Bijlage E – Voorwaarden IBP

Nummer	Hoofd-categorie	Sub-categorie	Informatiebeveiliging & Privacy
IBP-E01	Informatie-beveiliging & Privacy	Algemeen	De Oplossing moet opgezet en geleverd worden vanuit het basis principe “Secure-by-Design”.
IBP-E02	Informatie-beveiliging & Privacy	Algemeen	Opdrachtnemer heeft informatiebeveiliging en continuïteit aantoonbaar gestructureerd en gestandaardiseerd, en tevens een continue en procesmatige PDCA cyclus ingericht, op alle lagen van haar eigen organisatie en die van de Dienstverlening.
IBP-E03	Informatie-beveiliging & Privacy	Algemeen	De Dienstverlening en organisatie van de Opdrachtnemer moet zijn beveiligd door het implementeren en onderhouden van een set van passende technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de oplossing en de daarop opgeslagen en/of verwerkte informatie borgt op ten minste industriestandaard wijze.
IBP-E04	Informatie-beveiliging & Privacy	Algemeen	Voor het uitvoeren van onderhoud en/of aanpassingen van de Dienstverlening moet aantoonbaar een wijzigingsproces gehanteerd worden (“change management”) waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen of onderbrekingen tijdens het doorvoeren van veranderingen.
IBP-E05	Informatie-beveiliging & Privacy	Algemeen	Voor het uitvoeren van onderhoud en/of aanpassingen van de Dienstverlening dient een OTAP-proces te worden gehanteerd, waarbij in de ontwikkel-, test- en acceptatieomgevingen testgegevens worden gebruikt.
IBP-E06	Informatie-beveiliging & Privacy	Algemeen	Opdrachtnemer dient zorg te dragen dat software welke gebruikt wordt als onderdeel van de Oplossing, altijd wordt ondersteund door de leverancier van de software en blijft functioneren binnen BOOR werkomgeving.
IBP-E07	Informatie-beveiliging & Privacy	Beveiligings-incidenten	Opdrachtnemer meldt informatiebeveiligingsincidenten, waaronder, maar niet beperkt tot, datalekken, onmiddellijk en zonder onredelijke vertraging per e-mail aan de privacy officer van BOOR via het e-mailadres: privacy@stichtingboor.nl.
IBP-E08	Informatie-beveiliging & Privacy	Beveiligings-incidenten	In het geval van een informatiebeveiligingsincident moet Opdrachtnemer direct maatregelen treffen om de gevolgen en de schade te beperken voortkomend uit het incident.
