Bijlage A:
Programma van Eisen

Onderwerp	Auteur	Datum	Versie
Aanbestedingen MSP MSSP	GGD GHOR NL	06-06-2026	1.0

In dit document wordt GGD GHOR Nederland afgekort met '**GGN**'.

Algemene Eisen

1. Opdrachtnemer levert al haar diensten en documentatie in de Nederlandse taal, in woord en geschrift, tenzij daar per geval andere afspraken over worden gemaakt met de Opdrachtgever.

2. Opdrachtnemer levert professionele en in hoge mate gestandaardiseerde Managed Services.

3. Opdrachtnemer levert professionele en in hoge mate gestandaardiseerde Managed Security Services.

4. Opdrachtnemer houdt uit oogpunt van de administratieve organisatie een strikte scheiding aan tussen afdelingen en/ of teams die Managed Services leveren en afdelingen en/ of teams die Managed Security Services leveren.

5. Opdrachtnemer garandeert dat voor het beheer van de Managed Services en Managed Security Services te allen tijde gebruik wordt gemaakt van beheeraccounts waarvoor de rechten middels Privileged Identity Management (PIM) worden uitgegeven, beheerd en gelogd.

6. Opdrachtnemer garandeert dat alle data/ gegevens/ informatie die gepaard gaan met het leveren van- of ontstaan door het leveren van Managed Services en Managed Security Services te allen tijde worden bewaard binnen de EER.

7. Opdrachtnemer gaat akkoord met de inhoudelijke eisen met betrekking tot de verwerkingen van de persoonsgegevens zoals zijn opgenomen in **Bijlage C – Standaard (sub)Verwerkersovereenkomst**.

8. Opdrachtnemer zal bij de uitvoering van de werkzaamheden voor Opdrachtgever nooit meer persoonsgegevens verwerken dan strikt noodzakelijk.

9. Opdrachtnemer houdt zich aantoonbaar aan de definitief vastgestelde en van toepassing zijnde wetten, kaders en normen.

10. Opdrachtnemer heeft aantoonbaar voorzieningen (organisatorisch/ technisch/ juridisch) waarmee enige inbreuk/ schending van datasoevereiniteit kan worden voorkomen/ bestreden/ vertraagd/ aangevochten.

11. Opdrachtnemer richt de Managed Services processen en de Managed Security Services processen in hetzij met gebruikmaking van de GGN-eigen ServiceNow-omgeving hetzij met een koppeling tussen de servicemanagement omgeving van Opdrachtnemer en de GGN-eigen ServiceNow-omgeving.

12. Opdrachtnemer is op de hoogte van het feit dat GGN voor haar eigen managed services en managed security services vrijwel uitsluitend gebruik maakt van Microsoft-producten en van producten die Microsoft-compatible zijn. GGN maakt hiervoor bij haar Cloud Solution Provider gebruik van de Microsoft-regeling voor non-profit organisaties. Opdrachtnemer garandeert daarom dat zij te allen tijde en zoveel als mogelijk gebruik zal maken van Microsoft-producten en Microsoft-compatible producten, tenzij anders schriftelijk overeengekomen met Opdrachtgever.

13. Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office.

14. Opdrachtnemer garandeert dat te allen tijde voor de Managed Services en de Managed Security Services uitsluitend gebruik wordt gemaakt van medewerkers die daartoe aantoonbaar bekwaam en geschikt zijn. Opdrachtnemer hanteert hiervoor conform haar kwaliteit- en beveiligingssystemen vooraf bepaalde en bij de medewerkers getoetste criteria, zoals het hebben van een Verklaring Omtrent het Gedrag (VOG) inzake:

    a. Bevoegdheid hebben tot het raadplegen en/ of bewerken van systemen (MSP, MSSP)
    b. Met gevoelige/ vertrouwelijke informatie omgaan (MSP, MSSP)
    c. Kennis dragen van veiligheidssystemen, controlemechanismen en verificatieprocessen (MSSP).

15. Opdrachtnemer en Opdrachtgever stellen gezamenlijk bij aanvang van de Opdracht een Architectuurplaat (processen, data, applicaties) samen waarin de kantoorautomatisering en managed services worden gevisualiseerd. Deze Architectuurplaat is doorlopend voor Opdrachtgever te raadplegen en wordt tenminste halfjaarlijks door Opdrachtnemer geactualiseerd.

