OVEREENKOMST MANAGED ICT-SERVICES. 2026040217:00

Stichting ICT Beheer

EN

Opdrachtnemer XXX

Versie: Concept 0.1

Datum: 01 April 2026

Opgesteld door:

PARTIJEN

Stichting ICT Beheer ("SIB"), een stichting naar Nederlands recht, statutair gevestigd te Haarlem, kantoorhoudende aan te 2132 RZ Hoofddorp aan het Raadhuisplein 7, ingeschreven in het Handelsregister onder nummer 83104607, hierbij rechtsgeldig vertegenwoordigd door de heer C.G. Feurich (voorzitter raad van bestuur) en mevrouw R.M.J. Van Acker (directeur), hierna te noemen: "Opdrachtgever";

Hierbij mede handelend namens en ten behoeve van haar beide deelnemende organisaties:
- Bibliotheek Zuid-Kennemerland ("BZK");
- Cpunt ("Cpunt"),

BZK en Cpunt gezamenlijk ook aangeduid als de "Gebruikersorganisaties";

EN

[Naam OpdrachtnemerXXX], een [rechtsvorm] naar Nederlands recht, gevestigd te [adres], ingeschreven in het Handelsregister onder nummer [KvK-nummer], hierbij rechtsgeldig vertegenwoordigd door [naam en functie], hierna te noemen: "Opdrachtnemer";

SIB en XXX hierna gezamenlijk ook te noemen: "Partijen" of elk afzonderlijk "Partij".

PARTIJEN OVERWEGEN ALS VOLGT

A. Opdrachtgever heeft via het Tendernedplatform een Europese openbare aanbestedingsprocedure uitgevoerd voor het verlenen van managed ICT-services ten behoeve van de Gebruikersorganisaties onder kenmerk T..... ;

B. Opdrachtnemer is als winnende inschrijver aangewezen op grond van de beste prijs-kwaliteitverhouding (BPKV) overeenkomstig de aanbestedingsdocumenten);

C. Opdrachtgever beschikt niet over een eigen ICT-afdeling voor de operationele uitvoering van ICT-beheer en wenst de operationele ICT-dienstverlening volledig uit te besteden aan externe leveranciers;

D. Partijen wensen de voorwaarden waaronder de Opdrachtnemer de Managed ICT-services aan Opdrachtgever verleent in deze Overeenkomst vast te leggen, mede met inachtneming van de verplichtingen die voortvloeien uit de Europese NIS2-richtlijn (2022/2555/EU) en de Nederlandse implementatiewetgeving (Cyberbeveiligingswet, Stb. 2025);

E. Partijen ernaar streven gedurende de looptijd van de Overeenkomst de ICT-dienstverlening te verbeteren, de beheerlast van Opdrachtgever te verlagen en toe te groeien naar een meer eenduidige SPOC-structuur;

PARTIJEN ZIJN OVEREENGEKOMEN ALS VOLGT

HOOFDSTUK 1 – DEFINITIES EN INTERPRETATIE

Artikel 1. Definities

In deze Overeenkomst hebben de volgende begrippen de hierna omschreven betekenis:

Aanbestedingsdocumenten De Leidraad, het Programma van Eisen (PvE, Bijlage 11@), de KPI-SLA-structuur (Bijlage 12@), de Kwalificatiegrenzen SWC (Bijlage 13), het Architectuurkader Informatiebeveiliging en Overdraagbaarheid SIB (Bijlage 10) en alle overige bij de aanbesteding behorende bijlagen, zoals nader omschreven in Bijlage 1 bij deze Overeenkomst.

Architectuurkader Het Architectuurkader Informatiebeveiliging en Overdraagbaarheid SIB (Bijlage 10), zoals van tijd tot tijd herzien door Opdrachtgever.

Beheer all-in De reguliere en terugkerende werkzaamheden die noodzakelijk zijn om de ICT-omgeving operationeel, beschikbaar, veilig en actueel te houden, zoals nader omschreven in het PvE.

Beveiligingsbaseline Het bij aanvang vastgestelde normenkader voor beveiligingsmaatregelen binnen de scope van de Opdracht, zoals opgenomen in het Beveiligingsregister.

Contractmanager De door Opdrachtgever aangewezen functionaris die optreedt als primair aanspreekpunt voor de Eindgebruiker namens Opdrachtnemer en bevoegd is werkafspraken, scopewijzigingen en vergoedingen te accorderen.

Deliverables De in het PvE (Bijlage 11) aangeduide documenten, registers, rapportages en andere op te leveren producten (aangeduid als D01 t/m D34), die Opdrachtnemer in de uitvoeringsfase opstelt, oplevert en actueel houdt.

Eindgebruikers/ Gebruikers De medewerkers, vrijwilligers en overige personen die namens de Gebruikersorganisaties gebruik maken van de ICT-voorzieningen binnen de scope van deze Overeenkomst.

Exit by Design Het architectuurprincipe dat vervanging van componenten of leveranciers mogelijk moet zijn zonder fundamenteel herontwerp van het toegangs- en scheidingsmodel, zoals uitgewerkt in het Architectuurkader.

Governance-cadans De periodieke overlegstructuur zoals vastgelegd in D04 – DAP-Governance overlegstructuur, omvattend operationeel, tactisch en strategisch overleg.

ICT-omgeving De gezamenlijke hard- en softwarecomponenten, netwerken, platformen, diensten en applicaties die door Opdrachtnemer worden beheerd binnen de scope van deze Overeenkomst.

Incident Een onverwachte verstoring of vermindering van de kwaliteit van een ICT-dienst, ingedeeld naar prioriteit P1 t/m P4 conform de definities in Bijlage 12.

