BIO Comply or explain vragenlijst

Nr	Eisen		Comply	Explain
1.	VSP 5.1.1	Opdrachtnemer is aantoonbaar voor de overeengekomen Prestatie gecertificeerd conform de meest recente versie van de NEN-ISO/IEC 27001 norm of gelijkwaardig, en blijft dit voor ten minste de duur van de Overeenkomst.	Ja/nee/n.v.t.	
	VSP 5.1-SC-01a	Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.		
2.	VSP 6.1.1	Opdrachtnemer dient voor ten minste alle processen genoemd in de Overeenkomst aantoonbaar de verantwoordelijkheden, taken en bevoegdheden op de daartoe geëigende plaatsen binnen de (project)organisatie te beleggen.		
	VSP 7.3.1	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren van verantwoordelijkheden en taken met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel te communiceren dat: 1. deze van kracht blijven na beëindiging of wijziging van het dienstverband; 2. deze ten uitvoer moeten worden gebracht.		
3.	VSP 6.1.5	Opdrachtnemer dient te beschikken over een operationeel geborgd projectbeheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.		
	VSP 13.1.2	Opdrachtnemer dient beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle diensten betrokken bij de Prestatie opgenomen te hebben in een Service Level Agreement (SLA) met Opdrachtgever met ten minste aandacht voor de beveiligingsaspecten beschikbaarheid, melden van incidenten, doorvoeren van wijzigingen en escalatie.		
	VSP 18.2.SC-08	Opdrachtnemer dient zich te houden aan de afspraken en procedures op het gebied van informatiebeveiliging waarin doel, wijze, en frequentie van contact over de informatiebeveiliging beschreven staat op strategisch, tactisch en operationeel niveau.		
4.	VSP 15.1.3	De Opdrachtnemer dient te borgen dat, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, bij de inkoop van diensten of producten van bedrijven de beveiligingseisen van Opdrachtgever door betrokkenen worden aangehouden.		
	VSP 15.1.SC-25	De Opdrachtnemer dient, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, waarbij bij inkoop van diensten of producten vendorlock-in van een onderaannemer kan ontstaan en/of de nationale veiligheid in het geding kan worden gebracht, dit eerst voor te leggen aan Opdrachtgever.		
5.	VSP 8.1.1a	Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat van alle informatiesystemen betrokken bij de Prestatie een inventaris is opgesteld in een Configuration Management Database (CMDB), zodanig dat deze effectief kan worden gebruikt voor een effectief Configuration Management (CM) ITIL proces en dat deze CMDB actueel wordt gehouden.		

Nr	Eisen		Comply	Explain
	VSP 8.1.1b	Opdrachtnemer dient op verzoek van Opdrachtgever de gegevens vermeld in de Configuration Management Database (CMDB), van alle informatiesystemen betrokken bij de Prestatie, over te dragen.		
6.	VSP 8.1.SC-12	De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.		
7.	VSP 8.2.1	Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat alle informatie betrokken bij de Prestatie is geclassificeerd conform IBR-1: *Beleid voor gegevensclassificatie* {10} van Opdrachtgever en dat de hierbij behorende beveiligingsmaatregelen worden nageleefd.		
	VSP 8.3.x	Opdrachtnemer dient over operationeel geborgde processen te beschikken voor het veilig verwijderen van media, transport van media, en het beheer van verwijderbare media en het onherstelbaar verwijderen van onnodige inhoud van herbruikbare media betrokken bij de Prestatie conform IBR-1 *Beleid voor gegevensclassificatie* {10}van Opdrachtgever.		
	VSP 11.2.7	Opdrachtnemer dient aantoonbaar te beschikken over een operationeel geborgd proces voor het vernietigen van data op media bij afvoeren of vervangen van (delen van) informatiesystemen die deze media bevatten en betrokken zijn bij de Prestatie.		
	VSP 18.1.CC-09	Gegevens of programmatuur van Opdrachtgever, of door deze gegenereerde metadata, welke zich bevinden op informatiesystemen van Opdrachtnemer, is en blijft ten alle tijden eigendom van Opdrachtgever. Indien gegevens door Opdrachtgever aan Opdrachtnemer zijn verstrekt, mag Personeel dit alleen gebruiken voor het doel waarvoor dit is gebeurd.		
	VSP 18.1.CC-10	Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het vernietigen van gegevens of programmatuur van Opdrachtgever op apparatuur en alle back-up media van Opdrachtgever, na contractbeëindiging tussen beide partijen.		
