beheer en de levering van licenties, en met werking in Nederland en België. Op verzoek verstrekt Opdrachtnemer een verzekeringscertificaat met de verzekerde bedragen, eventuele sublimieten (waaronder voor cyber- en privacyincidenten) en het eigen risico. Opdrachtnemer informeert Opdrachtgever als de dekking wezenlijk wijzigt.

Artikel 10. Beëindiging, zeggenschap en exit

10.1 Bij het einde van de Overeenkomst, op welke grond ook, is Bijlage 5 (Exit-regeling) van toepassing.

10.2 Opdrachtgever behoudt te allen tijde de zeggenschap over zijn gegevens, zijn Microsoft-tenant, zijn domeinnamen en zijn Apparaten, en heeft daartoe steeds eigen beheerderstoegang (Bijlage 4, onderdeel B). Opdrachtnemer blokkeert die toegang nooit en maakt de overdracht van gegevens, documentatie en toegang niet afhankelijk van betaling. Beëindiging van de Beheerde Diensten is iets anders dan de beschikbaarheid van afzonderlijk betaalde Microsoft-abonnementen: die blijven beschikbaar volgens de Microsoft 365-licentiebijlage en kunnen alleen volgens artikel D.1.7 van de Algemene Voorwaarden worden geschorst, na waarschuwing en met de daar genoemde continuïteitsopties.

Artikel 11. Overige bepalingen

11.1 De Overeenkomst met bijlagen en het Opdrachtformulier bevatten alle afspraken tussen Partijen over het onderwerp ervan en vervangen alle eerdere mondelinge en schriftelijke afspraken.

11.2 Wijzigingen van de Overeenkomst zijn alleen geldig als zij schriftelijk zijn vastgelegd en door beide Partijen zijn bevestigd, waaronder per e-mail door een bevoegde Contactpersoon of via elektronische ondertekening.

11.3 Op de Overeenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de rechtbank Zeeland-West-Brabant, overeenkomstig artikel 19 van de Algemene Voorwaarden. Voor Belgische Opdrachtgevers geldt aanvullend artikel 20 van de Algemene Voorwaarden; de rechtskeuze wordt in het Opdrachtformulier afzonderlijk bevestigd.

11.4 De ontvangst en aanvaarding van de Algemene Voorwaarden, de Verwerkersovereenkomst en de Microsoft 365-licentiebijlage worden vastgelegd in het Opdrachtformulier.

Bijlage 1. Dienstbeschrijving en pakketten

A. Overzicht per pakket

Onderdeel	Essentieel	Compleet	Premium
Ondersteuning op afstand tijdens Kantoortijden	Tot 30 min per Gebruiker per maand (kwartaalgemiddelde)	Onbeperkt (fair use, art. C.2 AV)	Onbeperkt (fair use, art. C.2 AV)
Supportkanalen: portaal, e-mail, telefoon, WhatsApp	Ja	Ja	Ja
Monitoring, updates en overname op afstand van Apparaten	Ja	Ja	Ja
Beheer Microsoft 365: gebruikers, mail, Teams, SharePoint	Ja	Ja	Ja
Meervoudige verificatie (MFA) op alle accounts	Ja	Ja	Ja
Noodtoegang voor Opdrachtgever (Bijlage 4, onderdeel B)	Ja	Ja	Ja
Back-up van Microsoft 365 en Entra ID (dekking: onderdeel C)	Nee	Ja	Ja
Werkplekbeheer via Intune en Autopilot	Nee	Ja	Ja
Beveiligingsbaseline (Bijlage 4, onderdeel A)	Basis	Volledig	Volledig
24/7 geautomatiseerde bewaking van Microsoft 365-accounts met automatisch ingrijpen (ITDR)	Nee	Ja	Ja
Menselijke opvolging van bewakingsmeldingen	Kantoortijden	Kantoortijden	Kantoortijden, en buiten Kantoortijden voor P1 via de noodlijn (onderdeel D)
In- en uitdiensttreding van medewerkers	Uurtarief	Inbegrepen	Inbegrepen

Onderdeel	Essentieel	Compleet	Premium
Herstel na beveiligingsincident (artikel 8.4)	Uurtarief	Inbegrepen	Inbegrepen
Kwartaalcheck en maandrapportage	Nee	Ja	Ja
24/7 geautomatiseerde bewaking van Apparaten door een Security Operations Center (EDR)	Nee	Nee	Ja
Security awareness-training en phishingsimulaties	Nee	Nee	Ja
Noodlijn buiten Kantoortijden voor P1-storingen	Nee	Nee	Ja, vanaf de activeringsdatum in het Opdrachtformulier
Uren op locatie	Nee	Nee	2 uur per kwartaal, inclusief voorrijkosten
Hardware: adviseren, bestellen, inrichten, uitleveren en afvoeren (diensten; aanschaf apart)	Nee	Nee	Ja
Kwartaalrapport beveiliging en jaarlijks IT-plan	Nee	Nee	Ja
Vereiste Microsoft-licentie	Elke Microsoft 365-licentie	Microsoft 365 Business Premium	Microsoft 365 Business Premium
Optioneel tegen meerprijs (Opdrachtformulier)		Entra ID P2 voor risicogestuurde voorwaardelijke toegang	Entra ID P2 voor risicogestuurde voorwaardelijke toegang

B. Toelichting op de onderdelen

Ondersteuning op afstand. Het beantwoorden van vragen en het oplossen van storingen van Gebruikers over de Omgeving, Apparaten, Microsoft 365 en de standaard kantoorsoftware, via de supportkanalen van Bijlage 2. Voor Essentieel geldt een grens van gemiddeld dertig (30) minuten per Gebruiker per maand, gemeten over alle Gebruikers over een kalenderkwartaal; bij overschrijding meldt Opdrachtnemer dat en worden verdere uren alleen na voorafgaand akkoord tegen het uurtarief in rekening gebracht. Voor Compleet en Premium geldt de fair-userichtlijn van artikel C.2 van de Algemene Voorwaarden: één (1) uur per Gebruiker per maand als signaal voor overleg, zonder

automatische nacalculatie. Meegeteld worden supporturen op verzoek van Gebruikers; niet meegeteld worden monitoring, updates, rapportage, inrichting en herstel van eigen fouten.

Monitoring, updates en overname op afstand. Op ieder Apparaat installeert Opdrachtnemer beheersoftware die de status bewaakt (onder meer schijfruimte, updates, beveiligingsstatus), besturingssysteem en gangbare toepassingen bijwerkt en overname op afstand mogelijk maakt na toestemming van de Gebruiker of, bij onderhoud, buiten werktijd. Ondersteund worden Windows 10/11 en macOS binnen de door de fabrikant ondersteunde versies.