KPI-SLA De in Bijlage 12 vastgelegde doelen, KPI-normen, minimale eisen en rapportageafspraken.

Levenscyclusvervanging / LCM Het tijdig en gecontroleerd vervangen van componenten binnen de ICT-omgeving in het kader van einde-levensduurondersteuning (EoS/EoL), zonder fundamenteel herontwerp.

Major Incident Een Incident met uitzonderlijk hoge impact op de bedrijfsvoering, meerdere Gebruikers, kritieke diensten of bestuurlijke continuïteit, zoals nader omschreven in Bijlage 12.

Melding Een verzoek om ondersteuning of melding van een verstoring door een Gebruiker of Opdrachtgever aan Opdrachtnemer.

NIS2 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie,

alsmede de Cyberbeveiligingswet (Nederlandse implementatiewet) en daarop gebaseerde regelgeving.

Opdracht De gehele opdracht aan Opdrachtnemer zoals omschreven in deze Overeenkomst en de Aanbestedingsdocumenten.

PAM-systeem Privileged Access Management-systeem: het systeem dat beheerhandelingen via tijdgebonden rechten, minimale privileges en volledige traceerbaarheid faciliteert.

Project Een tijdelijk, doelgericht geheel van samenhangende werkzaamheden met een duidelijk begin en einde, dat vanwege complexiteit, omvang (doorgaans ≥ 16 uur) of organisatorische impact afzonderlijk wordt opgedragen en geoffreerd.

Programma van Eisen/ PvE Bijlage 11 bij deze Overeenkomst, bevattende de contractuele minimumeisen (ME) en bijbehorende Deliverables (Dxx).

Regie De stichtingsbrede sturing op, samenhang van en afstemming binnen de ICT-dienstverlening, zoals nader omschreven in artikel 8.

Security Incident Een Incident met directe en ernstige impact op de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens of systemen, zoals nader omschreven in Bijlage 12.

Standaard Wijziging Een vooraf geautoriseerde, routinematige wijziging, opgenomen in de Standaard Wijzigingen Catalogus (SWC, Bijlage 13).

Takeover De fase waarin Opdrachtnemer de verantwoordelijkheid voor de overeengekomen diensten gecontroleerd overneemt van de zittende ICT-dienstverlener, als bedoeld in artikel 7.

Vaste Beheervergoeding De periodiek verschuldigde vaste vergoeding voor Beheer all-in en regie, zoals vastgelegd in Bijlage 3 (Prijzenblad).

Verwerkersovereenkomst De overeenkomst als bedoeld in artikel 28 AVG, die tussen Partijen wordt gesloten ten aanzien van de verwerking van persoonsgegevens.

Wachtkamerovereenkomst De overeenkomst gesloten met de als tweede gerangschikte inschrijver, die uitsluitend onder de in Bijlage [x] genoemde voorwaarden kan worden geactiveerd.

Artikel 2. Interpretatie documenten

2.1 In geval van tegenstrijdigheid tussen documenten geldt de volgende rangorde waarbij het eerdergenoemde document prioriteit heeft boven het later genoemd:

1. Deze Overeenkomst (de Hoofdovereenkomst);

2. De Nota's van Inlichtingen;

3. De Verwerkersovereenkomst d.d. pm...;

4. Het Programma van Eisen (bijlage 11 Leidraad);

5. De KPI-SLA-structuur (bijlage 12 Leidraad);

6. Architectuurkader Informatiebeveiliging en Overdraagbaarheid (bijlage 10 Leidraad);

7. Prijzenblad d.d. ....pm ... zoals ingediend door Opdrachtnemer;

8. DFA meest updated versie;

9. Kwalificatiegrenzen SWC (bijlage 13 leidraad);

10. Inschrijving/offerte van Opdrachtnemer

11. Gibit 2025 en Toelichting op de Gibit 2025 (bijlage 8a en 8b Leidraad);

12. De Leidraad;

13. Wachtkamerovereenkomst.

2.2 Bijlagen maken integraal onderdeel uit van deze Overeenkomst. Bij tegenstrijdigheid tussen de Hoofdovereenkomst en een Bijlage prevaleert de Hoofdovereenkomst, tenzij in de betreffende Bijlage uitdrukkelijk anders is bepaald.

HOOFDSTUK 2 – LOOPTIJD EN VERLENGING

Artikel 3. Ingangsdatum en looptijd

3.1 Deze Overeenkomst treedt in werking op [datum] ("Ingangsdatum") en kent een initiële vaste periode van drie (3) jaar, derhalve tot en met [datum + 3 jaar].

3.2 Opdrachtgever heeft de mogelijkheid de Overeenkomst éénzijdig te verlengen met maximaal vier (4) maal één (1) jaar, zulks op grond van een schriftelijke kennisgeving uiterlijk drie (3) maanden vóór het einde van de dan lopende periode.

3.3 De maximale totale looptijd van de Overeenkomst bedraagt zeven (7) jaar.

3.4 De beslissing tot verlenging wordt door Opdrachtgever genomen op basis van:

- de resultaten van de periodieke prestatie-evaluaties conform artikel 14;

- relevante marktontwikkelingen;

- wijzigingen in wet- en regelgeving, waaronder NIS2-verplichtingen.

3.5 Opdrachtgever is niet gehouden tot verlenging. Opdrachtnemer kan aan de mogelijkheid tot verlenging geen rechten ontlenen.

HOOFDSTUK 3 – SCOPE EN DIENSTVERLENING

Artikel 4. Scope van de Opdracht

4.1 De Opdracht omvat het Beheer all-in van de bestaande ICT-omgeving van Opdrachtgever, gericht op het in stand houden van functionaliteit, continuïteit, beheerbaarheid en beveiliging, de afstemming hierover met Opdrachtgever en het ondersteunen van Gebruikers binnen de overeengekomen scope. Printing en Microsoft 365 back-up maken functioneel onderdeel uit van de dienstverlening.

