

Bijlage K – Template PvE Informatiebeveiliging en Privacy

1. Informatiebeveiliging

Deze should have zijn samen met het “ICT-beleid – Informatiebeveiligingscriteria” bedoeld als toetsingsdocument voor projecten, die worden uitgevoerd en leiden tot het implementeren van applicaties (en software services) die gehost gaan worden op de GRID infrastructuur.

Het ICT-beleid – Informatiebeveiligingscriteria zal bijgevoegd worden als bijlage.

De leverancier wordt in fase 2 van de offerte-uitvraag gevraagd in hoeverre men op dit moment kan voldoen aan de gestelde eisen over de gehele breedte en wat haar ontwikkeling is op dit gebied.

In fase 1 heeft de leverancier al aangegeven aan de minimale eis gesteld van samenwerkingspartner op het gebied van informatiebeveiliging te kunnen voldoen.

Nr.	Omschrijving Should have's	Kan voldoen (JA/NEE) Omschrijving oplossing indien NEE
1	De infrastructuur en de organisatie van Inschrijver zijn adequaat beveiligd volgens ISO/IEC 27001 en 27002 (of gelijkwaardig) en voldoen aan de voorwaarden genoemd in de Algemene verordening Gegevensbescherming (AVG).	
2	Inschrijver stelt jaarlijks een Third Party Mededeling (TPM-verklaring) conform de eisen vanuit ISO/IEC 27001 op (of gelijkwaardig).	
3	Er wordt een toereikend recovery proces ingericht waar back-up en restore onderdeel van uit maken.	
4	Er moet op jaarlijkse basis worden aangetoond dat het terugzetten (restore) van de back-ups (volledige Oplossing) succesvol verloopt, dit uiteraard in een tijdelijk daarvoor ingerichte restore omgeving, dus niet direct in Test- of Productie-omgevingen.	
5	De jaarlijkse TPM moet tenminste inzicht geven in hoeverre onderstaande procedures worden toegepast op basis van opzet, bestaan en werking. - Assetmanagement - Back-up en Restore - Business Continuïteitsmanagement - Risicomanagement - Changemanagement - Autorisatie en toegangsprocedure - Logging en Monitoring - Incidentmanagement en response - Malware, patching, hardening, versleuteling procedures	
6	Het eigendom van de data ligt te allen tijde bij de Drechtsteden.	
7	Inschrijver zal na gunning een incident response procesketen met de Drechtsteden inrichten en testen.	
8	Het eigendom van tussentijds gemaakte back-ups (zowel op file- als ook op blocklevel) ligt te allen tijde bij de Drechtsteden.	
9	Inschrijver draagt er zorg voor, dat m.b.t. de omgeving waarin de data binnen de applicatie worden verwerkt, passende technische en organisatorische maatregelen zijn opgenomen om te kunnen voldoen aan de wettelijke eisen waaraan de Drechtsteden moet voldoen. Hiervoor gelden BIO / AVG / GIBIT.	
10	De leverancier heeft een Escrow regeling voor de broncode.	

11	De leverancier garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen. Niet meer gebruikte gegevensdragers worden op een gecertificeerde wijze geschoond.	
12	Voor gebruikers die vanuit het LAN inloggen op het systeem kunnen bij voorkeur via single sign on of via username/wachtwoord combinatie inloggen.	
13	Bij datacommunicatie voor bestandsuitwisseling en voor de user interface wordt gebruik gemaakt van SSL versie 3 (Secure Sockets Layer) en cliënt- en servercertificaat technologie User, -> SaaS SSLv3 en enkelvoudig geldig certificaat. LAN <--> SaaS: Tweezijdig authenticatie middels certificaten.	
14	De medewerker van de leverancier heeft in het systeem alleen toegang tot de aan hem geautoriseerde functies en gegevens. Leverancier kan dit op verzoek aantonen.	
15	Er is een totaaloverzicht beschikbaar van alle autorisaties van zowel de leverancier als de losse Drechtsteden organisaties.	
16	IT-voorzieningen en apparatuur bij de leverancier zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.	
17	Systeemsoftware die bij de leverancier in gebruik is, wordt up-to-date gehouden.	
18	Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig worden onmiddellijk gemeld aan en besproken met de Drechtsteden.	
19	Het beleid van de leverancier voor informatiebeveiliging is onderdeel van het kwaliteitsbeleid van de organisatie. Het is aantoonbaar in een ISAE3402 type 2 ISO en 27001 ISO of vergelijkbare certificeringen.	
20	Inschrijver is verplicht de persoonsgegevens adequaat te beveiligen volgens de daarvoor van toepassing zijnde dataclassificatie. Inschrijver maakt expliciet welke beveiligingsmaatregelen met betrekking tot de door de Drechtsteden verzamelde persoonsgegevens worden genomen. Bij de beveiligingsmaatregelen moet worden gedacht aan de eisen die hieronder onder Informatieveiligheid zijn omschreven. Tevens moet een actuele en volledige beschrijving van het gehanteerde beveiligingsbeleid beschikbaar zijn voor de Drechtsteden.	
21	De persoonsgegevens moeten encrypted worden opgeslagen conform ISO 27001	
22	Inschrijver heeft een proces ingericht om beveiligingsincidenten en datalekken te constateren en onverwijld te melden aan de Drechtsteden en leeft deze na. Inschrijver heeft een gedetailleerd logboek van de beveiligingsincidenten en de maatregelen die op de beveiligingsincidenten zijn genomen. Drechtsteden mag dat inzien, wanneer zij daarom vraagt.	
23	Inschrijver beschikt over een recent certificaat of verklaring van een auditor (maximaal 1 jaar oud), waaruit blijkt dat de volledige, voor de aanbidding relevante, omgeving voldoet aan ISO27001 (of gelijkwaardig), BIO en AVG standaarden.	
24	De Drechtsteden hebben een 'right to audit' bij de leverancier. Zo behouden de Drechtsteden het recht om te onderzoeken of leverancier de gemaakte afspraken nakomt.	