	VSP 18.1.CC-12	Wanneer gegevens van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient bij contractbeëindiging tussen deze beide partijen, de Opdrachtnemer assistentie te leveren bij de overdracht van deze informatie naar de nieuwe leverancier of terug naar Opdrachtgever.		
	VSP 18.1.CC-14	Wanneer gegevens of programmatuur van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient Opdrachtnemer aan te geven waar deze informatiesystemen zich bevinden. Indien deze zich buiten de EU bevinden, mag dit uitsluitend in landen waar een passend niveau van gegevensbescherming wordt geboden; welke landen dit zijn, is bepaald door de Europese Commissie.		
8.	VSP 7.1.1	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor de screening van het Personeel dat werkzaamheden verricht: 1. op het gebied van ontwikkelen of herzien van ontwerptekeningen en/of -documenten; 2. ten behoeve van het ontwikkelen, testen, beheren, installeren, configureren en/of bedienen van programmatuur of apparatuur; 3. in bedienings- of technische ruimtes; 4. aan kabels en leidingen; 5. aan beveiligings- en veiligheidsdocumentatie en -instructies, betrokken bij de Prestatie middels ten minste een relevante Verklaring Omtrent Gedrag (VOG), waarbij gedurende de contractperiode een screening nooit ouder mag zijn dan 5 jaar. Hangende de aanvraag van een screening kan worden volstaan met een eigen verklaring van betreffende persoon gedurende een periode van maximaal zes weken gerekend vanaf de startdatum van deze persoon bij de Prestatie, welke niet verlengd kan worden.		

Nr	Eisen		Comply	Explain
	VSP 7.2.2a	Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel een opleiding en -training op het gebied van beveiligingsbewustzijn heeft ontvangen passend bij de aard van de uit te voeren werkzaamheden, alsmede jaarlijkse bijscholing krijgt, waarin ten minste ook persoonlijke verantwoordelijkheid en specifieke beveiligingskaders van Opdrachtgever ter sprake komen.		
9.	VSP 6.1.2	Opdrachtnemer dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende, en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen.waarmee ook ongeautoriseerde toegang tot bedrijfsmiddelen wordt waargenomen of voorkomen.		
	VSP 9.1.1	Opdrachtnemer dient te zorgen voor een operationeel geborgde procedure voor het verschaffen van fysieke dan wel logische toegang tot informatieverwerkende faciliteiten, inclusief de uitgifte en inname van accounts en autorisaties, en een actuele registratie hiervan.		
	VSP 9.1.SC-02	Indien Opdrachtgever of derde partij verantwoordelijk is voor het verschaffen van de fysieke of logische toegang tot informatieverwerkende faciliteiten, dan dient Opdrachtnemer zich te houden aan de door Opdrachtgever of derde partij gehanteerde toegangsprocedure.		
	VSP 9.2.x	Opdrachtnemer dient minimaal om het halve jaar zowel de fysieke als logische toegangsrechten tot informatieverwerkende faciliteiten van het Personeel te beoordelen en te actualiseren via een operationeel geborgd en formeel proces en zijn medewerking te verlenen voor de periodieke controle en schoning van de eindgebruikers accounts en rechten van Opdrachtgever.		
	VSP 11.1.1	Opdrachtnemer dient fysieke beveiligingszones te hebben gedefinieerd en in gebruik te hebben om gebieden te beschermen, die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten, met betrekking tot de Prestatie.		
	VSP 11.1.5	Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor het werken in beveiligde gebieden, zoals bedoeld in eis VSP 11.1.1.		
	VSP 11.2.8	Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor de bescherming van onbeheerde informatiesystemen, die betrokken zijn bij de Prestatie.		
10	VSP 9.3.1	Opdrachtnemer dient van het Personeel te eisen dat het zich houdt aan de richtlijn IBR-3 *Beleid voor wachtwoordgebruik* {10} van Opdrachtgever bij het gebruiken van authenticatiegegevens gerelateerd aan de Prestatie.		
11	VSP 12.3.1a	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het minimaal dagelijks maken van back-ups van alle informatie en programmatuur in gebruik voor de Prestatie.		
	VSP 12.3.1b	Opdrachtnemer dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar Opdrachtgever te communiceren over de uitkomst hiervan.		

Nr	Eisen		Comply	Explain
12	VSP 9.4.5	Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat uitsluitend Personeel die daartoe specifiek bevoegd is, toegang heeft tot de Broncode van informatiesystemen betrokken bij de Prestatie.		