4.2 De dienstverlening kent drie onderling samenhangende lagen:

- Operationele laag: dagelijks beheer, afhandeling van Meldingen, incidentmanagement, changemanagement en netwerkbeheer;

- Proactieve laag: ontzorging, ketenafstemming, signalering, trendanalyse en proactieve verbetersturing;

- Sturende laag: regie- en governancestructuur, periodieke evaluatie en bijsturing.

4.3 Opdrachtnemer verricht geen activiteiten gericht op het ontwerpen, ontwikkelen, vernieuwen of herontwikkelen van applicaties of functionaliteit op applicatieniveau. Dergelijke activiteiten maken geen onderdeel uit van deze Opdracht, tenzij dit uitdrukkelijk schriftelijk is overeengekomen als afzonderlijk Project.

4.4 De Aanbestedende dienst behoudt de functionele regie over de functionele aansturing en prioritering (wat/wanneer) en voert contractmanagement. De Opdrachtnemer heeft de operationele regie over de uitvoering binnen het eigen domein.

4.5 Levenscyclusvervangingen (LCM) van onderdelen van de ICT-omgeving worden aangemerkt als onderdeel van Beheer all-in en vallen binnen de scope van deze Opdracht, mits zij geen fundamentele herontwerpopdracht betreffen.

4.6 Voorbehoud toekomstige platformwijziging: Opdrachtgever behoudt zich het recht voor om bij wezenlijke wijzigingen van: wet- en regelgeving, security-beleid of data-soevereiniteit de lopende Overeenkomst gedeeltelijk te beëindigen en een deel van de dienstverlening opnieuw aan te besteden. Opdrachtnemer dient bij dergelijke omstandigheden proactief mee te denken en de overdraagbaarheid te faciliteren.

Artikel 5. Meldingen en aanspreekpuntstructuur

5.1 Opdrachtgever hanteert bij aanvang van de Overeenkomst een meervoudige aanspreekpuntstructuur: Gebruikers kunnen Meldingen zowel richten aan het interne aanspreekpunt van Opdrachtgever als rechtstreeks aan Opdrachtnemer.

5.2 Opdrachtnemer is binnen zijn eigen domein verantwoordelijk voor adequate intake, opvolging, afstemming en terugkoppeling van Meldingen conform de KPI-SLA.

5.3 Per Melding is te allen tijde één eigenaar aangewezen (single owner-principe). Opdrachtnemer borgt dat richting de melder eenduidige statusinformatie wordt verstrekt.

5.4 Partijen werken gedurende de looptijd van de Overeenkomst toe naar een meer eenduidige SPOC-structuur. De voortgang hierop wordt periodiek beoordeeld in de Governance-cadans.

5.5 De startafspraken over intake, registratie, triage, routering en terugkoppeling worden door Opdrachtnemer uiterlijk in week 6–10 na de Ingangsdatum opgeleverd (D01 en D02).

Artikel 6. Ontzorging

6.1 Opdrachtnemer is gehouden Opdrachtgever en haar Gebruikers aantoonbaar te ontzorgen. Ontzorging omvat ten minste:

a) afhandeling van Meldingen met passende doorlooptijd, duidelijke terugkoppeling en minimale impact op Gebruikers;

b) voorkomen van herhaalverstoringen door structurele analyse (probleemmanagement, RCA) en doorvoering van verbetermaatregelen;

c) proactieve signalering en opvolging (monitoring, trendanalyse, verbetervoorstellen) zodat verstoringen waar mogelijk vóór gebruikersimpact worden onderkend of verholpen;

d) regievoering richting Derden en Ketenleveranciers, zodat Opdrachtgever niet als doorgeefluik hoeft te fungeren;

e) remote ondersteuning waar passend, aangevuld met on-site inzet waar noodzakelijk, met een aantoonbare en overdraagbare werkwijze;

f) vergroten van de autonomie van Gebruikers door inzet van toegankelijke self-service faciliteiten en een actuele kennisbank.

6.2 Opdrachtnemer signaleert tijdig relevante ontwikkelingen die invloed kunnen hebben op de continuïteit, beveiliging, beheerbaarheid en ondersteuning van de ICT-omgeving en brengt deze signalering in ieder geval in tijdens de periodieke Governance-cadans.

HOOFDSTUK 4 – TAKEOVER EN TRANSITIE

Artikel 7. Takeover

7.1 De Opdracht vangt aan met een Takeover: het gecontroleerd overnemen van het Beheer all-in van de bestaande ICT-omgeving door Opdrachtnemer, op basis van as-is beheer.

7.2 De Takeover start op de Ingangsdatum en dient uiterlijk drie (3) maanden na de Ingangsdatum te zijn afgerond. De Takeover eindigt met een formele schriftelijke Transitie-acceptatie door Opdrachtgever.

7.3 De Takeover omvat:

a) overdracht en/of inrichting van de voor de dienstverlening noodzakelijke kennis, documentatie en configuratiegegevens;

b) inrichting van toegangs-, autorisatie- en beheerpaden;

c) inrichting van logging- en monitoringvoorzieningen;

d) overnemen van lopende tickets en changes binnen scope;

e) uitvoering van een initiële risicorapportage (binnen 2 weken) en een geactualiseerde risicorapportage (binnen 8 weken), beide conform D15.

7.4 Gedurende de Takeover geldt een change-freeze conform de regeling in D10, tenzij sprake is van een security- of continuïteitsnoodgeval, te accorderen door de Contractmanager van Opdrachtgever.