Beheer Microsoft 365. Het aanmaken, wijzigen en verwijderen van gebruikers, mailboxen, groepen, gedeelde mailboxen, Teams en SharePoint-sites, het beheren van licenties en het instellen van beleid, op verzoek van een bevoegde Contactpersoon.

Back-up van Microsoft 365 en Entra ID. Een van Microsoft onafhankelijke back-up volgens de dekkingsmatrix van onderdeel C, opgeslagen in de Europese Unie bij de in de Verwerkersovereenkomst genoemde leverancier, met de daar vermelde bewaartermijn en herstelmogelijkheden. Bewaartermijnen zijn een keuze van Opdrachtgever in het Opdrachtformulier (onderdeel F).

Werkplekbeheer via Intune en Autopilot. Het inschrijven van Apparaten in Microsoft Intune, het toepassen van configuratie- en nalevingsbeleid, versleuteling (BitLocker of FileVault), het uitrollen van toepassingen en het inrichten van nieuwe Apparaten via Windows Autopilot, zodat een nieuw Apparaat rechtstreeks bij de Gebruiker kan worden afgeleverd.

Beveiligingsbaseline. De maatregelen van Bijlage 4, onderdeel A. Basis (Essentieel) omvat MFA en de uitschakeling van verouderde aanmeldmethoden; Volledig (Compleet en Premium) omvat alle maatregelen die met Microsoft 365 Business Premium mogelijk zijn. Risicogestuurde voorwaardelijke toegang (op basis van gebruikers- en aanmeldrisico) vereist Microsoft Entra ID P2 en wordt alleen ingericht als Opdrachtgever die licentie via het Opdrachtformulier heeft afgenomen; zonder P2 steunt de detectie van risicovolle aanmeldingen op de ITDR-bewaking.

24/7 bewaking van accounts (ITDR) en Apparaten (EDR). Geautomatiseerde bewaking door een Security Operations Center van een gespecialiseerde leverancier dat dag en nacht verdachte aanmeldingen, doorstuurregels, sessiediefstal en (bij EDR) kwaadaardige activiteit op Apparaten onderzoekt. Onderdeel D beschrijft per pakket wie wat doet en wanneer een mens van Opdrachtnemer reageert. Deze onderdelen gelden als geleverd vanaf de in het activeringsverslag of het Opdrachtformulier vermelde activeringsdatum.

In- en uitdiensttreding. Het aanmaken, inrichten en beveiligen van accounts en Apparaten voor nieuwe medewerkers en het gecontroleerd afsluiten daarvan bij vertrek (toegang intrekken, mailbox omzetten, gegevens overdragen, Apparaat wissen), op verzoek van een bevoegde Contactpersoon en met een aankondiging van ten minste twee (2) Werkdagen; spoedgevallen via de spoedroute van artikel 8.5.

Kwartaalcheck en maandrapportage. Maandelijks een rapport over tickets, updates, back-ups en beveiligingsstatus; per kwartaal een controle van licenties, beveiligingsinstellingen, back-ups (inclusief een proefherstel) en openstaande aanbevelingen, met een kort verslag aan de Contactpersoon.

Security awareness-training. Korte online trainingen en periodieke phishingsimulaties voor alle Gebruikers, met rapportage aan de Contactpersoon.

Noodlijn buiten Kantoortijden. Bereikbaarheid voor P1-storingen buiten Kantoortijden via het supportnummer, met de reactietijd van Bijlage 2, vanaf de in het Opdrachtformulier vermelde activeringsdatum. Zolang de noodlijn niet is geactiveerd, geldt buiten Kantoortijden uitsluitend de geautomatiseerde bewaking van onderdeel D. Werkzaamheden buiten Kantoortijden worden tegen het tarief van Bijlage 3 in rekening gebracht, tenzij het incident aan Opdrachtnemer toerekenbaar is.

Uren op locatie. Twee (2) uur per kalenderkwartaal op een locatie van Opdrachtgever in Nederland of België, in overleg in te plannen; niet-gebruikte uren vervallen aan het einde van het kwartaal. Voorrijkosten zijn inbegrepen.

Hardware. Het adviseren, bestellen, inrichten, uitleveren en aan het einde van de levensduur veilig wissen en afvoeren van Apparaten, volgens module D van de Algemene Voorwaarden. De aanschafkosten van hardware vallen buiten het pakket en worden vooraf geoffreerd.

Kwartaalrapport beveiliging en jaarlijks IT-plan. Per kwartaal een beveiligingsrapport met bevindingen en aanbevelingen; jaarlijks een IT-plan met de voorgestelde vervangingen, verbeteringen en begroting voor het volgende jaar.

C. Dekkingsmatrix back-up (Compleet en Premium)

Workload	Gedekt	Niet gedekt (beperkingen van de dienst)
Exchange Online	Gebruikersmailboxen en gedeelde mailboxen (ook gedeelde mailboxen zonder Microsoft-licentie), standaardagenda, contacten, taken, archiefmailboxen	Mailboxen buiten de tenant; gegevens die vóór de eerste back-up zijn verwijderd; gedeelde en niet-standaard agenda's, uitnodigingsreacties, de groepsmailbox en groepsagenda van Microsoft 365-groepen en Planner-taken (geen Microsoft-API beschikbaar volgens de leverancier)
OneDrive	Bestanden en mappen van Gebruikers, inclusief versies volgens de leverancier	Items in de map "Gedeeld" (eigendom van andere gebruikers) en de prullenbak; gedeelde koppelingen en machtigingen worden hersteld voor zover de leverancier dat ondersteunt
SharePoint	Sites, documentbibliotheken, lijsten en pagina's	De prullenbak; aangepaste webonderdelen, workflows en machtigingsstructuren voor zover de leverancier die niet meeneemt
Teams	Teams (Microsoft 365-groepen), openbare en privékanalen, kanaalberichten en bestanden in kanalen (via de SharePoint-site van het team); privéchats (1:1), groepschats en vergaderchats inclusief bijlagen via de Archiver-functie van het gecontracteerde	Vergaderopnames, apps en tabbladen van derden, telefoniegegevens; gearchiveerde Teams (eerst dearchiveren) en externe Teams