16. Opdrachtnemer en Opdrachtgever stellen gezamenlijk bij aanvang van de Opdracht een Architectuurplaat (processen, data, applicaties) samen waarin de securityvoorzieningen en de managed security services worden gevisualiseerd. Deze Architectuurplaat is doorlopend voor Opdrachtgever te raadplegen en wordt tenminste halfjaarlijks door Opdrachtnemer geactualiseerd.

17. Opdrachtnemer rapporteert minimaal ééns per kwartaal aan Opdrachtgever over het gebruik en het aantal CSP-licenties en Azure-abonnementen en doet voorstellen voor besparingen.

Managed Services

18. Opdrachtnemer heeft nadrukkelijk kennis genomen van de IST en SOLL situatie inzake Managed Services zoals beschreven in de Aanbestedingsleidraad, alsook van de daarin opgenomen Definities.

19. Opdrachtnemer verzorgt direct bij ingang van de Overeenkomst een Due Diligence onderzoek op de GGN-eigen Managed Services en levert hiervan binnen 2 maanden de resultaten en een definitief Implementatie- en Uitrolplan.

20. Opdrachtnemer verzorgt direct bij ingang van de Overeenkomst een Exit-plan voor de Managed Services conform de specificaties als beschreven in **Bijlage Q – Template Exit-plan** ten behoeve van Inkoopproces en levert dit binnen 2 maanden op aan Opdrachtgever.

21. Opdrachtnemer verzorgt tenminste éénmaal per jaar een nieuwe versie van het Exit-plan en legt dit ter goedkeuring voor aan Opdrachtgever.

22. Opdrachtnemer begrijpt dat we in dit Programma van Eisen met 'as is' de huidige IST situatie bedoelen en Opdrachtnemer garandeert dat de managed services as is, dus met bestaande instellingen, configuraties, protocollen en regels, worden overgenomen.

23. Indien Opdrachtnemer op basis van de Due Diligence mogelijkheden voor verbetering ziet door bijvoorbeeld het vervangen van (diensten)componenten die aantoonbaar gelijkwaardig of beter zijn, dan is het Opdrachtnemer, na schriftelijke toestemming van Opdrachtgever, toegestaan deze (diensten)componenten te vervangen.

24. Opdrachtnemer verzorgt de Managed Services in het eerste jaar op basis van de volgende fasering:

    a. Inbeheername-fase.
    Inbeheername as-is van bestaande voorzieningen bij GGN en borging van de continuïteit/ going concern;

    b. Definitie- en Planningsfase.
    Samen met Opdrachtgever definiëren van een Backlog Managed Services voor optimalisatie van de Managed Services-voorzieningen uit oogpunt van gebruikers, kosten, veiligheid, beschikbaarheid en continuïteit en het maken van een planning van de daaruit voorkomende sprints/ changes/ projecten;

    c. Uitvoer- en Optimalisatiefase.
    Conform planning realiseren van de Backlog Managed Services.

25. Opdrachtnemer neemt de rol van Cloud Solution Provider (CSP) over van de huidige GGN-leverancier zonder dat het gebruik van de daarin afgenomen licenties wordt onderbroken/ verstoord.

26. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Kantoorautomatisering as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Kantoorautomatisering in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

27. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Kantoorinfrastructuur, Netwerkomgeving en Firewalls as-is als Managed Services in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Kantoorinfrastructuur, Netwerkomgeving en Firewalls in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

28. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Kantoor Internettoegang en Internetverbindingen as-is als Managed Services in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Kantoor Internettoegang en Internetverbindingen in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

29. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Kantoor Cloudhosting as-is als Managed Services in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Kantoor

Cloudhosting in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

30. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Kantoor Back-up & Recovery as-is als Managed Services in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Kantoor Back-up & Recoveryvoorzieningen in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

31. Opdrachtnemer maakt tenminste eenmaal per 24 uur een volledige back-up van alle e-maildata, Teams-data, SharePoint-data, OneDrive-data, Microsoft 365-groepen, Viva Engage-data en de volledige Entra-ID-configuratie.

32. Opdrachtnemer maakt tenminste eenmaal per 24 uur een volledige back-up van alle data die gerelateerd zijn aan- en worden gegenereerd door de Managed Services.

33. Opdrachtnemer verzorgt updates, patches en upgrades in Kantoorautomatisering, Kantoorinfrastructuur, Netwerkomgeving, Firewalls, Kantoor Internettoegang, Internetverbindingen, Kantoor Cloudhosting, Kantoor Back-up & Recovery dan wel via een vooraf vastgesteld schema, dan wel via de Backlog Managed Services.