7.5 De kosten van de Takeover zijn inbegrepen in de aanbiedingsprijs conform Bijlage 3, tenzij schriftelijk anders overeengekomen.

HOOFDSTUK 5 – REGIE EN GOVERNANCE

Artikel 8. Regie en governance

8.1 Regie omvat de stichtingsbrede sturing op, samenhang van en afstemming binnen de ICT-dienstverlening. Regie betreft niet de uitvoering van reguliere beheertaken, maar omvat:

a) coördinatie van de operationele dienstverlening op keten- en stichtingsniveau;

b) afstemming tussen Opdrachtgever, Opdrachtnemer, interne aanspreekpunten, Derden en relevante Ketenleveranciers;

c) bewaking van opvolging, eigenaarschap en terugkoppeling bij Meldingen en verstoringen die meerdere partijen raken.

8.2 Opdrachtnemer draagt actief bij aan de uitvoering van de regie- en ontzorgingsdoelstellingen. Dit is een resultaatgerichte verplichting, niet uitsluitend een inspanningsverplichting.

8.3 De Governance-cadans omvat minimaal:

- Operationeel overleg: maandelijks (KPI-rapportage en incidentbespreking);

- Tactisch overleg: kwartaals (deliverableset, lifecycle, verbetercyclus);

- Strategisch overleg: jaarlijks (toekomstbestendigheid, NIS2-compliance, SLA-herijking).

8.4 Indien een kwestie het tactisch-operationeel niveau overstijgt, hanteren Partijen een escalatiepad naar directieniveau. Dit escalatiepad houdt in dat de verantwoordelijk directeur of gemachtigde vertegenwoordiger van Opdrachtgever en de accountverantwoordelijke van Opdrachtnemer gezamenlijk binnen 15 werkdagen na escalatie overleg voeren.

8.5 Opdrachtgever wijst bij aanvang van de Overeenkomst een Contractmanager aan als primair aanspreekpunt. Het mandaat en de contactgegevens van de Contractmanager worden uiterlijk op de Ingangsdatum verstrekt en opgenomen in D04.

HOOFDSTUK 6 – PRESTATIES, KPI'S EN SLA

Artikel 9. Prestatieverplichtingen

9.1 Opdrachtnemer is verplicht de dienstverlening te leveren conform de in Bijlage 12 (KPI-SLA) vastgelegde doelen, KPI-normen en minimale eisen.

9.2 De door Opdrachtnemer bij inschrijving opgegeven normen (leveranciersnormen) gelden na gunning als contractuele referentie gedurende de volledige contractperiode.

9.3 De volgende minimale prestatie-eisen gelden in ieder geval als contractuele verplichtingen:

| KPI | Norm |

A Beschikbaarheid servicedesk (binnen servicevenster) | ≥ 99,5%

B First response P1 | ≤ 15 min (95% van de gevallen)

C First response P2 | ≤ 1 uur (95% van de gevallen)

D Oplostijd P1 – stabilisatie / definitieve oplossing | ≤ 4 uur / ≤ 48 uur

E Oplostijd P2 | ≤ 8 werkuren (95%)

F Time-to-containment Security Incident P1 / P2 | ≤ 4 uur / ≤ 24 uur

G Piketstand (P1, buiten servicevenster) | 24/7 beschikbaar

H Patch compliance beheerde omgeving | ≥ 90%

I Device compliance (Conditional Access, Entra ID) | ≥ 95%

J Kwetsbaarheden CVSS ≥ 8: mitigatie | 100% binnen 14 kalenderdagen

K Beschikbaarheid netwerkinfrastructuur per locatie | ≥ 99,0% (minimumeis)

L Beschikbaarheid M365-kernservices (in invloedssfeer ON) | ≥ 99,5%

M Back-up compliance/ jaarlijkse restoretest | ≥ 99% / 1x per jaar

N Overdrachtsset documentatie actueel | 100% binnen 20 werkdagen na wijziging

9.4 Wijziging van KPI-normen vereist schriftelijke instemming van beide Partijen via de Governance-cadans, gaat in per kwartaalgrens en wordt gedocumenteerd in het contractdossier.

Artikel 10. Malus en escalatie bij KPI-afwijking

10.1 Bij structurele afwijking van één of meer KPI-normen (gedurende twee achtereenvolgende rapportageperioden of drie perioden binnen twaalf maanden) is Opdrachtnemer verplicht:

a) binnen 10 werkdagen een verbeterplan op te stellen met concrete maatregelen, mijlpalen en verantwoordelijken;

b) het verbeterplan ter goedkeuring voor te leggen aan de Contractmanager van Opdrachtgever;

c) rapportage over de voortgang van het verbeterplan op te nemen in de maandelijkse KPI-rapportage.

10.2 Indien een KPI tevens een minimale contracteis betreft en niet aan deze eis wordt voldaan, is sprake van een tekortkoming in de nakoming. Opdrachtgever is in dat geval gerechtigd:

a) een malus te vorderen ter hoogte van [3% /bedrag in te vullen door Partijen, maximaal 10% van de maandelijkse Vaste Beheervergoeding per aaneengesloten periode van niet-nakoming];

b) te escaleren naar directieniveau conform artikel 8.4;

c) bij voortdurende tekortkoming (> drie maanden) de Overeenkomst (gedeeltelijk) te ontbinden conform artikel 23.

10.3 De malus als bedoeld in lid 2 sub a) laat overige rechtsmiddelen, waaronder ontbinding en schadevergoeding, onverlet.