Workload	Gedekt	Niet gedekt (beperkingen van de dienst)
	abonnement (Backup+Archiver), uitsluitend als download (EML, PDF of CSV), niet als herstel in Teams	
Entra ID	Gebruikers, groepen, rollen en beheerders, beleidsregels voor voorwaardelijke toegang, benoemde locaties, authenticatiemethoden en -sterkte, app-machtigingen en service principals, administratieve eenheden, apparaatbeheerbeleid en andere door de leverancier ondersteunde objecten	Wachtwoorden en MFA-registraties; BitLocker-herstelsleutels en apparaatobjecten (wel geback-upt, niet herstelbaar); objecten buiten de ondersteunde lijst

Kenmerk	Afspraak
Frequentie	Ten minste dagelijks; waar de leverancier dat ondersteunt meerdere malen per dag (SharePoint driemaal daags; Entra ID naar keuze iedere 8 of 24 uur)
Beoogd maximaal gegevensverlies (RPO)	24 uur voor alle workloads; korter waar de frequentie hoger is
Herstel	Per item, per gebruiker, per site of volledig, naar de oorspronkelijke of een andere locatie; export in een gangbaar formaat op verzoek
Hersteldoel (RTO)	Streefwaarde: start van het herstel binnen de reactietijd van de SLA; herstel van een enkel item binnen één (1) Werkdag; volledig herstel van een mailbox of site binnen drie (3) Werkdagen, afhankelijk van omvang en de snelheid van Microsoft en de leverancier. De RTO is een streefwaarde, geen garantie
Bewaartermijn	Volgens de keuze van Opdrachtgever in het Opdrachtformulier: het gecontracteerde abonnement (NinjaOne SaaS Backup, Backup+Archiver met Entra) biedt iedere termijn van dertig (30) dagen tot dertien (13) jaar of onbeperkt, met de mogelijkheid per gegevenssoort (mail, OneDrive, SharePoint) een eigen termijn te kiezen. Opdrachtgever legt zijn keuze en de reden daarvoor vast; is geen keuze gemaakt, dan geldt vier (4) jaar voortschrijdend totdat Opdrachtgever anders instrueert
Verwijdering	Verwijdering per gebruiker (mailbox en OneDrive) is mogelijk; verwijdering van afzonderlijke items uit SharePoint-, Groups- of Teams-back-ups is niet mogelijk, alleen van die volledige back-up. Waar selectieve verwijdering niet mogelijk is, wordt de toegang beperkt en verloopt de verwijdering via de bewaartermijn. Na een herstel worden eerder gegeven wisinstructies opnieuw

Kenmerk	Afspraak
	uitgevoerd
Opslag	Europese Unie, gescheiden van de productieomgeving, met de door de leverancier geboden bescherming tegen wijziging of verwijdering (onveranderbaarheid voor zover contractueel bevestigd)
Tests	Proefherstel per kwartaal (onderdeel B); uitkomst in de kwartaalcheck; mislukt een proefherstel, dan meldt Opdrachtnemer dat binnen twee (2) Werkdagen met een herstelplan
Escalatie	Bij een mislukte back-up of herstel escaleert Opdrachtnemer naar de leverancier en informeert hij de Contactpersoon over de verwachte oplossing

De dekking is beperkt tot wat de in de Verwerkersovereenkomst genoemde leverancier voor het gecontracteerde product ondersteunt. Opdrachtnemer bevestigt het product, de opslagregio en de bescherming tegen wijziging vóór de activering in het activeringsverslag.

D. Bewaking en opvolging per pakket

Onderwerp	Essentieel	Compleet	Premium
Wie kijkt 24/7	Niemand (alleen Microsoft-standaardbeveiliging)	Geautomatiseerd SOC (ITDR)	Geautomatiseerd SOC (ITDR en EDR)
Toegestane automatische acties	Geen	Blokkeren van een gecompromitteerd account, intrekken van sessies, uitschakelen van kwaadaardige doorstuurregels	Idem, plus isoleren van een Apparaat
Wie wordt gewaarschuwd	Niet van toepassing	Opdrachtnemer (portaal en e-mail); de Contactpersoon bij een geblokkeerd account per e-mail	Opdrachtnemer (portaal, e-mail en telefonisch bij P1); de Contactpersoon en het noodcontact bij een geblokkeerd account of geïsoleerd Apparaat
Menselijke opvolging door Opdrachtnemer	Kantoortijden, reactietijd SLA	Kantoortijden, reactietijd SLA; buiten Kantoortijden vanaf de eerstvolgende Kantoortijd	Kantoortijden, reactietijd SLA; buiten Kantoortijden binnen de P1-reactietijd via de noodlijn zodra geactiveerd

Onderwerp	Essentieel	Compleet	Premium
Achtervang bij afwezigheid van Opdrachtnemer	Documentatie en noodtoegang van Opdrachtgever	Idem, plus automatische SOC-acties	Idem, plus de noodlijn vanaf de activeringsdatum

E. Buiten het pakket

Buiten ieder pakket vallen, tenzij in onderdeel A of B uitdrukkelijk als inbegrepen vermeld of in het Opdrachtformulier anders overeengekomen: projecten en migraties (waaronder de overstap van een andere leverancier of mailomgeving, behalve de inrichting van artikel 5), werkzaamheden op locatie buiten de inbegrepen uren, werkzaamheden buiten Kantoortijden, trainingen anders dan de security awareness-training in Premium, het beheer van servers, netwerkapparatuur, printers, telefonie en bedrijfsapplicaties die niet in de goedgekeurde inventarisatie zijn opgenomen, het herstel van schade door handelen van Opdrachtgever of derden, de niet-inbegrepen onderdelen van artikel 8.4, en de kosten van Producten. Deze werkzaamheden worden na akkoord van een bevoegde Contactpersoon uitgevoerd tegen de tarieven van Bijlage 3; ook bij een omvang van minder dan vier uur wordt vooraf akkoord gevraagd. Een uitdrukkelijk inbegrepen dienst gaat voor op deze algemene uitsluiting.

F. Inventarisatie

De Apparaten, Gebruikers, locaties, bedrijfsapplicaties en overige onderdelen die onder de Beheerde Diensten vallen, worden bij de start vastgelegd in een gedateerde inventarisatie die door beide Partijen wordt goedgekeurd (startinventaris bij het Opdrachtformulier) en die bij iedere wijziging in het klantenportaal wordt bijgewerkt en door de Contactpersoon wordt bevestigd. Onderdelen die niet in de goedgekeurde inventarisatie staan, vallen buiten de Beheerde Diensten; een onderdeel dat Opdrachtgever tijdig heeft gemeld maar dat door een omissie van Opdrachtnemer niet is vastgelegd, valt niet om die reden buiten de Beheerde Diensten.

