Bijlage 4
Programma van Eisen

Status : versie 1.0

Algemene eisen (1)

1. Alle (online/offline en live) contacten met opdrachtgever dienen door Opdrachtnemer (leidinggevende en accountverantwoordelijke) in correct en verstaanbaar Nederlands te geschieden.

2. Opdrachtnemer levert de in het aanbestedingsdocument beschreven gewenste situatie.

3. Op verzoek van Opdrachtgever kunnen uitvoerende werkzaamheden buiten kantooruren uitgevoerd worden.

4. Opdrachtgever heeft te maken met diverse wet- en regelgeving die mede van invloed zijn op de IT-inrichting:
   - Baseline Informatiebeveiliging Overheid (BIO): basisnormenkader voor de inrichting van informatiebeveiliging binnen overheidsorganisaties; en NIS2-richtlijn.
   - Algemene Verordening Gegevensbescherming (AVG); Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.
   - Archiefwet: Verplichting voor elke overheidsorganisatie om haar informatie duurzaam toegankelijk te maken en te houden, en te vernietigen wanneer de bewaartermijn is verlopen.

   Structureel voldoen aan de genoemde wet- en regelgeving is een eis aan de huidige en toekomstige IT-inrichting, opdrachtnemer voldoet aan de geldende regels en is voorbereid op toekomstige regelgeving, zoals NIS-2.

5. Alle opslag en verwerking van data van Opdrachtgever door Opdrachtnemer vindt plaats op systemen die vallen binnen de Europese Economische Ruimte (EER).

6. Opdrachtnemer gebruikt binnen de geboden oplossing alleen algemeen geaccepteerde en bewezen standaarden.

7. Opdrachtnemer levert tijdens uitvoering van de opdracht (voor gebruikers en beheerder) duidelijke documentatie en (online) handleidingen ten aanzien van de door hem geleverde oplossing.

8. Opdrachtnemer stelt in samenwerking met en na overleg met Opdrachtgever na gunning de geldende SLA's en concept DAP samen, met inbegrepen de van toepassing zijnde product- en servicebeschrijvingen van de geboden oplossing(en), inclusief de wijze van beheer en monitoring van de omgeving;

9. Voor alle documentatie geldt dat deze dient te zijn opgesteld in het Nederlands, zowel online als offline beschikbaar is en is voorzien van een leeswijzer die alle documentatie omvat.

10. De Opdrachtnemer garandeert dat bij storingen en calamiteiten de technici binnen 60 minuten aanwezig zullen zijn op de getroffen locatie.

11. Opdrachtnemer draagt zorg dat medewerkers eventueel benodigde certificaten bezitten die nodig zijn voor uitvoering van onderhavig opdracht.

12. Opdrachtnemer maakt samen met Opdrachtgever duidelijke afspraken over de transitie naar een nieuwe contractpartij na expiratie van de overeenkomst waarbij bijvoorbeeld risico's met betrekking tot een verlaagde beschikbaarheid of kansen van uitval zoveel mogelijk dienen te worden beperkt;

Eisen Techniek Beheeractiviteiten en Services (2)

Ter verduidelijking van en in aanvulling op gewenste situatie (zie ook paragraaf 1.3.2 van Beschrijvend Document), als ook de services, voldoet Opdrachtnemer aan de volgende eisen met betrekking tot het beheer en services:

13. Opdrachtnemer acteert proactief om incidenten te voorkomen en verzorgt zo een optimale “sizing” van de IT-omgeving op basis van gebruik, continuïteit en beschikbaarheid.

14. Opdrachtnemer zorgt voor continuïteit in beschikbaarheid van resources, zoals opgenomen in de SLA/DAP en zorgt naast een primair eerste aanspreekpunt voor borging via een 2e aanspreekpunt op naam;

15. Bij zware incidenten, in de technisch- en functionele dienstverlening van de opdrachtnemer, met grootschalige onbeschikbaarheid (waarbij 50% of meer van de medewerkers haar werkzaamheden niet kan uitvoeren) van de geleverde voorzieningen (binnen of buiten kantoortijd) geldt maximaal vier uur tot herstel (tijdens kantooruren van 07:00 uur tot 17:30 uur).