HOOFDSTUK 7 – INFORMATIEBEVEILIGING EN NIS2-COMPLIANCE

Artikel 11. Informatiebeveiliging – algemeen

11.1 Opdrachtnemer is verplicht de ICT-omgeving te beheren conform de Beveiligingsbaseline die bij aanvang van de Overeenkomst wordt vastgesteld (D26 – Beveiligingsregister Baseline), aangevuld met de beveiligingsarchitectuurprincipes uit het Architectuurkader (Bijlage 10).

11.2 De beveiligingsmaatregelen omvatten ten minste:

a) identity-, endpoint- en netwerkbeveiliging conform de gangbare normen;

b) tijdige opvolging van Security Incidenten;

c) e-mailbeveiliging (anti-phishing, anti-spam, DMARC/DKIM/SPF) en beveiligingsgerelateerde DNS-instellingen, voor zover in scope;

d) Zero Trust/ identity-first benadering: expliciete toegang op basis van identiteit, context en device-posture (Conditional Access), least privilege, herleidbare beheerhandelingen en impactbeperking.

11.3 Opdrachtnemer levert binnen 8 weken na contractstart een Beveiligingsroadmap (D28) op, gebaseerd op een gap-analyse ten opzichte van de vastgestelde Beveiligingsbaseline, georiënteerd op NIS2 en BIO2. De roadmap bevat concrete aanbevolen maatregelen buiten de standaarddienstverlening, met mijlpalen, afhankelijkheden en besluitpunten voor Opdrachtgever. Een visiedocument zonder planning volstaat niet.

11.4 De Beveiligingsroadmap wordt minimaal jaarlijks herzien, of vaker wanneer de baseline, de NIS2/BIO2-oriëntatie of externe ontwikkelingen daartoe aanleiding geven.

Artikel 12. NIS2-compliance

12.1 Toepasselijkheid en zorgplicht. Partijen erkennen dat SIB als entiteit die gebruik maakt van kritieke ICT-diensten valt onder de werkingssfeer van NIS2-gerelateerde verplichtingen. Opdrachtnemer treedt op als beheerder-dienstverlener (Managed Service Provider) en is als zodanig verplicht passende technische en organisatorische maatregelen te treffen ter beheersing van de risico's voor de beveiliging van de netwerk- en informatiesystemen.

12.2 Risicobeheersmaatregelen. Opdrachtnemer implementeert en handhaaft, als minimum, de volgende maatregelen zoals vereist door artikel 21 NIS2-richtlijn en de Cyberbeveiligingswet:

a) Beleid inzake risicoanalyse en beveiliging van informatiesystemen: Opdrachtnemer voert minimaal jaarlijks een risicoanalyse uit en legt de resultaten vast in D28;

b) Incidentbehandeling: Opdrachtnemer beschikt over een gedocumenteerde procedure voor detectie, beheersing, melding en herstel van beveiligingsincidenten (D08, D09);

c) Bedrijfscontinuïteit en crisisbeheer: Opdrachtnemer beschikt over een actueel continuïteitsplan, inclusief back-up, herstelmaatregelen en uitwijkprocedures conform D29 en Bijlage 10, Hoofdstuk 7;

d) Beveiliging van de toeleveringsketen: Opdrachtnemer beoordeelt en beheert de risico's van zijn sub-leveranciers en sub-verwerkers die betrokken zijn bij de levering van de diensten. Voor kritieke beheerplatformen geldt de verplichting uit de Geschiktheidseisen (ISO 27001 of gelijkwaardige assurance). Opdrachtnemer verstrekt op verzoek een overzicht van kritieke sub-leveranciers en de op hen van toepassing zijnde beveiligingscertificeringen;

e) Beveiliging bij verwerving, ontwikkeling en onderhoud: Opdrachtnemer past lifecycle management (LCM), patchbeheer en kwetsbaarheidsbeheer toe conform de KPI-normen in artikel 9.3;

f) Beleid en procedures inzake het gebruik van cryptografie: Opdrachtnemer versleutelt communicatie over onvertrouwde netwerken conform actuele normen zoals vastgesteld in een erkend nationaal of Europees referentiekader (Bijlage 10, artikel 4.5);

g) Beveiligd personeelsbeheer en toegangscontrole: Opdrachtnemer hanteert least privilege, minimale privileges, tijdgebonden rechten en periodieke review van kritieke beheerrechten via het PAM-systeem (D18);

h) Multi-factor authenticatie: Opdrachtnemer past meervoudige verificatie (MFA) toe voor alle beheerhandelingen en toegang tot gegevensgevoelige diensten;

i) Fysieke beveiliging: Opdrachtnemer treft passende maatregelen voor de fysieke beveiliging van systemen en installaties die onderdeel uitmaken van de scope.

12.3 Meldplicht beveiligingsincidenten. Opdrachtnemer is verplicht:

a) beveiligingsincidenten die (mogelijk) significante impact hebben op de dienstverlening of op de netwerk- en informatiesystemen van Opdrachtgever onverwijld – en in ieder geval binnen 24 uur na ontdekking – te melden aan de Contractmanager van Opdrachtgever;

b) binnen 72 uur na ontdekking een voorlopige notificatie te verstrekken aan Opdrachtgever met de (voorlopige) aard van het incident, de getroffen systemen en de reeds genomen maatregelen;

c) Opdrachtgever te ondersteunen bij de nakoming van eventuele wettelijke meldplichten jegens het CSIRT-NL en/of de Autoriteit Persoonsgegevens (bij datalekken), inclusief het tijdig verstrekken van de benodigde technische informatie.