Bijlage 2. Service Level Agreement (SLA)

A. Supportkanalen en tijden

Kanaal	Gegevens	Beschikbaar
Klantenportaal	Link wordt bij de start verstrekt; tickets en status inzien	24/7
E-mail	support@van-oosten.nl	24/7 (afhandeling tijdens Kantoortijden)
Telefoon	+31 85 109 1360	Kantoortijden; Premium: ook buiten Kantoortijden voor P1 zodra de noodlijn is geactiveerd
WhatsApp Business	+31 85 109 1360	Kantoortijden; niet voor wachtwoorden of vertrouwelijke gegevens
Noodkanaal bij uitval van de telefonie	E-mail aan support@van-oosten.nl met "SPOED" in het onderwerp, plus het reservenummer +31 6 40330125	24/7

Kantoortijden: Werkdagen van 08:30 tot 17:00 uur Nederlandse tijd, met uitzondering van in Nederland algemeen erkende feestdagen. Voor Belgische Opdrachtgevers gelden dezelfde Nederlandse Kantoortijden en feestdagen; Belgische feestdagen die geen Nederlandse feestdag zijn, gelden als Werkdag.

Iedere melding wordt vastgelegd als ticket met een uniek nummer. Opdrachtgever ontvangt een bevestiging en kan de status volgen in het klantenportaal.

B. Prioriteiten

Prioriteit	Omschrijving	Voorbeelden
P1 Kritiek	De hele organisatie of een bedrijfskritisch proces kan niet werken, of er is een acuut beveiligingsincident	Niemand kan inloggen of mailen; ransomware; gecompromitteerd account
P2 Hoog	Eén Gebruiker kan niet werken, of een belangrijke functie werkt niet voor meerdere Gebruikers	Laptop start niet; Teams werkt niet voor een afdeling
P3 Normaal	Vragen, wijzigingen en storingen met een werkbaar alternatief	Nieuwe medewerker; printer op één laptop; vraag over Outlook

De prioriteit wordt bij aanmelding vastgesteld op basis van de informatie van Opdrachtgever, volgens de bovenstaande omschrijvingen; Opdrachtgever geeft de prioriteit die hij nodig acht aan en Opdrachtnemer wijkt daar alleen gemotiveerd van af. Opdrachtgever meldt P1-storingen telefonisch; is de telefoon niet bereikbaar, dan via het

noodkanaal. Opdrachtnemer blijft verantwoordelijk voor triage, escalatie en communicatie, ook als de oorzaak buiten zijn invloed ligt.

C. Reactietijden

Prioriteit	Essentieel	Compleet	Premium
P1 Kritiek	4 werkuren	2 werkuren	1 uur, ook buiten Kantoortijden (vanaf activering noodlijn)
P2 Hoog	1 Werkdag	4 werkuren	2 werkuren
P3 Normaal	2 Werkdagen	1 Werkdag	4 werkuren

Start van de klok. De reactietijd begint op het moment van aantoonbare ontvangst van de melding door Opdrachtnemer via een supportkanaal (het tijdstip van de e-mail, het portaalbericht, het WhatsApp-bericht of het telefoongesprek), of, bij een storing die Opdrachtnemer zelf via zijn monitoring constateert, op het moment van de monitoringmelding. De klok start niet pas bij de interne registratie als ticket. Buiten Kantoortijden ontvangen meldingen gelden als ontvangen bij aanvang van de eerstvolgende Kantoortijden, behalve voor Premium P1 via de noodlijn.

Reactie is het moment waarop een medewerker van Opdrachtnemer met de melding aan de slag gaat en Opdrachtgever daarover informeert. Werkuren en Werkdagen worden geteld binnen Kantoortijden.

Pauzeren van de klok. De klok wordt alleen gepauzeerd zolang Opdrachtnemer aantoonbaar wacht op door hem gevraagde informatie, toegang of een beslissing van Opdrachtgever, en Opdrachtgever daarover is geïnformeerd.

De reactietijd is geen oplostijd. Opdrachtnemer streeft naar oplossing binnen de kortst mogelijke termijn en houdt Opdrachtgever op de hoogte van de voortgang: bij P1 ten minste iedere twee (2) uur, bij P2 ten minste dagelijks.

D. Uitsluitingen

De reactietijden gelden niet voor zover een melding het gevolg is van of vertraging ondervindt door: (a) overmacht in de zin van de Algemene Voorwaarden; (b) het niet nakomen door Opdrachtgever van zijn verplichtingen, waaronder het niet verlenen van toegang of medewerking; (c) apparatuur, software of onderdelen die niet in de goedgekeurde inventarisatie zijn opgenomen; (d) wijzigingen die Opdrachtgever of derden zonder overleg hebben aangebracht; (e) vooraf aangekondigd onderhoud. Een storing bij Microsoft of een andere leverancier ontslaat Opdrachtnemer niet van zijn eigen reactieverplichting: Opdrachtnemer reageert binnen de reactietijd, stelt de oorzaak vast, escaleert naar de leverancier en informeert Opdrachtgever; alleen de oplostijd en de beschikbaarheid van die dienst liggen buiten zijn invloed.

E. Onderhoud

Gepland onderhoud aan de Omgeving voert Opdrachtnemer zoveel mogelijk buiten Kantoortijden uit en kondigt hij ten minste twee (2) Werkdagen vooraf aan bij de Contactpersoon, tenzij het onderhoud spoedeisend is vanwege een beveiligingsrisico.

Updates van besturingssystemen en toepassingen op Apparaten worden automatisch en gefaseerd uitgerold.

F. Rapportage en meting

Opdrachtnemer meet de reactietijden in zijn ticketsysteem op basis van het ontvangsttijdstip van onderdeel C en rapporteert daarover in de maandrapportage (Compleet en Premium) of op verzoek (Essentieel). De registratie in het ticketsysteem van Opdrachtnemer geldt tussen Partijen als bewijs, behoudens tegenbewijs door Opdrachtgever, bijvoorbeeld met het verzendtijdstip van zijn melding.

G. Servicecredit bij het niet halen van reactietijden

1. **Meetperiode en noemer.** Per kalenderkwartaal worden alle P1- en P2-tickets geteld die in dat kwartaal zijn ontvangen. Tickets die uit hetzelfde incident voortkomen, tellen als één ticket.

2. **Drempel.** Als bij meer dan twintig procent (20%) van die tickets, of bij ten minste twee (2) tickets wanneer het kwartaal minder dan tien P1- en P2-tickets telt, de reactietijd niet is gehaald om redenen die aan Opdrachtnemer toerekenbaar zijn, heeft Opdrachtgever recht op een servicecredit.

