Bijlage A Programma van Eisen

Het formulier dient door de Inschrijver naar waarheid te worden ingevuld en dient te worden ondertekend door een persoon die blijkens het handelsregister of een volmacht van degene die blijkens het handelsregister bevoegd is om Inschrijver te vertegenwoordigen en om namens Inschrijver dit formulier te ondertekenen.

Indien een eis of vraag met "nee" wordt beantwoord zal de Inschrijving voor verdere beoordeling worden uitgesloten.

Conformiteitenlijst			
1.	Het indienen van een Inschrijving houdt in dat door Inschrijver onvoorwaardelijk met de bepalingen, eisen en voorwaarden van dit Beschrijvend document en de Nota van inlichtingen wordt ingestemd.	Ja ☐	Nee ☐
2.	NEN 7510 compliant	Ja ☐	Nee ☐
3.	Gedragslijn NVZ compliant. Dit met name v.w.b. potentiële toegang tot cliënten gegevens	Ja ☐	Nee ☐
4.	Inzicht verschaffen over privacy waarborgen voor zowel personeel als cliënten GGD HN	Ja ☐	Nee ☐
5.	Heldere afspraken (in SLA) over gebruik van data, inzage in data door opdrachtnemer en/of het gebruik van meta-data	Ja ☐	Nee ☐
6.	Aansluiting Z-cert ZorgDetectieNetwerk	Ja ☐	Nee ☐

Systemen			
Leveren en onderhouden			
7.	Non-disruptive. Geen impact op de bestaande infrastructuur en de daarop beschikbare diensten	Ja ☐	Nee ☐
8.	Mogelijkheid tot integratie met bestaande identity providers, zoals Microsoft AD, Azure AD of IAM systemen	Ja ☐	Nee ☐
9.	Ondersteunen audit-trails en logging	Ja ☐	Nee ☐
10.	Encryptie van data, zowel “in transit” (beveiligde verbindingen tussen opdrachtnemer en GGD HN) als “at rest” (opgeslagen op de systemen bij de opdrachtnemer als bij de GGD HN).	Ja ☐	Nee ☐
11.	Goede en gedocumenteerde configuratie management	Ja ☐	Nee ☐
12.	Bescherming tegen insider threats. Monitoring en logging moet gericht zijn op zowel aanvallen van buitenaf als van binnenuit	Ja ☐	Nee ☐
	Diensten en functionaliteiten		
13.	IDS/IPS (Intrusion Detection and Prevention) functionaliteit. “Hacker Alert”	Ja ☐	Nee ☐
14.	Detecteren ongeautoriseerde IT assets op de infrastructuur van GGD HN	Ja ☐	Nee ☐
15.	SIEM (Security Information and Event Management) functionaliteit, opvolging in overleg	Ja ☐	Nee ☐
16.	SOC (Security Operations Center) functionaliteit. 24/7 actief, opvolging in overleg	Ja ☐	Nee ☐

17.	Gebruik Proven Technology en producten; vermijden van zelfgebouwde applicaties en niet ondersteunde systemen.	Ja ☐	Nee ☐
18.	Implementatie traject moet voorzien in training voor personeel GGD HN (4 medewerkers)	Ja ☐	Nee ☐
19.	Heldere SLA met opdrachtnemer. Heldere exit strategie.	Ja ☐	Nee ☐
20.	Dagelijkse updates over bedreigingen en de status van de technische informatie beveiliging richting IT-Beheer en CISO. Custom rapportage mogelijkheid.	Ja ☐	Nee ☐
21.	Flexibiliteit in het afnemen van bepaalde diensten, bij voorkeur in abonnementsvorm.	Ja ☐	Nee ☐
22.	Mogelijkheid om gegevens uit een Vulnerability Scanner mee te nemen in de SIEM, zodat opvolging gestandaardiseerd is	Ja ☐	Nee ☐
23.	Bibliotheek met Use Cases. Mogelijkheid om zelf Use Cases toe te voegen	Ja ☐	Nee ☐
24.	$2^{e}/3^{e}$ lijns support in geval van calamiteiten	Ja ☐	Nee ☐
25.	Heldere communicatie strategie, met name in geval van calamiteiten. Overzicht van contactpersonen en case-managers.	Ja ☐	Nee ☐