12.4 Audit- en inspectierecht (NIS2). Opdrachtgever en bevoegde toezichthouders hebben het recht om, na voorafgaande kennisgeving van minimaal 5 werkdagen (behoudens spoedsituaties), de naleving van de beveiligingsvereisten bij Opdrachtnemer te controleren. Opdrachtnemer werkt volledig mee aan dergelijke audits, verstrekt tijdig alle gevraagde documentatie en informatie, en draagt de kosten van zijn eigen medewerking. De kosten van externe auditors zijn voor rekening van Opdrachtgever, tenzij uit de audit een materiële tekortkoming van Opdrachtnemer blijkt; in dat geval zijn de kosten voor rekening van Opdrachtnemer.

12.5 Beveiliging van de toeleveringsketen – contractuele doorwerking. Opdrachtnemer is verplicht met zijn sub-leveranciers en sub-verwerkers die betrokken zijn bij de levering van de dienstverlening contractuele afspraken te maken die ten minste gelijkwaardig zijn aan de in dit artikel 12 opgenomen beveiligingsvereisten. Opdrachtnemer verstrekt Opdrachtgever op eerste verzoek een actueel overzicht van de gehanteerde contractuele beveiligingsbepalingen jegens sub-leveranciers.

12.6 Jurisdictierisico. Bij de inzet van sub-leveranciers en sub-verwerkers houdt Opdrachtnemer rekening met het jurisdictierisico als bedoeld in Bijlage 10 (principe 9). Bij gelijkwaardige alternatieven heeft een leverancier onder Europese jurisdictie met data-opslag in Nederland of de EU de voorkeur.

12.7 Wijzigingen in wet- en regelgeving. Partijen overleggen over de gevolgen van materiële wijzigingen in NIS2-gerelateerde wet- en regelgeving voor de uitvoering van deze Overeenkomst. Indien aanpassing van de dienstverlening noodzakelijk is, worden de consequenties hiervan, waaronder eventuele kosten, in onderling overleg via de Governance-cadans afgestemd.

Artikel 13. Architectuurkader – referentiekader en Exit by Design

13.1 Opdrachtnemer betrekt het Architectuurkader Informatiebeveiliging en Overdraagbaarheid SIB (Bijlage 10) realistisch bij de uitvoering van beheeractiviteiten binnen zijn domein, met name bij wijzigingen, uitzonderingen en Levenscyclusvervangingen.

13.2 Afwijkingen van het Architectuurkader zijn toegestaan, mits vooraf door beide Partijen schriftelijk vastgelegd in het Uitzonderingenregister (D07), met vermelding van

reden, scope, geïntroduceerd risico, compenserende maatregel, eigenaar en beoogde einddatum.

13.3 Opdrachtnemer past Exit by Design-principes toe gedurende de gehele looptijd van de Overeenkomst. Dit omvat ten minste:

a) gebruik van open standaarden voor authenticatie (SAML, OIDC) en provisioning (SCIM);

b) standaardexportformaten voor data-opslag;

c) exporteerbare logs in gangbare formaten (Syslog, CEF);

d) overdraagbare toegangsregels en policies.

13.4 Opdrachtnemer levert jaarlijks een beknopte signaleringsnotitie op (D32 – DAP-Aanpak Exit-by-design) als input voor de herijking van het Architectuurkader door Opdrachtgever.

HOOFDSTUK 8 – VERGOEDINGEN EN INDEXERING

Artikel 14. Vaste Beheervergoeding

14.1 Opdrachtgever is aan Opdrachtnemer een Vaste Beheervergoeding verschuldigd voor het leveren van Beheer all-in en regie, zoals gespecificeerd in Bijlage 3 (Prijzenblad).

14.2 De Vaste Beheervergoeding wordt maandelijks gefactureerd en is verschuldigd 30 dagen na ontvangst van een deugdelijke factuur.

14.3 De Vaste Beheervergoeding is gebaseerd op de in Bijlage 3 opgenomen referentievolumes. Afwijkingen van meer dan 20% van het referentievolume leiden tot aanpassing van de vergoeding overeenkomstig de variabele tarieven in Bijlage 3.

Artikel 15. Variabele tarieven en Projectvergoedingen

15.1 Voor werkzaamheden buiten de reguliere dienstverlening, waaronder Projecten en Niet-standaard Wijzigingen, gelden de in Bijlage 3 opgenomen uurtarieven en projecttarieven.

15.2 Projecten worden uitsluitend uitgevoerd na schriftelijke opdrachtverstrekking door de Contractmanager van Opdrachtgever, met vermelding van scope, resultaat, planning en maximaal budget.

15.3 Opdrachtnemer brengt geen kosten in rekening die niet zijn opgenomen in Bijlage 3. Opdrachtgever accepteert geen andere kosten dan vermeld in het Prijzenblad.

Artikel 16. Indexering

16.1 De Vaste Beheervergoeding en de tarieven in Bijlage 3 worden jaarlijks per 1 januari geïndexeerd op basis van de CBS-index Cao-lonen commerciële dienstverlening (of een daarvoor in de plaats tredende index), voor het eerst per [datum].

16.2 Indexering wordt door Opdrachtnemer uiterlijk 60 dagen voor de ingangsdatum schriftelijk medegedeeld aan de Contractmanager, met onderbouwing op basis van de toepasselijke index.

HOOFDSTUK 9 – INTELLECTUEEL EIGENDOM EN GEGEVENSBESCHERMING

Artikel 17. Intellectueel eigendom

17.1 Alle intellectuele eigendomsrechten op de door Opdrachtnemer in het kader van deze Overeenkomst tot stand gebrachte werken, documentatie, configuraties, rapportages en andere Deliverables die specifiek voor Opdrachtgever zijn ontwikkeld, berusten bij Opdrachtgever, tenzij Partijen schriftelijk anders overeenkomen.

17.2 Voor zover intellectuele eigendomsrechten op grond van de wet bij Opdrachtnemer berusten, verleent Opdrachtnemer hierbij aan Opdrachtgever een eeuwigdurende, onherroepelijke, royaltyvrije licentie voor gebruik binnen de organisatie.