3. **Hoogte.** De servicecredit bedraagt tien procent (10%) van de vergoeding voor de Beheerde Diensten over de drie maanden van het betreffende kwartaal. Rekenvoorbeeld: bij een beheervergoeding van € 339 per maand is de servicecredit 10% van € 1.017, dus € 101,70. Bij twee gemiste P1-reactietijden in hetzelfde kwartaal wordt de servicecredit verdubbeld.

4. **Toekenning.** Opdrachtnemer kent de servicecredit automatisch toe op de eerste factuur na afloop van het kwartaal, op basis van zijn eigen meetgegevens; Opdrachtgever hoeft geen aanvraag te doen. Opdrachtgever kan binnen zestig (60) dagen na ontvangst van de kwartaalrapportage aanvullende gemiste reactietijden aanmelden.

5. **Reikwijdte.** De servicecredit is de enige vergoeding voor de enkele overschrijding van een reactietijd. Zij laat onverlet de rechten van Opdrachtgever bij een afzonderlijke tekortkoming in de uitvoering van de Beheerde Diensten (zoals het niet uitvoeren van overeengekomen maatregelen, dataverlies of een schending van de Verwerkersovereenkomst), de rechten bij ontbinding en dwingendrechtelijke rechten.

6. **Beëindiging.** Als in twee (2) opeenvolgende kwartalen een servicecredit verschuldigd is, of in één kwartaal bij meer dan vijftig procent (50%) van de P1- en P2-tickets de reactietijd is gemist, mag Opdrachtgever de Overeenkomst schriftelijk opzeggen met een opzegtermijn van één (1) kalendermaand, ook tijdens de initiële termijn, zonder beëindigingsvergoeding.

H. Escalatie

Bij ontevredenheid over de afhandeling van een melding kan de Contactpersoon escaleren naar de directie van Opdrachtnemer via info@van-oosten.nl of het supportnummer. Opdrachtnemer reageert op een escalatie binnen één (1) Werkdag.

Bijlage 3. Prijzen en tarieven

Alle bedragen zijn in euro's, exclusief btw en exclusief de kosten van Microsoft-abonnementen en andere Producten. Prijzen per kalendermaand, per organisatie.

A. Pakketprijzen (staffels op basis van het aantal Gebruikers)

Pakket	1 tot 2 Gebruikers	3 tot 5 Gebruikers	6 tot 10 Gebruikers	11 tot 50 Gebruikers
Essentieel	€ 109	€ 229	€ 399	Op offerte; tot aanvaarding € 399 plus € 35 per Gebruiker boven 10
Compleet	€ 169	€ 339	€ 579	Op offerte; tot aanvaarding € 579 plus € 50 per Gebruiker boven 10
Premium	€ 249	€ 489	€ 829	Op offerte; tot aanvaarding € 829 plus € 75 per Gebruiker boven 10

De Beheerde Diensten zijn bedoeld voor organisaties tot vijftig (50) Gebruikers. Groeit Opdrachtgever daarboven, dan maken Partijen nadere afspraken; tot die zijn gemaakt, geldt de laatste kolom van de tabel.

B. Eenmalige en losse tarieven

Dienst	Tarief	Toelichting
Opstart en inrichting, 1 tot 2 Gebruikers	€ 395 eenmalig	Inventarisatie, beveiligingsbaseline, noodtoegang, documentatie, activeringsverslag
Opstart en inrichting, 3 tot 5 Gebruikers	€ 695 eenmalig	Idem
Opstart en inrichting, 6 tot 10 Gebruikers	€ 995 eenmalig	Idem; vervalt bij overname van een bestaande beheerde omgeving als dat op het Opdrachtformulier is vermeld
Projecten, migraties, advies	€ 125 per uur	Schriftelijk akkoord vooraf; offerte bij meer dan 4 uur
Werkzaamheden op locatie	€ 125 per uur plus € 75 voorrijkosten per bezoek	Premium: 2 uur per kwartaal inbegrepen
Werkzaamheden buiten Kantoortijden	€ 187,50 per uur	Alleen bij P1, minimaal 1 uur; niet bij een aan Opdrachtnemer toerekenbaar incident
Nieuw Apparaat inrichten via Autopilot	€ 95 per Apparaat	Inclusief levering aan de Gebruiker; Premium: inbegrepen
Training van	€ 125 per uur	In groep of individueel

Dienst	Tarief	Toelichting
Gebruikers		
Hardware	Inkoopprijs plus vooraf geoffreerde opslag	Altijd vooraf geoffreerd

Uren worden geregistreerd in eenheden van vijftien (15) minuten. Reistijd voor werkzaamheden op locatie wordt niet als werktijd gerekend; daarvoor gelden de voorrijkosten.

C. Prijs per Gebruiker (alleen als in het Opdrachtformulier gekozen)

In plaats van de staffelprijs van onderdeel A kan in het Opdrachtformulier een vaste prijs per Gebruiker per maand worden overeengekomen voor het gekozen pakket. Die prijs wordt maandelijks berekend over het aantal Gebruikers volgens artikel 4.2 van de Overeenkomst, wordt geïndexeerd volgens artikel 7.2 van de Algemene Voorwaarden en sluit de toepassing van onderdeel A en van de prijzen op www.van-oosten.nl uit. Het Opdrachtformulier vermeldt dat wordt afgeweken van onderdeel A.

D. Betaling

Maandelijkse vergoedingen worden vooraf gefactureerd. Betaling per overboeking binnen veertien (14) dagen na factuurdatum. Facturen worden elektronisch verzonden (pdf per e-mail; via Peppol op verzoek zodra Opdrachtnemer daarop is aangesloten).

Bijlage 4. Beveiligingsbaseline, noodtoegang, toegang van Opdrachtnemer en toeleveringsketen

A. Beveiligingsbaseline

Opdrachtnemer richt de Omgeving in volgens onderstaande baseline, binnen de termijnen van artikel 5.2, in overleg met Opdrachtgever en na inventarisatie van afhankelijkheden (zoals printers, scanners en toepassingen die nog via verouderde aanmeldmethoden mailen). Onderdelen gemarkeerd met (C) gelden voor Compleet en Premium; (P) alleen voor Premium; (P2) alleen als Entra ID P2 is afgenomen.