IBP-E09	Informatie-beveiliging & Privacy	Beveiligings-incidenten	Opdrachtnemer verleent medewerking bij het onderzoeken en oplossen van het informatiebeveiligingsincident en stelt, indien gevraagd, alle informatie met betrekking tot het incident (in het kader van de Dienstverlening) ter beschikking aan BOOR. De informatie dient minimaal 60 dagen na aanval nog beschikbaar te zijn. Deze informatie wordt ook beschikbaar gesteld bij eventueel onderzoek door een derde partij in opdracht van BOOR.
IBP-E10	Informatie-beveiliging & Privacy	Beveiligings-incidenten	Opdrachtnemer heeft monitoring-, meld- en responsprocedures geïmplementeerd (en evalueert periodiek de effectiviteit daarvan) om informatiebeveiligingsincidenten (waaronder datalekken m.b.t. persoonsgegevens) te detecteren, melden en de gevolgen daarvan te mitigeren.
IBP-E11	Informatie-beveiliging & Privacy	Clouddiensten	BOOR-gegevens zijn altijd logisch en functioneel gescheiden van die van de overige afnemers c.q. klanten van Opdrachtnemer.
IBP-E12	Informatie-beveiliging & Privacy	Clouddiensten	In het kader van dataportabiliteit moet Opdrachtnemer de volgende voorzieningen binnen de contractueel gedefinieerde termijn ter beschikking stellen voor het exporteren van data (na beëindiging van de dienstverlening): Data moet beschikbaar zijn in een voor BOOR bruikbaar format zoals CSV, Excel (xlsx) en PDF (1.7). In het geval er sprake is van aanlevering van documenten tijdens gebruik van de dienst, dan moet het “originele / oorspronkelijke” format van het document (inclusief mappenstructuren) beschikbaar zijn.
IBP-E13	Informatie-beveiliging & Privacy	Clouddiensten	De Oplossing versleutelt alle gegevens in de cloud waarbij gebruik gemaakt wordt van de geldende ‘best practices’ (afhankelijk van de stand der techniek) m.b.t. versleuteling.
IBP-E14	Informatie-beveiliging & Privacy	Clouddiensten	De bij Opdrachtnemer gebruikte encryptiesleutels voor het encrypten van de data binnen de Oplossing moet op elk moment in het proces per direct ingetrokken of onbruikbaar kunnen worden gemaakt.
IBP-E15	Informatie-beveiliging & Privacy	Controle en Audits	BOOR wordt geïnformeerd over de eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. de door haar ingestelde beveiligingstest/-audits of onderzoek ihkv de Dienstverlening en deze dienen meegenomen te worden bij de doorontwikkeling van de Oplossing en zo nodig op de kortst mogelijke