	VSP 12.1.1	Opdrachtnemer dient aantoonbaar operationeel geborgde bedieningsprocedures te hebben en beschikbaar te stellen aan het Personeel en, indien van toepassing de medewerkers van Opdrachtgever, dat ze nodig heeft voor de Prestatie.		
13	VSP 7.2.2b	Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel verantwoordelijk voor het testen van informatiesystemen betrokken bij de Prestatie, beschikken over actuele en gespecialiseerde kennis, ervaring en opleiding met betrekking tot het testen van de beveiliging hiervan.		
	VSP 14.2.SC-06a	Opdrachtnemer dient voor informatiesystemen betrokken bij de Prestatie binnen 60 dagen na kennisneming van kwetsbaarheden in het geval van programmatuur en binnen 6 maanden in het geval van apparatuur, kosteloos aanpassingen of patches vrij te geven (ten minste tot de door de Leverancier aangeduide End of Life (EOL) van dit informatiesysteem) met als doel deze kwetsbaarheden te verhelpen.		
	14.2.SC-06b	Opdrachtnemer dient te beschikken over een operationeel geborgd proces voor het periodiek doorvoeren van security patches of software updates om de informatiesystemen up te date te houden.		
	VSP 14.3.1	Opdrachtnemer dient testgegevens betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik.		
14	VSP 12.2.1	Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor bescherming tegen malware op informatiesystemen betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan preventie, detectie, communicatie en herstel.		
	VSP 15.2.1	Opdrachtgever heeft het recht om audit(s) uit te voeren waarin de eisen uit het contract tussen Opdrachtgever en Opdrachtnemer worden getoetst op opzet, bestaan, en/of werking. Aan deze audit dient Opdrachtnemer vrijwillig medewerking te verlenen.		
15	VSP 9.4.4	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het controleren van het gebruik van systeemhulpmiddelen, die in staat zijn om beheersmaatregelen te omzeilen voor informatiesystemen betrokken bij de Prestatie. Het gebruik ervan dient gelogd te worden.		
	VSP 12.2.SC-17	De Opdrachtnemer dient bij onderhoudswerkzaamheden en koppeling van randapparatuur aan de ICT van de Opdrachtgever de richtlijn IBR-8 *Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS* {10} en Handreiking: BIO Mobile Device Management {9}aan te houden voor bescherming tegen malware.		
16	VSP 12.4.1	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het voldoende periodiek beoordelen van logbestanden van informatiesystemen betrokken bij de Prestatie, waarbij het interval tussen twee beoordelingen nooit meer mag bedragen dan één maand.		
	VSP **12.4.3**	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het maandelijks beoordelen van activiteiten van systeembeheerders en -operators op informatiesystemen betrokken bij de Prestatie, welke zijn vastgelegd in logbestanden.		
	VSP 12.4.SC-21	Opdrachtnemer dient logbestanden van informatiesystemen betrokken bij de Prestatie minmaal drie maanden (en bij een vermoed incident minimaal 3 jaar) beschikbaar te houden tenzij met Opdrachtgever een andere bewaartermijn is overeengekomen, en op verzoek deze logbestanden ter inzage te overhandigen aan Opdrachtgever.		

Nr	Eisen		Comply	Explain
17	VSP 13.1.1	Opdrachtnemer dient, om informatie in informatiesystemen te beschermen, aantoonbaar operationeel geborgde processen te hebben voor beheer en beheersing van netwerken betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan onderstaande aspecten: - Management of network security - Technical vulnerability management - Identification and authentication - Network audit logging and monitoring - Intrusion detection and prevention - Protection against malicious code - Cryptographic based services - Business continuity management		
	VSP 13.1.SC-15	Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico's oplevert. Voor elke koppeling is een risicoanalyse en afweging gemaakt.		
	VSP 13.1.SC-18	Opdrachtnemer dient op verzoek van Opdrachtgever een actueel overzicht aan te leveren waarin alle datanetwerkkoppelingen worden weergegeven met bijbehorende security maatregelen.		
18	VSP 6.2.2	Toegang op afstand van alle informatiesystemen betrokken bij de Prestatie in het netwerk van Opdrachtgever is uitsluitend toegestaan via een speciaal hiervoor ingerichte Toegang Derden dienst {2} van Opdrachtgever.		
	VSP 13.2.1	Opdrachtnemer dient aantoonbaar operationeel geborgde beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de Prestatie, dat via alle soorten communicatiefaciliteiten verloopt.		