17.3 Opdrachtnemer draagt er zorg voor dat de Deliverables en de ICT-omgeving geen inbreuk maken op intellectuele eigendomsrechten van derden.

Artikel 18. Gegevensbescherming

18.1 In het kader van de uitvoering van deze Overeenkomst verwerkt Opdrachtnemer persoonsgegevens ten behoeve van Opdrachtgever. Partijen sluiten ter zake een Verwerkersovereenkomst als bedoeld in artikel 28 AVG, welke als Bijlage [x] aan deze Overeenkomst is gehecht.

18.2 Opdrachtnemer verwerkt persoonsgegevens uitsluitend conform de instructies van Opdrachtgever en niet voor eigen doeleinden.

18.3 Opdrachtnemer treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, mede ter voldoening aan artikel 32 AVG.

18.4 Bij een datalek als bedoeld in artikel 4 lid 12 AVG informeert Opdrachtnemer Opdrachtgever onverwijld en uiterlijk binnen 24 uur na ontdekking.

HOOFDSTUK 10 – CERTIFICERING EN VERZEKERING

Artikel 19. Certificering

19.1 Opdrachtnemer beschikt gedurende de gehele looptijd van de Overeenkomst over:

a) een geldig ISO/IEC 27001-certificaat of daarmee gelijkwaardige onafhankelijke assurance (SOC 2 Type II en/of ISAE 3402 Type II), passend bij de betreffende dienst en scope;

b) OPTIE indien aangeboden een geldig ISO 9001:2015 -certificaat of een aantoonbaar gelijkwaardig kwaliteitsmanagementsysteem.

19.2 Opdrachtnemer overlegt op verzoek van Opdrachtgever kopieën van de geldige certificaten, inclusief het bijbehorende scope statement.

19.3 Voor kritieke beheerplatformen van sub-leveranciers geldt een overeenkomstige verplichting tot het aantonen van adequate assurance.

19.4 Indien een certificaat vervalt of wordt ingetrokken, stelt Opdrachtnemer Opdrachtgever daarvan onverwijld in kennis en presenteert hij binnen 10 werkdagen een herstelplan.

Artikel 20. Verzekering

20.1 Opdrachtnemer handhaaft gedurende de gehele looptijd van de Overeenkomst een adequate bedrijfs- of beroepsaansprakelijkheidsverzekering (BAV) met een dekking inclusief cybersecurityclausule van minimaal € 1.500.000 per gebeurtenis en € 3.000.000 per jaar.

20.2 Opdrachtnemer overlegt op eerste verzoek een actueel verzekeringsoverzicht of -certificaat.

HOOFDSTUK 11 – AANSPRAKELIJKHEID

Artikel 21. Aansprakelijkheid

21.1 Opdrachtnemer is aansprakelijk voor schade die Opdrachtgever lijdt als gevolg van een toerekenbare tekortkoming in de nakoming van de verplichtingen uit deze Overeenkomst.

21.2 De totale aansprakelijkheid van Opdrachtnemer voor directe schade is per schadegeval beperkt tot de door Opdrachtnemer in de twaalf maanden voorafgaande aan het schadeveroorzakende voorval gefactureerde Vaste Beheervergoeding. De totale

aansprakelijkheid over de gehele contractperiode is beperkt tot tweemaal de jaarlijkse Vaste Beheervergoeding.

21.3 Aansprakelijkheid voor indirecte schade, gevolgschade, gederfde winst en gemiste besparingen is uitgesloten, behalve in geval van opzet of bewuste roekeloosheid van Opdrachtnemer of zijn leidinggevenden.

21.4 De beperkingen in de leden 2 en 3 gelden niet bij:

a) overtreding van de NIS2-meldplicht als bedoeld in artikel 12.3;

b) opzettelijke of bewust roekeloze schending van beveiligingsverplichtingen;

c) schending van de geheimhoudingsverplichting (artikel 22);

d) inbreuk op intellectuele eigendomsrechten (artikel 17).

HOOFDSTUK 12 – GEHEIMHOUDING

Artikel 22. Geheimhouding

22.1 Partijen behandelen alle informatie die zij in het kader van de uitvoering van deze Overeenkomst over en weer ontvangen als strikt vertrouwelijk, voorzover deze informatie als vertrouwelijk is aangeduid of redelijkerwijs als zodanig moet worden beschouwd.

22.2 Partijen maken vertrouwelijke informatie uitsluitend bekend aan medewerkers en sub-leveranciers voor zover dit noodzakelijk is voor de uitvoering van de Overeenkomst, en uitsluitend nadat deze personen aan een gelijkwaardige geheimhoudingsverplichting zijn gebonden.

22.3 De geheimhoudingsverplichting geldt tijdens de looptijd van de Overeenkomst en gedurende vijf (5) jaar na beëindiging daarvan.

HOOFDSTUK 13 – OVERDRAAGBAARHEID EN EXIT

Artikel 23. Exit-verplichtingen

23.1 Opdrachtnemer past gedurende de gehele looptijd Exit by Design-principes toe en levert jaarlijks een signaleringsnotitie op (D32).

23.2 Bij beëindiging van de Overeenkomst (om welke reden dan ook) is Opdrachtnemer verplicht:

a) volledig medewerking te verlenen aan een beheerste overdracht aan de opvolgende leverancier of aan Opdrachtgever zelf;

b) de volledige Overdrachtset op te leveren (D33 – Overdrachtset Exit), omvattende alle exports, configuratieoverzichten, log-auditextracten (conform bewaartermijnen en reconstructiebehoefte), toegangs- en autorisatieoverzichten, en openstaande tickets met cut-off afspraken;

c) één tot twee overdrachtsworkshops te verzorgen, gericht op toelichting en kennisoverdracht ten behoeve van de opvolgende leverancier of Opdrachtgever;

d) gedurende een exitperiode van maximaal zes (6) maanden na beëindiging actief medewerking te verlenen aan de overdracht, op basis van de dan geldende tarieven in Bijlage 3.