			termijn te worden gepatcht.
IBP-E16	Informatie-beveiliging & Privacy	Controle en Audits	Opdrachtnemer draagt in het kader van de Dienstverlening jaarlijks zorg voor inzicht (in overleg e/o in rapportage) in onderstaande onderwerpen: - De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; - Overzicht van afwijkingen ten opzichte van beleid of contract; - Overzicht van de risico acceptatie; en - Een recente onafhankelijke audit-verklaring die past bij de aard van de Dienstverlening (zoals een ISAE 3000 rapportage op basis van één of meerdere SOC2 – Trusted Services Principes, of gelijkwaardig).
IBP-E17	Informatie-beveiliging & Privacy	Eisen aan personeel	Alle medewerkers van de Opdrachtnemer die participeren in de levering van de Dienstverlening moeten aantoonbaar bekend zijn met de verantwoordelijkheid op het gebied van informatiebeveiliging en privacy die als onderdeel van zijn / haar rol van toepassing zijn.
IBP-E18	Informatie-beveiliging & Privacy	Eisen aan personeel	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de Dienstverlening een geheimhoudingsovereenkomst ondertekenen en hier naar handelen.
IBP-E19	Informatie-beveiliging & Privacy	Infrastructurele beveiligings-eisen	De Dienstverlening (incl. te gebruiken componenten) en organisatie van Opdrachtnemer moet zijn beveiligd door het implementeren en onderhouden van een set van passende technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de Oplossing en de daarop opgeslagen en/of verwerkte informatie borgt op ten minste industriestandaard wijze.
IBP-E20	Informatie-beveiliging & Privacy	Infrastructurele beveiligings-eisen	Malicieuze activiteiten moeten worden gesignaleerd en gelogd aan de hand van detectieregels en afwijkingspatronen die vooraf in overleg met BOOR zijn vastgesteld, en die gebaseerd zijn op industriestandaarden en best practices.
IBP-E21	Informatie-beveiliging & Privacy	Logische toegangs-beveiliging	Opdrachtnemer stelt BOOR in staat om aan te tonen dat er betrouwbare, effectieve en controleerbare mechanismen worden ingezet voor het vastleggen en vaststellen van de identiteit van gebruikers, (en het toekennen van rechten aan gebruikers bij het gebruik van de Dienstverlening) door gebruikers. Onder gebuikers worden hier, en in de overige IBP eisen, verstaan alle Medewerkers die op enige wijze gebruik maken van de Dienstverlening of toegang hebben tot de Oplossing.
IBP-E22	Informatie-beveiliging & Privacy	Logische toegangs-beveiliging	De Dienstverlening moet afdwingen dat gebruikers alleen toegang hebben tot informatie, beheertaken en speciale bevoegdheden voor zover dat voor de uitoefening van de werkzaamheden noodzakelijk is (“need to know”, “need to use”, “least privilege”) en ze hiervoor herleidbaar geautoriseerd zijn.
IBP-E23	Informatie-beveiliging & Privacy	Logische toegangs-beveiliging	Het gebruikersaccount van medewerkers van de Opdrachtnemer, die in enige vorm toegang hebben tot (bedrijfs)gegevens van BOOR, dient ten minste te zijn voorzien van multifactor-authenticatie.
IBP-E24	Informatie-beveiliging & Privacy	Logische toegangs-beveiliging	Opdrachtnemer is verantwoordelijk voor de periodieke controle (minimaal eens per kwartaal) van de toegangsrechten van medewerkers die werkzaamheden uitvoeren in het kader van de Dienstverlening. Bij afwijkingen of bijzonderheden stelt Opdrachtnemer Stichting BOOR hiervan direct op de hoogte.
IBP-E25	Informatie-beveiliging & Privacy	Overleg & rapportage	Opdrachtnemer stelt een vaste contactpersoon aan die voor de Dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBP-E26	Informatie-beveiliging & Privacy	Overleg & rapportage	Opdrachtnemer moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de Dienstverlening.
IBP-E27	Informatie-beveiliging & Privacy	Patch management	Patch management moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de Dienstverlening en borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd.
IBP-E28	Informatie-beveiliging & Privacy	Penetratie-testen	BOOR heeft het recht om een pentest uit te laten voeren om de beveiliging te testen in het kader van de Dienstverlening. BOOR kiest hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. De (opvolging van de) voor BOOR relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met BOOR afgesproken rapportagecyclus.
IBP-E29	Informatie-beveiliging & Privacy	Penetratie-testen	Penetratietesten moeten procesmatig en procedureel, ondersteund door richtlijnen, worden uitgevoerd op alle ICT componenten van de Oplossing.
IBP-E30	Informatie-beveiliging & Privacy	Penetratie-testen	Opdrachtnemer rapporteert in het kader van de Dienstverlening de resultaten van de penetratietesten direct aan BOOR en legt vervolgens periodiek (minimaal eens per kwartaal) verantwoording af over de opvolging van de