16. Opdrachtnemer garandeert dat de geleverde producten en diensten mee kunnen groeien en krimpen met ontwikkelingen bij Opdrachtgever (bijvoorbeeld bij meer of minder devices, applicaties, opslag, gebruikers).

17. Opdrachtnemer verzorgt het beheer van alle ingezette hardware en software conform de omschreven scope in paragraaf 1.3.3 van het Beschrijvend Document en eisen in dit document. In deze paragraaf is tevens duidelijk aangegeven welke hardware binnen het beheer valt en welke daarbuiten.

18. Opdrachtnemer dient minimaal de volgende beheertaken uit te voeren:
    - Beheer op de storageomgeving (incl. updates, patches en evt. rollback van deze activiteiten);
    - Beheer op de applicatie laag op Microsoft producten, (Azure) Active Directory;
    - Beheer van de infrastructuur, zoals switches/routers, firewalls, wifi-netwerk;
    - Telefonisch/ online 1e, 2e en 3e lijns-support, inclusief registratie van incidenten en andere meldingen in een applicatie inclusief het oplossen van incidenten en meldingen;
    - Beheer van de Microsoft omgeving van Opdrachtgever.

19. Tot de door Opdrachtnemer als onderdeel van de opdracht uit te voeren (beheer)werkzaamheden behoren in ieder geval ook:
    - Beheren van de digitale werkplekken (KA omgeving);
    - Inschakelen, aansturen en coördineren van de eventueel bij de 2e lijns ondersteuning betrokken partijen;
    - Uitrollen van nieuwe software en van updates/upgrades. Distributie van packages, updates en security patches, als onderdeel van het actualiseren van de aangeboden oplossing. Uitrol van updates of upgrades van operating systems;
    - Aannemen, registreren en afhandelen van incident meldingen aangemeld door Opdrachtgever;
    - Beantwoorden van vragen van eindgebruikers over het gebruik van de werkplek, kantoorautomatisering en Mobile Device Management.

20. Opdrachtnemer stelt een plan op voor en ondersteunt bij de verdere adoptie van Microsoft365.

21. Opdrachtnemer rapporteert en adviseert proactief over beschikbaarheid en kosten van benodigde resources, zoals bijvoorbeeld, accounts, storage, licenties, etc. en adviseert en handelt hierin proactief.

22. Opdrachtnemer is verantwoordelijk voor het vastleggen en actueel houden van de configuratiegegevens, configuratiemanagement, asset management, lifecycle management en patchadministratie. Het doel is vastleggen en beheren van informatie over de ICT-omgeving en het op verzoek beschikbaar stellen van deze informatie aan bevoegde belanghebbenden van Opdrachtgever.

23. Signaleren van trends, vaak voorkomende incidenten, onderliggende oorzaken en verbanden. Deze trends worden periodiek besproken met de ICT-adviseur van Opdrachtgever; het doen van voorstellen op basis van bovenstaande analyse, ter voorkoming van incidenten.

24. De Opdrachtnemer draagt zorgt voor de aanschaf, inrichting, levering en uitgifte van hardware conform de specificaties in bijlage *Overzicht EA Kantoorautomatisering SNN tabblad 2.1 Specificaties aan te schaffen laptops.*

25. De Opdrachtnemer voorziet in integratie van verschillende meeting rooms (vergaderzalen) op het hoofdkantoor van SNN voor geavanceerde vergadering opstellingen. De Opdrachtnemer zorgt ervoor dat de werkplekken geïntegreerd worden en blijven met de aanwezige vergaderapparatuur (monitors, camera's en microfoons) in de vergaderzalen.

Backup en recovery (3)

26. Opdrachtnemer verzorgt een adequate back-up oplossing waarbij de data worden geback-upt en er sprake is van een maximale RPO (Recovery Point Objective) van vier (4) uur.

27. Opdrachtnemer garandeert dat gegevens die opgeslagen liggen in de back-up op een passende wijze zijn beveiligd tegen inzage van derde partijen door middel van back-up hardening en encryptie.

28. Opdrachtnemer test minimaal 1x per kwartaal het functioneren van de back-up door een back-up te restoren bij wijze van test. Opdrachtnemer levert hierover een rapportage met resultaten aan opdrachtgever.