2. Privacy

De Drechtsteden hanteert "privacy by design" voor applicaties en systemen waarmee persoonsgegevens verwerkt worden. Deze principes komen voort uit de geldende wetgeving (AVG), maar ook de intentie om als Drechtsteden de privacy van onze inwoners en medewerkers te respecteren en dit via onze systemen zo veel mogelijk te garanderen. Hiervoor is het noodzakelijk dat het systeem voldoet aan onze eisen en wensen (must en should have's) en dat de leverancier met ons mee denkt over het zo goed mogelijk inrichten van het systeem, zodat het voldoet aan een hoge standaard op het gebied van privacy.

De leverancier wordt in dit hoofdstuk gevraagd of men op dit moment kan voldoen aan de gestelde should have's en zo niet wat de ontwikkeling van de leverancier is op dit gebied.

Nr.	Omschrijving Should have's	Kan voldoen (JA/NEE) Omschrijving oplossing indien NEE
1	Inschrijver heeft de informatieprocessen ingericht op basis van de principes van privacy by design en privacy by default. Met nadruk op toepassing van dataminimalisatie op basis van need-to-know.	
2	De persoonsgegevens die worden ingevuld moeten eenvoudig onzichtbaar kunnen worden gemaakt voor andere gebruikers.	
3	Er is minimaal sprake van een koppeling GRID Active Directory voor het raadplegen van gegevens en niet voor opslag.	
4	Inschrijver kan voldoen aan SSO o.b.v. SAML koppeling (bij het maken van de SAML koppeling wordt besproken welke velden in de ADFS/SAML koppeling worden opgenomen).	
5	Inschrijver heeft maatregelen getroffen om gebleken onvolkomenheden op het gebied van privacy- en informatiebeveiliging te herstellen.	
6	Wanneer nieuwe wetgeving of gewijzigde inzichten door jurisprudentie zich voordoen, verzorgt inschrijver in overleg kosteloos aanpassingen in het systeem (privacy flexibiliteit).	
7	Inschrijver heeft een Functionaris Gegevensbescherming of een Privacy Officer met wie snel en op transparante wijze contact kan worden gelegd voor privacy gerelateerde onderwerpen en vragen.	
8	Inschrijver biedt de mogelijkheid documenten separaat te versleutelen.	
9	Inschrijver heeft een "state of the art" autorisatiematrix inrichting / architectuur en een "Role based access management" op een "need to know/least privilege basis.	
10	In geval van een SaaS- of een gehoste Applicatie vindt de opslag van gegevens plaats binnen de Europese Economische Ruimte.	
11	Indien de gegevens die worden gegenereerd opgeslagen of verwerkt worden in het Verenigd Koninkrijk, moet Inschrijver in	

	het geval van Brexit kosteloos een 'migratiescenario' leveren en uitvoeren om snel en adequaat te kunnen migreren naar een omgeving binnen de Europese Economische Ruimte.	
12	De Drechtsteden sluit met Inschrijver een schriftelijke overeenkomst met betrekking tot de bescherming en de verwerking van persoonsgegevens cf. artikel 28 lid 3 AVG. Daarbij wordt het model verwerkersovereenkomst van de Drechtsteden gehanteerd dat overeenkomstig is met het landelijke model van de VNG/IBD.	
13	Inschrijver verstrekt de gegevens niet zonder expliciete en schriftelijke toestemming van de Drechtsteden aan derden.	
14	Inschrijver mag de door de Drechtsteden verzamelde persoonsgegevens slechts in uitdrukkelijke opdracht van de Drechtsteden verwerken en mag de persoonsgegevens niet verder verwerken voor eigen doeleinden.	
15	Inschrijver mag bij het verwerken van de persoonsgegevens alleen groepsmaatschappijen en onderaannemers/sub verwerkers inschakelen als een schriftelijke overeenkomst is gesloten waarin dezelfde verplichtingen zijn opgenomen als in het model verwerkersovereenkomst van de Drechtsteden en hiervoor toestemming is verkregen van opdrachtgever (verwerkingsverantwoordelijke).	
16	Inschrijver heeft een proces ingericht om mee te werken in geval van verzoeken van betrokkenen om hun wettelijke rechten uit te voeren. Inschrijver geeft in haar systemen toegang aan betrokkenen om hun gegevens in te zien en biedt mogelijkheden voor betrokkenen om hun overige rechten i.h.k.v. de AVG uit te oefenen. Hieronder valt tevens de mogelijkheid de verwerking te "beperken", m.a.w. te bevriezen, zoals in de AVG opgenomen.	
17	Inschrijver biedt de mogelijkheid de velden in haar systemen (data library) eenvoudig te kunnen verwijderen of te anonimiseren.	
18	Inschrijver heeft bewaartermijnen (op metadata) per categorie persoonsgegeven ingesteld met als gevolg dat de gegevens automatisch worden verwijderd na het verstrijken van deze bewaartermijnen.	
19	Inschrijver maakt geen gebruik van productiedata binnen de testomgeving of ondersteuningsomgeving.	
20	Gebruikersdata is eigendom van de Drechtsteden. Deze moet indien gewenst via export (b.v. excel) beschikbaar gemaakt kunnen worden.	
21	Persoonsgegevens worden niet vastgelegd aangaande bureaugebruik (logging).	