Maatregel	Inhoud
Meervoudige verificatie	MFA verplicht voor alle Gebruikers en beheerders, bij voorkeur via de Microsoft Authenticator-app; nummervergelijking ingeschakeld
Verouderde aanmelding uit	Blokkering van verouderde aanmeldmethoden (legacy authentication) na inventarisatie van afhankelijkheden
Voorwaardelijke toegang (C)	Beleid met de mogelijkheden van Microsoft 365 Business Premium (Entra ID P1): MFA afdwingen, verouderde aanmelding blokkeren, beheerdersrollen extra beperken, apparaatvereisten (Intune-naleving) en locatiebeleid; noodtoegangsaccounts uitgezonderd met alarmering
Risicogestuurde toegang (P2)	Beleid op basis van gebruikers- en aanmeldrisico (Entra ID Protection); alleen met Entra ID P2
Beheerdersaccounts	Aparte beheerdersaccounts zonder mailbox; geen dagelijks gebruik van beheerrechten; twee noodtoegangsaccounts volgens onderdeel B
Endpointbeveiliging (C)	Microsoft Defender for Business ingeschakeld en centraal beheerd; versleuteling van Apparaten; regels tegen misbruik van kantoortoepassingen
Updates	Besturingssystemen en gangbare toepassingen automatisch bijgewerkt via het beheerplatform; beveiligingsupdates binnen 14 dagen na beschikbaarheid, kritieke updates zo spoedig mogelijk
E-mailbeveiliging (C)	Anti-phishing, veilige bijlagen en koppelingen, SPF, DKIM en DMARC voor de domeinen van Opdrachtgever
Back-up (C)	Back-up van Microsoft 365 en Entra ID volgens Bijlage 1, onderdeel C
Bewaking (C)	24/7 geautomatiseerde bewaking van accounts (ITDR); (P) 24/7 geautomatiseerde bewaking van Apparaten (EDR); opvolging volgens Bijlage 1, onderdeel D
Logging	Auditlogboeken van Microsoft 365 ingeschakeld en bewaard volgens de mogelijkheden van de licentie; beheerhandelingen van Opdrachtnemer worden gelogd in

Maatregel	Inhoud
	het beheerplatform
Bewustwording (P)	Security awareness-training en phishingsimulaties
Documentatie	De configuratie van de Omgeving en de contactgegevens worden vastgelegd in het documentatieplatform van Opdrachtnemer, uitsluitend toegankelijk voor geautoriseerde medewerkers van Opdrachtnemer met MFA

Afwijkingen. Als Opdrachtgever een onderdeel van de baseline niet wil laten toepassen, legt Opdrachtnemer dat schriftelijk vast met de bijbehorende risico's en de handtekening of e-mailbevestiging van een bevoegde Contactpersoon. Opdrachtnemer is niet aansprakelijk voor schade die het gevolg is van een aldus geweigerde maatregel.

B. Noodtoegang van Opdrachtgever

1. Bij oplevering van de kritieke onderdelen (artikel 5.2) beschikt Opdrachtgever over zelfstandig bruikbare noodtoegang tot zijn tenant. Opdrachtnemer richt daartoe twee afzonderlijke cloud-only noodtoegangsaccounts (break-glass) in op het *.onmicrosoft.com-domein van Opdrachtgever, met de rol Global Administrator, zonder mailbox en zonder licenties die niet nodig zijn, volgens de richtlijnen van Microsoft voor noodtoegangsaccounts.

2. Beveiliging: een phishingbestendige verificatiemethode (FIDO2-beveiligingssleutel of passkey) per account, of, zolang Opdrachtgever daarover niet beschikt, een lange willekeurige wachtwoordzin in combinatie met een door Opdrachtnemer ter beschikking gestelde beveiligingssleutel. De accounts zijn uitgezonderd van het beleid voor voorwaardelijke toegang, zodat een fout in dat beleid niet beide accounts blokkeert, en ieder gebruik van deze accounts leidt tot een directe alarmering naar Opdrachtnemer en de Contactpersoon.

3. Bewaring: de gegevens van het eerste account worden bij oplevering aan de Contactpersoon overhandigd (verzegelde envelop of veilige digitale overdracht) voor bewaring door Opdrachtgever zelf, buiten de systemen van Opdrachtnemer. De gegevens van het tweede account worden versleuteld bewaard in de wachtwoordkluis van Opdrachtnemer en op verzoek van een bevoegde Contactpersoon direct verstrekt. Een kluis die alleen Opdrachtnemer kan openen, geldt niet als noodtoegang van Opdrachtgever.

4. Beheer: Opdrachtnemer test ieder kwartaal of beide accounts werken en documenteert dat in de kwartaalcheck; de sleutels of wachtwoordzinnen zijn uitgezonderd van automatisch verlopen en van automatische opschoning wegens inactiviteit en worden geroteerd bij vertrek van een betrokken medewerker van een van beide Partijen, bij een vermoeden van compromittering en bij het einde van de Overeenkomst. Opdrachtgever meldt direct als de bij hem bewaarde gegevens zoek of mogelijk bekend zijn geraakt.

5. Voor Essentieel zonder voorwaardelijke toegang gelden de punten 1, 3 en 4 onverkort; de uitzondering op het beleid van punt 2 is dan niet van toepassing.

C. Toegang van Opdrachtnemer: GDAP en app-machtigingen

1. **Menselijke beheertoegang** verloopt uitsluitend via een tijdgebonden beheerrelatie (GDAP) met de minimaal benodigde rollen, volgens de Microsoft 365-licentiebijlage en het Opdrachtformulier. Opdrachtnemer gebruikt geen permanente Global Administrator-rechten; tijdelijk benodigde Global Administrator-toegang wordt in een afzonderlijke, kortlopende GDAP-relatie aangevraagd en na afloop verwijderd.

2. **Machinetoegang** verloopt via app-registraties en service principals van de gebruikte tooling. Opdrachtgever machtigt Opdrachtnemer daartoe in het Opdrachtformulier. De technische toestemming (admin consent) in de tenant wordt, afhankelijk van de toepassing, vastgelegd door een beheerder van Opdrachtgever of door Opdrachtnemer op grond van de GDAP-rol Cloud Application Administrator via de daarvoor bestemde Microsoft-partnerinterface; Opdrachtnemer legt per toepassing vast op welke wijze en op welke datum de toestemming is gegeven. Bij aanvang zijn dat:

Toepassing	Doel	Eigenaar	Toegestane reikwijdte (scopes)
Beheerplatform voor Microsoft 365 (CIPP)	Uitrol en controle van beveiligingsinstellingen, gebruikersbeheer, rapportage	Opdrachtnemer	Lezen en beheren van gebruikers, groepen, beleid, licenties en beveiligingsinstellingen; volgens de bij activering vastgelegde lijst
Back-upplatform (NinjaOne SaaS Backup, Backup+Archiver met Entra)	Back-up en herstel van Exchange Online, OneDrive, SharePoint, Teams (inclusief archivering van privéchats) en Entra ID	Opdrachtnemer	Lezen en schrijven van de te beveiligen workloads; autorisatie bij activering door een beheerder van Opdrachtgever of door Opdrachtnemer via GDAP; de leverancier maakt daarbij eigen enterprise applications in de tenant aan (back-up en herstel gescheiden) en een back-upserviceaccount dat als gedocumenteerde uitzondering in het beleid voor voorwaardelijke toegang wordt opgenomen
Bewaking van accounts (ITDR)	Detectie van en ingrijpen bij gecompromitteerde accounts	Opdrachtnemer	Lezen van aanmeld- en auditlogboeken; blokkeren van accounts en intrekken van sessies
Beheer en monitoring van Apparaten (NinjaOne-agent)	Monitoring, updates en ondersteuning op afstand	Opdrachtnemer	Lokale beheerdersrechten op de Apparaten

3. Opdrachtnemer houdt in de documentatie een actueel overzicht bij van alle app-machtigingen, service principals, tokens en certificaten met doel, eigenaar, toegestane reikwijdte en datum van toestemming, en legt tijdelijke uitzonderingen tijdens de inrichting met een einddatum vast. Het overzicht wordt bij de kwartaalcheck gecontroleerd en op verzoek verstrekt.

4. Beëindiging van de GDAP-relatie trekt de machinetoegang niet automatisch in. Bij het einde van de Overeenkomst trekt Opdrachtnemer volgens Bijlage 5 ook alle app-machtigingen, service principals, tokens en certificaten in en bevestigt dat in een controleverslag.

D. Afspraken voor de toeleveringsketen (NIS2 en Cyberbeveiligingswet)

Dit onderdeel geldt als Opdrachtgever in het Opdrachtformulier heeft aangegeven dat hij onder de Nederlandse Cyberbeveiligingswet, de Belgische NIS2-wet of vergelijkbare sectorale beveiligingsverplichtingen valt, of als Opdrachtgever dat later schriftelijk meldt. Het geldt onafhankelijk van de vraag of Opdrachtnemer zelf onder die wetgeving valt.

1. **Beveiligingsmaatregelen.** Opdrachtnemer past voor de eigen organisatie en de gebruikte tooling maatregelen toe die passen bij de risico's, waaronder: MFA en least privilege voor alle beheertoegang, gescheiden beheerdersaccounts, versleutelde opslag van toegangsgegevens, logging van beheerhandelingen, geteste back-ups van de eigen documentatie, en beveiligingsupdates volgens onderdeel A. Opdrachtnemer werkt uitsluitend met leveranciers die beschikken over een geldig ISO 27001-certificaat of een actueel SOC 2-assurancerapport waarvan de reikwijdte de geleverde dienst omvat, of die een gelijkwaardig, aantoonbaar beveiligingsniveau hebben; Opdrachtnemer controleert de geldigheid en reikwijdte jaarlijks. Voor Belgische Opdrachtgevers hanteert Opdrachtnemer als referentiekader voor de eigen maatregelen het CyberFundamentals-raamwerk (CyFun) van het Centrum voor Cybersecurity België, niveau Basic.

2. **Incidentmelding.** Opdrachtnemer meldt beveiligingsincidenten die de Omgeving raken volgens artikel 8.2, met een eerste waarschuwing zo snel mogelijk en uiterlijk binnen vierentwintig (24) uur na ontdekking, zodat Opdrachtgever zijn eigen wettelijke meldtermijnen kan halen, en verleent redelijke medewerking aan de meldingen en rapportages van Opdrachtgever aan de bevoegde autoriteiten.

3. **Informatie en toetsing.** Opdrachtnemer verstrekt op verzoek, eenmaal per jaar en daarnaast bij een incident, een wezenlijke wijziging in de keten of een gemotiveerd verzoek van een toezichthouder, een beschrijving van zijn beveiligingsmaatregelen, een actueel overzicht van de gebruikte leveranciers (subverwerkers) met hun certificeringen en, voor zover beschikbaar, de rapporten van die leveranciers. Opdrachtgever mag eenmaal per jaar, na dertig (30) dagen aankondiging, en daarnaast bij gerechtvaardigde spoed na een incident of op verzoek van een toezichthouder met een kortere termijn, een toetsing van de naleving van deze bijlage laten uitvoeren door een onafhankelijke, aan geheimhouding gebonden deskundige. De redelijke kosten van de medewerking van Opdrachtnemer worden tegen het uurtarief in rekening gebracht, tenzij de toetsing een wezenlijke tekortkoming aantoont. Dit laat het auditrecht in de Verwerkersovereenkomst onverlet.

4. **Continuïteit.** Opdrachtnemer documenteert de Omgeving zodanig dat een andere bekwame IT-dienstverlener het beheer kan overnemen, houdt de noodtoegang van onderdeel B in stand en werkt mee aan de exit-regeling van Bijlage 5.

5. **Eigen positie van Opdrachtnemer.** Opdrachtnemer heeft een gedateerde scopeanalyse uitgevoerd aan de hand van de artikelen 8, 9 en 12 van de Cyberbeveiligingswet en de omvangscriteria van Aanbeveling 2003/361/EG (met inbegrip van partner- en verbonden ondernemingen), en van de Belgische NIS2-wet, op basis van zijn actuele bedrijfs- en groepsgegevens (omvang, omzet, verbonden ondernemingen, aangeboden diensten, waaronder beheerde ICT- en beveiligingsdiensten in de sector beheer van ICT-diensten, en eventuele aanwijzing door de bevoegde autoriteit). De uitkomst van die analyse en de datum van de volgende herbeoordeling vermeldt Opdrachtnemer in het activeringsverslag. Opdrachtnemer informeert Opdrachtgever binnen dertig (30) dagen als de uitkomst wijzigt. Deze bijlage vraagt van Opdrachtgever geen erkenning van de juridische status van Opdrachtnemer.

Bijlage 5. Exit-regeling

5.1 **Doel en classificatie.** Deze bijlage regelt de ordelijke overdracht van de Beheerde Diensten bij het einde van de Overeenkomst, zodat Opdrachtgever zonder onderbreking verder kan met een andere leverancier of met eigen beheer. Voor de toepassing van Verordening (EU) 2023/2854 (Data Act) geldt: de back-updienst van Bijlage 1, onderdeel C, is een dataverwerkingsdienst waarvoor Opdrachtnemer de daarvoor geldende overstapregels toepast; de overige Beheerde Diensten zijn menselijke beheer- en ondersteuningsdiensten en de Microsoft-abonnementen zijn diensten van Microsoft waarvoor de Microsoft-voorwaarden gelden. Voor zover de Data Act op een onderdeel van toepassing is, gaan de daarin dwingend voorgeschreven termijnen en kostenregels voor op deze bijlage.