19	VSP 14.1.1	Opdrachtnemer dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van informatiesystemen. Dit dient op basis van een expliciete risicoafweging worden uitgevoerd ten behoeven van het vaststellen van de beveiligingseisen conform de BIO Handreiking: Risicoanalysemethode {11} en de Handreiking: Risicomanagement ISO-27005 {13}. In het geval van programmatuur dienen hiertoe minimaal de maatregelen geïmplementeerd te worden genoemd in het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {3}.		
	VSP 14.1.SC-24	Opdrachtnemer dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van mobiele applicaties, hiertoe dienen minimaal de maatregelen geïmplementeerd te worden genoemd in het document "Handreiking Mobiele App Ontwikkeling en Beheer voor de Rijksoverheid {4}.		
	VSP 14.2.x	Opdrachtnemer dient informatiebeveiliging aantoonbaar operationeel geborgd te hebben in de processen die deel uitmaken van de ontwikkelingslevenscyclus van informatiesystemen betrokken bij de Prestatie, waarbij ten minste de proceseisen worden geïmplementeerd uit de Richtlijn IBR-4 *Richtlijnen voor beveiligen bij ontwikkelen* {10}. In het geval van software dienen hiertoe minimaal de proceseisen worden geïmplementeerd uit het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {3}.		

Nr	Eisen		Comply	Explain
	VSP 14.2.SC-05	Opdrachtnemer garandeert de werking van informatiesystemen (ten minste tot de door de Leverancier aangeduide End of Life (EOL) hiervan) die onderdeel uitmaken van de Prestatie, op/met producten of programmatuur die níet EOL zijn en met een up-to-date patchniveau, óf biedt een kosteloze upgrade aan om dit alsnog mogelijk te maken.		
20	VSP 17.1.2	Opdrachtnemer dient aantoonbaar te beschikken over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties conform de BIO Algemene handreiking continuïteitsbeheer {14}, waarin ook de continuïteit van de informatiebeveiliging is gewaarborgd.		
21	VSP 17.1.3	Opdrachtnemer dient het continuïteitsplan voor de Prestatie minimaal jaarlijks aantoonbaar te verifiëren en bij te werken om te waarborgen dat deze deugdelijk en doeltreffend blijft. Voor het continuïteitsplan kan uitgegaan worden van de BIO Algemene handreiking continuïteitsbeheer {14}.		
22	VSP 5.1.1	De Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging. Of de Opdrachtnemer is aantoonbaar voor de overeengekomen Prestatie gecertificeerd conform de meest recente versie van de NEN-ISO/IEC 27001 norm of gelijkwaardig, en blijft dit voor ten minste de duur van de Overeenkomst.		
	VSP 18.1.3	Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor het beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave, van registraties op informatiesystemen betrokken bij de Prestatie, in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen.		
	VSP 18.1.SC-20	De Opdrachtnemer dient maatregelen te treffen om documenten, zoals offertes, contracten, netwerkschema's, risicoanalyse uitwerkingen, kwetsbaarheidscans, penetratie testrapporten en accounts en wachtwoorden te beveiligen tegen spionage in de breedste zin des woords.		
23	VSP 6.2.1	Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het beveiligen en versleutelen van gegevens op mobiele apparatuur betrokken bij de Prestatie waarbij rekening wordt gehouden met de richtlijn IBR-1 *Beleid voor gegevensclassificatie* {10}, actualiteit van de veiligheid van de gebruikte versleutelingsmethoden {1} en de Handreiking: BIO Mobile Device Management {9}.		
24	VSP 10.1.x	Indien Opdrachtnemer contractueel of wettelijk verplicht is tot de inzet van cryptografie ter bescherming van informatie betrokken bij de Prestatie, dient Opdrachtnemer voor het gebruik van deze cryptografische beheersmaatregelen over beleid en operationeel geborgde processen te beschikken, inclusief het gebruik, de bescherming en de levensduur van de daarbij behorende cryptografische sleutels, tijdens hun gehele levenscyclus conform passende standaarden (bv PKI-Overheid of ISO 11770).		
	VSP 18.1.SC-23	De Opdrachtnemer dient bij inzet van certificaten voor publieke webdiensten van RWS of het authentiseren van servers met samenwerkingspartners gebruik te maken van PKI Overheid certificaten die aangevraagd moeten worden bij Opdrachtgever. In overige gevallen dienen de passende standaarden te worden gehanteerd conform de NCSC richtlijn ICT-beveiligingsrichtlijnen voor Transport Layer Security {1}.		