Servicedesk (4)

29. Opdrachtnemer verzorgt een volgens ITIL ingerichte servicedesk die beschikbaar is voor alle gebruikers van Opdrachtgever zoals omschreven in paragraaf 1.3.2 van het Beschrijvend Document, tijdens werkdagen van 07:00 uur tot 17:30 uur. Opdrachtnemer biedt ondersteuning middels e-mail, telefonisch en online portal en maakt gebruik van een ticketsysteem.

30. Medewerkers van Opdrachtnemer die gebruikers van Opdrachtgever telefonisch te woord staan, hebben kennis van de organisatie van Opdrachtgever en de operationele context en omgeving waarbinnen gewerkt wordt en weten hier mee om te gaan.

31. Opdrachtnemer zorgt voor een noodnummer, wat bereikbaar is buiten werkdagen van 07:00 tot 17:30 uur ten behoeve van het melden van en opvolging geven aan kritische verstoringen.

32. Opdrachtnemer draagt in het kader van de servicedesk functie zorg voor fysieke aanwezigheid op de locatie van Opdrachtgever voor minimaal één, maximaal twee werkdagen per week. De exacte momenten/dagen worden na gunning in overleg met Opdrachtgever en Opdrachtnemer bepaald en schriftelijk vastgelegd.

Wijzigingsbeheer (5)

33. Afhandeling van standaard wijzigingen dient inclusief te zijn in de opgegeven kosten op het prijzenblad en dienen binnen maximaal één (1) dag te zijn verwerkt. Deze wijzigingen zijn in ieder geval:
    - Rechten en/of instellingen van een gebruiker wijzigen;
    - Wachtwoord wijzigen of resetten;
    - Nieuwe gebruiker aanmaken en hardware gereedmaken voor gebruik;
    - Verwijderen van gebruiker inclusief zijn bestanden/ bestanden archiveren;
    - Groepen aanmaken, (leden) wijzigen of rechten aanpassen;
    - Applicatie toewijzen of verwijderen;
    - Distributielijst of groepsmailbox maken, aanpassen of verwijderen;
    - Aanpassen quota (opslag, mail, etc.);
    - Ingezette systemen/ hardware resetten;
    - Instellingen aan apparatuur wijzigen of apparatuur wijzigen om aan afgesproken prestaties te (blijven) voldoen.

    Overzicht van de historische geregistreerde tickets zijn te vinden in paragraaf 3 van bijlage *Overzicht EA Kantoorautomatisering SNN*. Voor inzicht in de wijzigingen/meldingen historie zie ook bijlage *Overzicht EA Kantoorautomatisering SNN paragraaf 3.*

34. Het uitvoeren van niet-standaard wijzigingen (anders dan hierboven gespecificeerd) worden enkel uitgevoerd op verzoek van- en na goedkeuring door Opdrachtgever. Dergelijke wijzigingen worden als separate opdracht onder de Raamovereenkomst geoffreerd en verrekend;

35. Opdrachtnemer draagt zorg voor gepland preventief en adaptief onderhoud en andere systeem belastende werkzaamheden tussen 19:00 en 07:00 uur, dus buiten kantooruren, zodat de gevraagde beschikbaarheid gehaald kan worden;

36. Analyseren van gewenste wijzigingen in de werkplekinrichting en/of infrastructuur en vervolgens op geautoriseerd verzoek van SNN doorvoeren en aanbieden van de wijzigingen. Opdrachtnemer dient bij niet-standaard wijzigingen een Plan van Aanpak voor de niet-standaard wijziging in, Waarin in ieder geval de planning, voorziene impact en de verwachte kosten zijn beschreven.

Authenticatie en beveiliging (6)

37. Opdrachtnemer garandeert dat met de aangeboden oplossing gebruikers slechts eenmalig te hoeven worden opgevoerd (bijv. in een AD of soortgelijke repository), dat hierin rollen en rechten worden bepaald en dat andere applicaties gebruik kunnen maken van deze bron.

38. Opdrachtgever vereist MFA. Opdrachtnemer is verantwoordelijk voert de implementatie, support en betrokkenheid en integratie uit.

39. Authenticatie tot SaaS omgevingen van derden vindt plaats op basis van een enkelvoudige login (SSO), mogelijk in combinatie met MFA (waar dat ook mogelijk is vanuit de specifieke SaaS-opdrachtnemer).