34. Opdrachtnemer verzorgt kritieke updates, patches en upgrades in Kantoorautomatisering, Kantoorinfrastructuur, Netwerkomgeving, Firewalls, Kantoor Internettoegang, Internetverbindingen, Kantoor Cloudhosting, Kantoor Back-up & Recovery in lijn met de termijnen uit de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) en relevante kaders van de Wet digitale overheid.

35. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Fysieke werkplekken van de medewerkers as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Fysieke werkplekken van de medewerkers in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

36. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Virtuele werkplekken van de medewerkers as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Virtuele werkplekken van de medewerkers in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

37. Opdrachtnemer draagt ervoor zorg dat, behoudens de hardwarecomponent, de Virtuele werkplek qua gebruikerservaring gelijkwaardig is aan de Fysieke werkplek. Hiermee bedoelen we dat vanaf het moment van inloggen op de werkplek dezelfde omgeving, functionaliteiten en applicaties worden geboden.

38. Opdrachtnemer verzorgt niet alleen de werkplekken voor de GGN-medewerkers, maar verzorgt desgevraagd ook Fysieke en/ of Virtuele werkplekken voor door GGN aangewezen gebruikers-groepen waaronder mogelijk medewerkers van regionale GGD'en, GHOR-bureaus en/ of GGN-ketenpartners. Hierbij geldt dat alle werkplekken (fysiek en virtueel, eigen en andere gebruikersgroepen) allen op dezelfde wijze zijn geconfigureerd.

39. Opdrachtnemer garandeert dat alle werkplekken (fysiek en virtueel, eigen en andere gebruikers-groepen) volledig 'locatie-onafhankelijk' correct functioneren. Hiermee bedoelen we dat gebruikers vanaf eender welke locatie (werk, privé, onderweg, buitenland voor zover het de EER betreft) met een geschikte internetverbinding overal toegang hebben tot hun werkomgeving en benodigde diensten en data.

40. Opdrachtnemer garandeert dat het aantal werkplekken van circa 300 bij aanvang van de opdracht in beheer kunnen worden genomen en is bereid het aantal te beheren werkplekken te laten meegroeien en/ of meekrimpen met de ontwikkelingen en organisatie-omvang van GGN.

41. Opdrachtnemer garandeert dat in geval van een crisissituatie de Virtuele werkplekdiensten snel kunnen worden opgeschaald met tenminste 100 virtuele werkplekken binnen en per 48 uur, zonder onderbreking of verstoring van bestaande dienstverlening.

42. Opdrachtnemer draagt ervoor zorg dat alle Fysieke en Virtuele werkplekken te allen tijde middels Microsoft Intune (of gellijkwaardig) als Unified Endpoint Management (UEM)-oplossing centraal worden beheerd.

43. Opdrachtnemer verzorgt een portal / omgeving / platform, bijvoorbeeld- of tenminste gelijkwaardig aan Microsoft InTune Company Portal, waarmee gebruikers van Opdrachtgever zelfstandig optionele aanvullende applicaties kunnen installeren op basis van hun rol / functie / afdeling/ autorisatie.

44. Opdrachtnemer draagt ervoor zorg dat toegang/ uitgifte van de Fysieke en Virtuele werkplekdiensten te allen tijde via het GGN-provisioningsysteem Hello-ID (of gelijkwaardig) verloopt op basis van een persoonlijk @ggdghor.nl-account.

45. Opdrachtnemer neemt de GGN-eigen voorzieningen voor Printen en Reproductie as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Print- en Reproductievoorzieningen in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

46. Opdrachtnemer neemt de GGN-eigen Vergadervoorzieningen as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Vergadervoorzieningen van de medewerkers in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

47. Opdrachtnemer neemt de GGN-eigen Zakelijke Telecommunicatievoorzieningen as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Zakelijke Telecommunicatievoorzieningen in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services.

48. Opdrachtnemer werkt initieel samen met de GGN-eigen Servicedesk en neemt op aangeven van Opdrachtgever de servicedeskwerkzaamheden op termijn deels of in haar geheel als Managed Service over.

49. Opdrachtnemer garandeert dat alle beheerapplicaties, kantoor- en werkplekapplicaties en optionele aanvullende applicaties nooit meer dan één hoofdversie achterlopen op de dan meest actuele versie.

50. Opdrachtnemer garandeert tenminste/ minimaal aan de Service Level Requirements voor de Managed Services te kunnen voldoen, zoals zijn opgenomen in de **Bijlage J - Concept SLA-MSP**.