			bevindingen.
IBP-E31	Informatie-beveiliging & Privacy	Privacy	De Dienstverlening moet gedurende de gehele looptijd van de Overeenkomst voldoen aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de AVG (Algemene Verordening Gegevensbescherming).
IBP-E32	Informatie-beveiliging & Privacy	Privacy	In lijn met Verwerkersovereenkomst moet de Opdrachtnemer de van BOOR ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van BOOR verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die Partijen zijn overeenkomen, en zal de Opdrachtnemer de persoonsgegevens dus niet gebruiken voor het uitvoeren van testen en/of het uitvoeren van data-analyses.
IBP-E33	Informatie-beveiliging & Privacy	Privacy	Daar waar BOOR geen volledige toegang heeft tot de persoonsgegevens moet Opdrachtnemer BOOR ondersteunen bij verzoeken tot inzage, correctie en eventueel het wissen van persoonsgegevens.
IBP-E34	Informatie-beveiliging & Privacy	Privacy	De Dienstverlening moet de mogelijkheid bieden om gegevenscomponenten die niet strikt noodzakelijk zijn voor latere verwerkingen of waarvoor geen doelbinding of rechtsgrond aanwezig is, te verwijderen.
IBP-E35	Informatie-beveiliging & Privacy	Privacy	Bij toepassing van data-protection-by-default door Opdrachtnemer moeten tenminste de volgende aspecten meegewogen worden: 1. Beperk zoekfunctionaliteit m.b.t. persoonsgegevens en geef alleen zoekresultaten weer na het invoeren van een aantal specifieke persoonsgegevens. 2. Pas whitelisting toe voor het opvragen van persoonsgegevens, waarbij de sterkte van de whitelisting afhankelijk is van de implementatie. Een goede aanpak is het gebruik van een mechanisme of tool die onafhankelijk opereert van de gebruiker (bijvoorbeeld een workflow-systeem dat ervoor zorgt dat de gebruiker alleen toegang heeft tot de persoonsgegevens van de betrokkene waar hij op dat moment mee bezig is).
IBP-E36	Informatie-beveiliging & Privacy	Privacy	Tijdelijke bestanden en logbestanden die voortvloeien uit de dienstverlening dienen in de productieomgeving zo min mogelijk persoonsgegevens te bevatten. De opdrachtnemer is verplicht dit periodiek te evalueren. Onder geen beding mag een bijzonder persoonsgegeven voorkomen in de logbestanden van de opdrachtnemer.
IBP-E37	Informatie-beveiliging & Privacy	Risico analyses	Opdrachtnemer heeft procedures om analyseren van risico's te borgen in het kader van de Dienstverlening. De (opvolging van de) voor BOOR relevante (IB)-risico's en mitigerende maatregelen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met BOOR afgesproken rapportagecyclus.
IBP-E38	Informatiebeveiliging & Privacy	Risico analyses	Opdrachtnemer legt bekende risico’s vast in een register en deze wordt door Opdrachtnemer voorzien van de nodige (borgings-)maatregelen ter mitigatie van de risico’s.
IBP-E39	Informatie-beveiliging & Privacy	Security Hardening	Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de Oplossing.
IBP-E40	Informatie-beveiliging & Privacy	Security Hardening	Opdrachtnemer hanteert internationaal erkende security hardening standaarden, (de CIS (Center of Internet Security) benchmarks), als basis voor het vaststellen van de security hardening richtlijn voor de ICT componenten.
IBP-E41	Informatie-beveiliging & Privacy	Tracking en tracing / logging	Alle activiteiten moeten worden vastgelegd in een logbestand dat ten minste 180 dagen bewaard blijft.
IBP-E42	Informatie-beveiliging & Privacy	Tracking en tracing / logging	De logbestanden kunnen niet achteraf worden aangepast.
IBP-E43	Informatie-beveiliging & Privacy	Vulnerability management	Opdrachtnemer heeft een procedure waar wordt geborgd dat continu naar nieuwe kwetsbaarheden en dreigingen wordt gezocht (vulnerability management) in het kader van regulier beheer en bij in gebruik name van een nieuwe dienst/ict-component/significante wijziging. De (opvolging van de) voor BOOR relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met BOOR afgesproken rapportagecyclus.
IBP-E44	Informatie-beveiliging & Privacy	Vulnerability management	Opdrachtnemer moet borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd en zorgt dat installatie van nieuwe patches geen afbreuk doet aan de continuïteit en beschikbaarheid van de Dienstverlening.
IBP-E45	Informatie-beveiliging & Privacy	Vulnerability management	Voor ingebruikname van een nieuwe dienst / ICT component en bij een significante wijziging van de Oplossing moet een kwetsbaarhedenscan uitgevoerd worden en moeten de bevindingen opgelost worden.