5.2 **Exitperiode en termijnen.** De exitperiode begint op de dag van de opzegging of ontbinding en eindigt dertig (30) dagen na de einddatum van de Overeenkomst, of zoveel eerder als de overdracht is voltooid. Voor de back-updienst geldt (artikel 25 Data Act): een overstapverzoek van Opdrachtgever wordt binnen dertig (30) kalenderdagen uitgevoerd (transitieperiode). Opdrachtgever mag de transitieperiode eenmaal verlengen met een door hem opgegeven periode die hij voor zijn doeleinden passender acht. Als dertig dagen technisch niet haalbaar is, meldt Opdrachtnemer dat gemotiveerd binnen veertien (14) werkdagen na het overstapverzoek en noemt hij een alternatieve transitieperiode van ten hoogste zeven (7) maanden, waarin de dienst wordt voortgezet. Opdrachtgever kan gedurende ten minste dertig (30) kalenderdagen na afloop van de transitieperiode zijn gegevens ophalen (ophaalperiode). De opzegtermijn voor het starten van de overstap bedraagt nooit meer dan twee (2) maanden. Op verzoek van Opdrachtgever kan de exitperiode voor de overige diensten eenmaal met maximaal dertig (30) dagen worden verlengd tegen de dan geldende maandelijkse vergoeding naar rato per dag.

5.3 **Medewerking van Opdrachtnemer.** Opdrachtnemer:

a) verstrekt Opdrachtgever de actuele documentatie van de Omgeving: inventarisatie van Apparaten en Gebruikers, configuratieoverzicht, domein- en DNS-gegevens, licentieoverzicht, een overzicht van de ingestelde beveiligingsmaatregelen, het overzicht van app-machtigingen (Bijlage 4, onderdeel C) en de contactgegevens van leveranciers, met het blijvende gebruiksrecht van artikel 13.2 van de Algemene Voorwaarden voor Opdrachtgever en zijn opvolgende dienstverlener;

b) verstrekt de gegevens van de noodtoegangsaccounts (Bijlage 4, onderdeel B) en van alle accounts en systemen die op naam van Opdrachtgever staan, via een veilig kanaal (versleuteld bestand met apart verzonden sleutel of overdracht in de wachtwoordkluis van Opdrachtgever) aan een bevoegde Contactpersoon, en roteert daarna de eigen toegang;

c) werkt mee aan de overdracht van de Microsoft-abonnementen aan een andere wederverkoper of aan beëindiging per einde looptijd, volgens de Microsoft 365-licentiebijlage;

d) verwijdert na de overdracht, op een met Opdrachtgever afgesproken moment en nadat de opvolger werkt, zijn beheerrelatie (GDAP), alle app-machtigingen, service principals, tokens en certificaten, beheersoftware, monitoringagenten

en beveiligingsagenten uit de Omgeving en van de Apparaten, en verstrekt een controleverslag van de verwijderde toegang;

e) stelt de back-upgegevens van Microsoft 365 en Entra ID gedurende de exitperiode en de ophaalperiode beschikbaar voor terugzetten en levert op verzoek een export in een gangbaar formaat; de verwijdering van back-ups volgt de uniforme regeling van artikel 5.7;

f) draagt hardware die op naam van Opdrachtnemer bij een fabrikant of beheerplatform is geregistreerd over aan Opdrachtgever of verwijdert de registratie, volgens artikel D.2.4 van de Algemene Voorwaarden, en draagt op verzoek domeinregistraties en DNS-beheer die Opdrachtnemer namens Opdrachtgever voert over;

g) verwijdert of retourneert alle overige gegevens van Opdrachtgever volgens de Verwerkersovereenkomst en verstrekt op verzoek een schriftelijke verklaring van verwijdering die ook de subverwerkers omvat.

5.4 **Medewerking van Opdrachtgever.** Opdrachtgever wijst tijdig een opvolgende leverancier of een eigen beheerder aan, keurt de beheerrelatie van de opvolger goed, zorgt dat de opvolger de Microsoft-transferprocedure start en geeft aan op welk moment de tooling van Opdrachtnemer mag worden verwijderd.

5.5 **Kosten.** De werkzaamheden onder 5.3 onder a, b, d, e (voor zover het de export en beschikbaarstelling van de back-up betreft) en g zijn inbegrepen en worden niet afzonderlijk in rekening gebracht. Voor de back-updienst brengt Opdrachtnemer geen overstapkosten in rekening voor zover de Data Act dat verbiedt; tot 12 januari 2027 kunnen alleen de rechtstreeks met de overstap verbonden kosten worden doorberekend, daarna geen. Een vergoeding voor de resterende looptijd bij voortijdige beëindiging en de gewone dienstvergoeding zijn geen overstapkosten in de zin van de Data Act. De beheervergoeding over de exitperiode wordt naar rato per dag berekend. Overige exitwerkzaamheden (zoals migratie naar een andere omgeving of het inrichten van de omgeving van de opvolger) zijn adviesdiensten die tegen het uurtarief van Bijlage 3 worden verricht na akkoord, tenzij de Overeenkomst is beëindigd wegens een toerekenbare tekortkoming van Opdrachtnemer. Opdrachtnemer mag de werkzaamheden onder 5.3 onder a, b en e nooit opschorten wegens een betalingsachterstand.

5.6 **Doorlopende verplichtingen.** Gedurende de exitperiode blijft de Overeenkomst van toepassing op de nog niet overgedragen onderdelen. De geheimhoudingsverplichtingen en de Verwerkersovereenkomst blijven na de exitperiode van kracht voor zover Opdrachtnemer nog gegevens van Opdrachtgever onder zich heeft.

5.7 **Uniforme verwijdering.** Na afloop van de exitperiode (of, voor de back-updienst, de ophaalperiode als die later eindigt) verwerkt Opdrachtnemer de resterende gegevens van Opdrachtgever uitsluitend voor veilige verwijdering of voor een concreet toepasselijke wettelijke bewaarplicht. Actieve kopieën worden uiterlijk dertig (30) dagen na het einde van de exitperiode verwijderd; resterende back-upkopieën uiterlijk negentig (90) dagen na het einde van dezelfde exitperiode. Tot verwijdering worden deze kopieën afgeschermd en niet voor andere doeleinden gebruikt. Deze termijnen gelden ook voor de subverwerkers; Opdrachtnemer bevestigt de uitvoering schriftelijk op verzoek. Dezelfde regeling staat in artikel 9.2 van de Verwerkersovereenkomst.