23.3 Opdrachtnemer stelt bij beëindiging alle data, configuraties, logs en documentatie ter beschikking in een open, gangbaar formaat, vrij van proprietary afhankelijkheden, zodat verdere verwerking door Opdrachtgever of zijn opvolgende leverancier zonder Opdrachtnemer mogelijk is.

23.4 De exitverplichtingen als bedoeld in dit artikel zijn resultaatsverplichtingen.

HOOFDSTUK 14 – WIJZIGING, OPZEGGING, ONTBINDING EN BEËINDIGING

Artikel 24. Wijziging van de Overeenkomst

24.1 Wijzigingen van de Overeenkomst zijn uitsluitend geldig indien deze schriftelijk zijn overeengekomen en door beide Partijen zijn ondertekend.

24.2 Opdrachtnemer is niet gerechtigd de uitvoering van de Overeenkomst eenzijdig te wijzigen.

24.3 Wezenlijke wijzigingen van de Opdracht, die aanbestedingsrechtelijk kwalificeren als een wezenlijke wijziging in de zin van artikel 2.163b Aanbestedingswet 2012, kunnen uitsluitend worden doorgevoerd na een nieuwe aanbestedingsprocedure.

Artikel 25. Opzegging

25.1 Opdrachtgever is gerechtigd de Overeenkomst zonder rechterlijke tussenkomst op te zeggen met inachtneming van een opzegtermijn van zes (6) maanden, met dien verstande dat:

a) gedurende de initiële vaste periode van drie (3) jaar geen opzegging kan plaatsvinden, tenzij sprake is van een zwaarwegende grond als bedoeld in lid 2 dan wel Opdrachtnemer voor een achtereenvolgende periode 2 of meer KPI’s niet heeft behaald ondanks daartoe door Opdrachtgever te zijn aangemaand;

b) na de initiële periode opzegging per het einde van een verlengingsjaar kan plaatsvinden.

25.2 Opzegging wegens zwaarwegende gronden is te allen tijde mogelijk bij:

a) voortdurende ernstige tekortkoming in de nakoming van NIS2-beveiligingsverplichtingen;

b) faillissement, surseance van betaling of ontbinding van Opdrachtnemer;

c) het intrekken van een voor de uitvoering van de Overeenkomst vereist certificaat (artikel 19);

d) schending van de geheimhoudingsverplichting met significante impact.

25.3 Bij tussentijdse beëindiging in het eerste initiële contractjaar is Opdrachtgever gerechtigd gebruik te maken van de Wachtkamerconstructie conform de daarvoor geldende bijlage.

Artikel 26. Ontbinding

26.1 Ieder der Partijen is gerechtigd de Overeenkomst geheel of gedeeltelijk te ontbinden indien de andere Partij, na schriftelijke ingebrekestelling met een redelijke hersteltermijn van minimaal 10 werkdagen (of korter bij spoedsituaties die continuïteit of veiligheid in gevaar brengen), tekortschiet in de nakoming van haar verplichtingen.

26.2 Ontbinding laat het recht op schadevergoeding onverlet.

HOOFDSTUK 15 – SLOTBEPALINGEN

Artikel 27. Toepasselijk recht en forumkeuze

27.1 Op deze Overeenkomst is uitsluitend Nederlands recht van toepassing.

27.2 Alle geschillen die voortvloeien uit of verband houden met deze Overeenkomst worden bij uitsluiting voorgelegd aan de Rechtbank Noord-Holland, zittingsplaats Haarlem.

27.3 Alvorens een geschil aan de rechter voor te leggen, treden Partijen in overleg om het geschil in der minne te schikken, met inachtneming van de escalatieprocedure als bedoeld in artikel 8.4. Dit overleg duurt maximaal 30 dagen tenzij Partijen een kortere of langere termijn overeenkomen.

Artikel 29. Overige bepalingen

29.1 Volledige overeenkomst. Deze Overeenkomst inclusief bijlagen vormt de volledige overeenkomst tussen Partijen met betrekking tot het onderwerp hiervan en treedt in de plaats van alle eerdere afspraken, correspondentie en onderhandelingen.

29.2 Deelbaarheid. Indien een bepaling van deze Overeenkomst nietig of vernietigbaar is, tast dit de geldigheid van de overige bepalingen niet aan. Partijen zullen de nietige of vernietigde bepaling vervangen door een geldige bepaling met een zo gelijkluidende strekking als rechtens mogelijk.

29.3 Afstand van recht. Het niet uitoefenen van een recht door een Partij houdt geen afstand van dat recht in.

29.4 Overdracht. Opdrachtnemer is niet gerechtigd rechten en verplichtingen uit deze Overeenkomst zonder voorafgaande schriftelijke toestemming van Opdrachtgever over te dragen aan derden.

29.5 Publicatiebepaling. Opdrachtgever is gerechtigd de gunningsbeslissing en de essentiële contractgegevens openbaar te maken conform de verplichtingen van de Aanbestedingswet 2012.

ONDERTEKENING

Aldus overeengekomen en in tweevoud ondertekend te [plaats], op [datum].

Te op 2026	Te op, 2026
Opdrachtgever	Opdrachtnemer
Stichting ICT Beheer	XXXX
_____	_____
Naam	Naam
Functie	Functie