40. Binnen de omgeving dient het mogelijk te zijn om specifiek afgebakende onderdelen voor externen open te stellen waarbij deze inloggen met username/password en MFA.

41. Opdrachtnemer draagt gedurende de looptijd van de overeenkomst zorg voor volledige beveiliging tegen virussen, malware en ongeautoriseerde toegang van de aangeboden ICT-voorzieningen voor wat betreft de servers en werkplekken. Met andere opdrachtnemers van Opdrachtgever voor verbindingen, firewalls en

switches wordt de totale security scope afgestemd (zowel centraal als op de werkplekken), gezamenlijk gecheckt en onderhouden.

42. Opdrachtnemer geeft opdrachtnemers van door Opdrachtgever gebruikte applicaties toegang tot hun applicatie indien noodzakelijk. De installatie van specifieke applicaties wordt door de applicatie opdrachtnemer of Opdrachtgever verzorgd.

43. Opdrachtnemer garandeert dat minimaal 1x per jaar een Microsoft Azure penetratietest wordt uitgevoerd, de eerste keer aan het einde van de transitiefase, en legt de uitkomsten voor aan Opdrachtgever. Deze penetratietest wordt uitgevoerd door een onafhankelijke derde partij. Indien uit deze test aandachtspunten naar voren komen zal Opdrachtnemer maatregelen treffen om deze aandachtpunten op te lossen;

44. De aanwezige beveiliging tegen ongeautoriseerde toegang vanaf externe netwerken en het internet (zowel centraal als op de werkplek) moet continue voldoen aan de gestelde norm vanuit de BIO/NIS2/ISO27001

45. Spamfiltering: bij 98% van de gebruikers geen enkele spammail per dag in hun persoonlijke e-mail. Bij de resterende 2% van de gebruikers wordt dit beperkt tot maximaal 1 spammail per dag.

Service Management (7)

46. Opdrachtgever heeft Servicemanagement ingericht volgens de ITIL standaard.

47. Opdrachtnemer adviseert (proactief) de Teamleider Informatievoorziening.

48. Opdrachtnemer meet maandelijks de performance, capaciteit en gebruikte aantallen van de geleverde diensten en rapporteert en adviseert hierover aan Opdrachtgever.

49. Dienstverlening en bijbehorende service afspraken wordt door Opdrachtnemer in overleg met Opdrachtgever definitief vastgelegd in een SLA/XLA en binnen één (1) maand na gunning in een DAP waarover periodiek wordt gerapporteerd en die periodiek worden besproken.

50. Opdrachtnemer initieert Periodiek overleg met de Teamleider Informatievoorziening van Opdrachtgever over de stand van zaken rondom gerapporteerde dienstverlening.

51. Opdrachtnemer initieert Periodiek overleg met de CISO van Opdrachtgever en de CISO van Opdrachtnemer over de stand van zaken rondom gerapporteerde onderdelen.

52. Het opleveren van (service level) rapportages van de geleverde diensten en het verschaffen van inzicht daarover aan Opdrachtgever maakt deel uit van de dienstverlening. De (service level) rapportages inclusief de daarin opgenomen service levels zoals die voor SNN gaan gelden dienen te worden aangeleverd bij de Inschrijving en zijn onderdeel van de gunningscriteria.

53. Opdrachtnemer voert Operationeel, tactisch en strategisch overleg met SNN over de geleverde diensten. De overlegstructuren inclusief de periodiciteit zoals die gaan gelden voor SNN worden aangeleverd bij de Inschrijving en zijn onderdeel van de gunningscriteria.

54. Opdrachtnemer rapporteert maandelijks over het ingezette aantal licenties, gebruikte resources en alle variabele onderdelen van de dienstverlening, of maakt dit binnen een webportal voor Opdrachtgever beschikbaar.

55. Opdrachtnemer stelt Opdrachtgever in de gelegenheid om tussentijds prioritering en status van incidenten, problemen, serviceverzoeken, standaard wijzigingen en niet-standaard wijzigingen te kunnen volgen.

Opdrachtgever moet de mogelijkheid hebben om de prioriteit van een specifiek probleem naar een hoger level om te zetten. De Opdrachtnemer handelt ook pro-actief in eigen prioritering naar een hoger niveau.