IBP-E46	Informatie-beveiliging & Privacy	Vulnerability management	Opdrachtnemer rapporteert periodiek (minimaal eens per kwartaal) over de resultaten van de kwetsbaarhedenscans en de daarbij behorende (voorgestelde) mitigerende maatregelen.
IBP-E47	Informatie-beveiliging & Privacy	Webapplicatie	Opdrachtnemer dient bij het ontwikkelen, implementeren en beheren van de Dienstverlening de principes "Security by Design and default" (secure software development) en “Privacy by Design and Default" toe te passen.
IBP-E48	Informatie-beveiliging & Privacy	Webapplicatie	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid zodat de Dienstverlening voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
IBP-E49	Informatie-beveiliging & Privacy	Webapplicatie	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid om de op basis van de OWASP top tien (https://owasp.org/www-project-top-ten/) meest kritische beveiligingsrisico’s binnen een webapplicatie te vermijden voor wat betreft de Dienstverlening.
IBP-E50	Informatie-beveiliging & Privacy	Webapplicatie	In het kader van opslag en/of transport van persoonsgegevens moet de Oplossing voldoen aan de cryptografische beveiligingsvoorzieningen zoals voorgeschreven in de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS). https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
IBP-W01	Informatie-beveiliging & Privacy	Algemeen	Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Dienstverlening.
IBP-W03	Informatie-beveiliging & Privacy	Clouddiensten	Alle Koppelingen tussen de Oplossing en bron-en doelsystemen van BOOR moeten op basis van open standaarden 'comply or explain' plaatsvinden.
IBP-W04	Informatie-beveiliging & Privacy	Clouddiensten	Bij multi-tenancy worden alle gegevens die binnen de Oplossing worden opgeslagen of verwerkt ten behoeve van BOOR versleuteld en gescheiden verwerkt op gehardende (virtuele) machines.
IBP-W06	Informatie-beveiliging & Privacy	Infrastructurele beveiligings-eisen	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd als onderdeel van het informatiebeveiliging incidentenproces.
IBP-W09	Informatie-beveiliging & Privacy	Overleg & rapportage	Gestructureerd en periodiek dient overleg tussen Opdrachtnemer en BOOR plaats te vinden om zowel de rapportages als (eventuele) issues te bespreken.
IBP-W10	Informatie-beveiliging & Privacy	Overleg & rapportage	Elk kwartaal moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de Dienstverlening): - Een overzicht van de beveiligingsincidenten (inclusief datalekken) inclusief trends, evaluaties en (root cause) analyses; - Rapportages van risico’s, kwetsbaarheden (vulnerability scan resultaten), patch management, hardening afwijkingen en voortgangsrapportages over bijbehorende remediation plannen; en - Analyse van de logging en monitoring informatie.
IBP-W11	Informatie-beveiliging & Privacy	Overleg & rapportage	Jaarlijks moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de Dienstverlening): - De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; - Overzicht van afwijkingen ten opzichte van beleid of contract; en - Overzicht van de risico acceptatie.
IBP-W14	Informatie-beveiliging & Privacy	Penetratie-testen	Opdrachtnemer heeft een procedure om bij significante wijzigingen (bijvoorbeeld in gebruikname nieuwe dienst/ICT componenten) in het kader van de Dienstverlening af te wegen of deze wijziging moet worden onderworpen aan een pentest. De (opvolging van de) voor BOOR relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met BOOR afgesproken rapportagecyclus.
IBP-W16	Informatie-beveiliging & Privacy	Risico analyses	Opdrachtnemer moet BOOR direct op de hoogte stellen van risico’s die de classificatie “hoog” bestempeld krijgen, zoals vastgelegd in het risicoregister (zie IBP-E15).
IBP-W18	Informatie-beveiliging & Privacy	Security Hardening	Bij het vaststellen en toepassen van de security hardening richtlijnen moet minimaal onderscheid gemaakt worden tussen de volgende ICT componenten: - Applicaties; - Middleware en databases; - Platformen / infrastructuur; - Netwerken; - Connectiviteit.

IBP-W22	Informatie-beveiliging & Privacy	Privacy	Voor de Dienstverlening moet verwijderen (oa ihkv bewaartermijnen) zijn ingericht met betrekking tot tijdelijke bestanden en/of logs waarin persoonsgegevens staan. De tijdelijke bestanden en/of logs wordt in ieder geval niet langer bewaard dan maximaal 13 maanden.

Voor akkoord:

Ondergetekende verklaart hierbij de inhoud van deze bijlage volledig te hebben gelezen en begrepen, en akkoord te gaan met alle hierin gestelde voorwaarden. Tijdens de implementatieperiode zullen deze requirements getoetst worden. Indien u niet voldoet aan de requirements, is dat reden tot ontbinding van de overeenkomst. In geval van ontbinding zullen de reeds gefactureerde kosten gecrediteerd worden.

Handtekening: _____ Datum / /

Naam en functie _____ Plaats _____

Als rechtsgeldig vertegenwoordiger van: _____