Bijlage: Security eisen

Dit document beschrijft de eisen specifiek met betrekking tot Security aan de levering van de Diensten door Opdrachtnemer.
Het betreft de beveiliging van de vertrouwelijke gegevens, in dit geval de persoonsgegevens van:

- Medewerkers die de tooling gebruiken en waarvan de credentials zijn vastgelegd
- Externe professionals, zoals NAW gegevens en identificatie gegevens

Inschrijver dient volledig en onvoorwaardelijk te voldoen aan alle eisen zoals hieronder opgenomen. Door het indienen van een Inschrijving verklaart Inschrijver aan alle gestelde eisen en voorwaarden te voldoen. Indien Inschrijver op één of meerdere onderdelen niet volledig of onvoorwaardelijk voldoet, wordt hij uitgesloten van de aanbesteding.

De indeling van de eisen in categorieën dient uitsluitend ter ordening en heeft geen invloed op de reikwijdte, inhoud, interpretatie of afdwingbaarheid van de betreffende eisen.

Nr.	Categorie	Beschrijving Eis
1.	Wet- en regelgeving:	Inschrijver moet kunnen aantonen dat zij en haar producten en voldoen aan de Nederlandse en EU-wetgeving die op hun dienstverlening van toepassing is, zoals Wet Computercriminaliteit, Cyberbeveiligingswet (Cbw/NIS2), Algemene Verordening Gegevensbescherming (AVG) en Archiefwet.
2.	Wet- en regelgeving:	Inschrijver en aangeboden oplossing voldoet bij oplevering en gedurende de volledige looptijd van het contract aan de genoemde wet- en regelgeving.
3.	Standaarden:	Inschrijver moet gedurende de volledige doorlooptijd van het contract voldoen aan de gestelde eisen vanuit de Baseline Informatiebeveiliging Overheid (BIO) 2.0.
4.	Informatie-beveiligingsbeleid:	De Inschrijver is in bezit van een gedocumenteerd informatiebeveiligingsbeleid, onderhoudt dit en handhaaft het. Dit beleid is door het management goedgekeurd en aan al het personeel en relevante derden worden gecommuniceerd. Deze procedures ondersteunen een informatiebeveiligingsbeheersysteem (ISMS).
5.	Toegangsbeheer:	De Inschrijver implementeert toegangscontrolebeleid en -procedures die de toegang tot informatie en systemen beperken op basis van functies en bedrijfsbehoeften, met gedefinieerde processen voor goedkeuring, beoordeling en intrekking van toegang. De Inschrijver zorgt dat de toegang tot informatiesystemen en gegevens beperkt is tot geautoriseerde personen op basis van bedrijfsbehoeften en het principe van minimale bevoegdheden.
6.	Cryptografie	De Inschrijver past passende cryptografische beheersmaatregelen toe om de vertrouwelijkheid, integriteit en authenticiteit van gevoelige informatie in rust en tijdens transport te beschermen, inclusief het gebruik van, in de branche erkende (bijv. NCSC), aanvaarde encryptiestandaarden, en documenteert hoe encryptie wordt geïmplementeerd in de relevante systemen.
7.	Operationele beveiliging:	De Inschrijver dient operationele procedures en controles te implementeren en te handhaven om een veilige verwerking, opslag en overdracht van informatie te waarborgen, inclusief netwerkbeveiliging, wijzigingsbeheer, logging, monitoring en bescherming tegen malware. Inschrijver dient gegevensstromen en opslaglocaties gedocumenteerd te hebben.
8.	Beheer van beveiligingsincidenten:	De Inschrijver dient een incidentbeheerproces te hebben ingericht voor de identificatie, opvolging, rapportage en het tijdig melden van securityincidenten aan NWO.
9.	Datalocatie:	Alle data, logging en back-ups moeten worden opgeslagen op een externe locatie binnen de EU. Inschrijver is verantwoordelijk voor naleving en moet aantonen dat gegevensopslag en back-upbeheer voldoen aan de geldende regelgeving en dataveiligheidseisen.