56. Opdrachtnemer neemt een coördinatieverplichting als Single Point of Contact op zich waarmee we verwachten dat de Opdrachtnemer regie neemt op de ICT-dienstverlening van Opdrachtgever.

Privacy

57. Opdrachtnemer hanteert privacybeleid en processen en procedures zodat duidelijk is op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en zodat in een cyclisch proces transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost. De opdrachtnemer waarborgt dat eenieder die persoonsgegevens verwerkt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt; deze personen hebben daarvoor de benodigde kennis.

58. Medewerkers van opdrachtnemer welke betrokken zijn bij de dienstverlening aan opdrachtgever zijn voor aanvang van hun werkzaamheden gescreend en met iedere medewerker is een schriftelijke geheimhoudingsplicht overeengekomen.

59. Opdrachtnemer documenteert hoe in de geboden oplossing de principes van privacy door ontwerp en privacy door standaardinstellingen (Privacy by Design en Privacy by Default) wordt toegepast en hoe de opdrachtnemer hierin de aanbestedende dienst ondersteunt bij zijn verantwoordingsplicht op grond van de AVG. Vooraf aan het ontwerp van de oplossing en bij een verandering wordt een inschatting gemaakt van de privacyrisico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.

60. Alle onderdelen van de geboden oplossing (waaronder hier en bij alle andere punten in ieder geval - maar niet uitsluitend - wordt verstaan applicaties, communicatievoorzieningen en cloudplatformen) bieden de mogelijkheden om te voldoen aan de eisen van dataminimalisatie. De opdrachtnemer documenteert dit en geeft aan hoe hij hierin de aanbestedende dienst ondersteunt bij zijn verplichtingen op grond van de AVG.

61. Alle onderdelen van de geboden oplossing zijn zodanig ingericht en opgebouwd dat betrokkenen al hun rechten kunnen uitoefenen en de oplossing faciliteert het voldoen aan verzoeken van betrokkenen inzake de uitoefening van hun wettelijke rechten. In het bijzonder biedt de oplossing de mogelijkheid om op aangeven van betrokkene, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.

62. Binnen alle onderdelen van de geboden oplossing is het mogelijk het verlenen van toegang tot persoonsgegevens te beperken op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar. De toegang kan naar keuze rol gebaseerd en waar nodig taak gebaseerd worden verstrekt en aanvullend is logging en monitoring mogelijk.

63. Alle onderdelen van de geboden oplossing behoren op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de betreffende persoon/medewerker heeft opgevraagd, ingezien en aangepast. Logbestanden worden geregistreerd en bewaard.

64. Waar de functionele eisen aan de geboden oplossing dat toelaten, maken alle onderdelen van de geboden oplossing gebruik van gegeneraliseerde gegevens.

65. Alle onderdelen van de geboden oplossing bieden mogelijkheden voor het scheiden naar verwerkingsdoel op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en de oplossing is hierop getoetst.

66. Alle onderdelen van de geboden oplossing, en iedere Functie binnen deze oplossing, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de oplossing en verwerking binnen een functie alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.

67. Opdrachtnemer is verplicht medewerking te verlenen aan de uitvoering van een DPIA en een DTIA/FRIA, voor zover de aanbestedende dienst bepaalt dat die nodig zijn.

68. Opdrachtnemer meldt als er AI wordt ingezet, wat de werking daarvan is, borgt dat deze algoritmes transparant zijn en dat grondrechten worden geborgd en de opdrachtnemer is verplicht om mee te werken aan de uitvoering van een Impact Assessment Mensenrechten en Algoritmen (IAMA)/FRIA, indien die naar het oordeel van de aanbestedende dienst nodig is.

69. Opdrachtnemer heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen en heeft een procedure om de werking van de maatregel te evalueren.

70. Opdrachtnemer heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.

71. Opdrachtnemer adviseert opdrachtgever met marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over strategische ontwikkeling en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.

72. De oplossing slaat gegevens veilig op in databases of bestanden, waarbij gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.

73. De oplossing (software) past versleuteling toe op de communicatie van gegevens die passend is bij het classificatieniveau van de gegevens en controleert hierop.

74. De oplossing biedt mechanismen om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.

75. Opdrachtnemer hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.