Managed Security Services

51. Opdrachtnemer heeft nadrukkelijk kennis genomen van de IST en SOLL situatie inzake Managed Security Services zoals beschreven in de Aanbestedingsleidraad, alsook van de daarin opgenomen Definities.

52. Opdrachtnemer verzorgt direct bij ingang van de Overeenkomst een Due Diligence onderzoek op de GGN-eigen Managed Security Services en levert hiervan binnen 2 maanden de resultaten en een definitief Implementatie- en Uitrolplan.

53. Opdrachtnemer verzorgt direct bij ingang van de Overeenkomst een Exit-plan voor de Managed Security Services conform de specificaties als beschreven in **Bijlage Q – Template Exit-plan** ten behoeve van Inkoopproces en levert dit binnen 2 maanden op aan Opdrachtgever.

54. Opdrachtnemer verzorgt tenminste éénmaal per jaar een nieuwe versie van het Exit-plan en legt dit ter goedkeuring voor aan Opdrachtgever.

55. Opdrachtnemer verzorgt de Managed Security Services in het eerste jaar op basis van de volgende fasering:

    a. Inbeheername-fase.
       Inbeheername as-is van bestaande SOC/ SIEM/ Managed Security Services-voorzieningen bij GGN en borging van de continuïteit/ going concern;

    b. Definitie- en Planningsfase.
       Samen met Opdrachtgever definiëren van een Backlog Managed Security Services voor optimalisatie van de Managed Security Services-voorzieningen uit oogpunt van klant, veiligheid, techniek en kosten en het maken van een planning van de daaruit voorkomende sprints/ changes/ projecten;

    c. Uitvoer- en Optimalisatiefase.
       Conform planning realiseren van de Backlog Managed Security Services.

56. Opdrachtnemer maakt voor de inbeheername van de Managed Security Services gebruik van de licenties van de Cloud Solution Provider (CSP) welke onder Managed Services door Opdrachtnemer in beheer is genomen, zonder dat het gebruik van de daarin afgenomen licenties wordt onderbroken/ verstoord.

57. Opdrachtnemer neemt de GGN-eigen SOC/ SIEM-voorzieningen as-is als Managed Security Services in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Security Services.

58. Opdrachtnemer garandeert dat in het algemeen voor haar dienstverlening én voor vervanging of toevoeging van nieuwe securityproducten en/ of securitysoftware te allen tijde gebruik wordt gemaakt van proven technology ofwel moderne betrouwbare producten die zich bewezen hebben.

59. Opdrachtnemer garandeert dat voor vervanging of toevoeging van nieuwe securityproducten en/ of securitysoftware te allen tijde gebruik wordt gemaakt van toekomstbestendige mainstream

producten en/ of software. Producten en/ of software waarvan de leverancier end-of-life heeft aangekondigd, voldoen niet aan deze eis.

60. Opdrachtnemer garandeert dat- en werkt mee aan dat- de Managed Security Services-voorzieningen te allen tijde conform de verplichte standaarden van het Forum Standaardisatie zijn ingericht.

61. Opdrachtnemer garandeert dat- en/ of werkt mee aan dat- de Managed Security Services, de onderliggende applicaties en infrastructuur, de SIEM-data (zowel in rust als in transit) te allen tijde met ruim voldoende versleuteling tussen Opdrachtnemer en Opdrachtgever worden beveiligd, conform de standaarden van het Forum Standaardisatie.

62. Opdrachtnemer signaleert en informeert na inbeheername proactief Opdrachtgever over aanstaande veranderingen in securitydreigingen, technologische ontwikkelingen en innovaties, wet- en regelgeving en overige zaken die relevant zijn om de cyberweerbaarheid van Opdrachtgever in stand te houden en te verbeteren.

63. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van Monitoring & Threat Detection: **Preventie, Monitoring & Detectie Services** als Managed Security Services, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

64. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Endpoint Beveiliging** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

65. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Microsoft Office 365 Beveiliging** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

66. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst **de rol van Cloud Access Security Broker (CASB) voor de beveiliging van externe Cloudapplicaties** als Managed Security Service, teneinde beleidsregels voor gebruik van deze Cloudapplicaties af te dwingen.

67. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Threat Hunting** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

68. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Identity & Access Management (IAM middels Entra-ID) Beveiliging als** Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

69. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **User and Entity Behaviour Analytics** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog

Managed Security Services.

70. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Vulnerability Management** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

71. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Cyber Threat Intelligence** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

72. Opdrachtnemer signaleert en informeert na inbeheername proactief Opdrachtgever over cyberdreigingen in het algemeen en indien actueel ook specifiek over de zorgsector en overige ontwikkelingen in de zorgsector die relevant zijn om de cyberweerbaarheid van Opdrachtgever in stand te houden en te verbeteren.

73. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van het **verzamelen/ ontvangen, opslaan, ontsluiten en distribueren van loggegevens uit verschillende bronnen en ten behoeve van het SOC/SIEM** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

74. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **toevoegen, aanpassen en verwijderen van systemen die moeten worden gemonitord** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

75. Opdrachtnemer garandeert dat het bewaren van loginformatie te allen tijde voldoet aan actuele wet- en regelgeving inzake bewaartermijn, de NIS2-richtlijn, NEN7513 als aanvullende specifieke norm voor logging in de zorg, de Baseline Informatiebeveiliging Overheid (BIO) en het actuele informatiebeveiligingsbeleid van GGN.

76. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Security Incident en Event Management (SIEM)** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

77. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Log Management** als Managed Security Service, waaronder tenminste het uitvoeren van bevragingen en het aanpassen van bevragingen op de loggegevens.

78. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Functionele Log Monitoring** als Managed Security Service, waaronder het beschikbaar maken van SIEM-functionaliteiten en het aanleveren van SIEM-data voor data-analyse en onderzoek achteraf op basis van use cases.

79. Opdrachtnemer garandeert dat alle functionaliteiten (business rules, use cases, dashboards, alerts etc.) welke ten behoeve van Opdrachtgever worden overgenomen, ontsloten, ontwikkeld,

geïmplementeerd en toegepast te allen tijde beschikbaar blijven voor Opdrachtgever, zowel gedurende de looptijd van de overeenkomst alsook daarná. Met 'daarná' wordt bedoeld dat al deze functionaliteiten middels het Exit-plan volledig moeten worden overgedragen/ in beheer gegeven bij een door Opdrachtgever aan te wijzen opvolger.

80. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Security Operations Centre (SOC) - Tier 1tot en met Tier 3** als Managed Service.
    Hieronder wordt tenminste verstaan:
    Tier 1:
    a. 24/7 Monitoring van SIEM-meldingen, Log data en EDR/XDR alerts;
    b. Triage / Eerste analyse: vaststellen, indelen en verrijken van meldingen;
    c. Classificatie & prioritering van meldingen;
    d. Escalatie naar Tier 2 en Tier 3
    Tier 2:
    e. Incidentonderzoek & containment
    f. In overleg met Opdrachtgever besluitvorming en resolutie van de meldingen
    Tier 3:
    g. Advanced Threats, Forensics en Threat Hunting.

81. Opdrachtnemer werkt tijdens en na inbeheername samen met het GGN-eigen SOC en neemt op aangeven van Opdrachtgever de SOC-werkzaamheden op termijn deels of in haar geheel als Managed Security Services over.

82. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Honeypot Functionaliteiten/ Voorzieningen** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

83. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst het geheel van **Vulnerability Scanning Functionaliteiten/ Voorzieningen** als Managed Security Service, welke samen met het GGN-eigen SOC voor Opdrachtgever wordt geoptimaliseerd conform de nader overeen te komen Backlog Managed Security Services.

84. Deelnemer levert een geïntegreerde oplossing voor Network Detection & Response (NDR), Intrusion Detection System (IDS) en Intrusion Prevention System (IPS), inclusief beheer, monitoring en rapportage, waarbij 24/7 detectie, analyse en mitigatie van netwerkdreigingen wordt gegarandeerd volgens de geldende beveiligingsstandaarden.

85. Opdrachtnemer verzorgt na inbeheername en gedurende de overeenkomst nader overeen te komen real-time dashboards en maakt deze beschikbaar voor het GGN-eigen SOC.

86. Opdrachtnemer verzorgt op aanvraag van- en in overleg met Opdrachtgever de ontwikkeling van Security Orchestration, Automation, and Response (SOAR)-voorzieningen.

87. Opdrachtnemer verzorgt op aanvraag van- en in overleg met Opdrachtgever consultancy, training en advies op alle onderwerpen en aspecten van de managed security services.

88. Opdrachtnemer garandeert tenminste/ minimaal aan de Service Level Requirements voor de Managed Security Services te kunnen voldoen, zoals deze zijn opgenomen in de **Bijlage K – Concept Service Level Agreement - MSSP**.