Eisen en Informatiebeveiliging.

Informatiebeveiliging

Deze lijst van eisen kan worden gebruikt ter controle op de te nemen beveiligingsmaatregelen door een potentiële leverancier. Houd hierbij rekening dat deze lijst niet sluitend is en dat aanvullende beveiligingsmaatregelen nog steeds van toepassing kunnen zijn.

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).	
Inschrijver stelt jaarlijks een Third Party Mededeling (TPM-verklaring) conform de eisen vanuit ISO/IEC 27001en 27002 op (of gelijkwaardig).	
Er wordt een toereikend recovery proces ingericht waar back-up en restore onderdeel van uit maken.	
Er moet op jaarlijkse basis worden aangetoond dat het terugzetten (restore) van de backups (volledige Oplossing) succesvol verloopt, dit uiteraard in een tijdelijk daarvoor ingerichte restore omgeving, dus niet direct in Test-/ of Productie omgevingen.	
"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.	
Het eigendom van de data ligt te allen tijde bij de Drechtsteden.	
Inschrijver zal na gunning een incident response procesketen met de Drechtsteden inrichten en testen.	
Het eigendom van tussentijds gemaakte back-ups (zowel op file- als ook op blocklevel) ligt te allen tijde bij de Drechtsteden.	
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 de BIO en de AVG.	
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.	
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 minimaal TLS1.2 en enkelvoudig geldig certificaat. LAN <--> SaaS: Tweezijdig authenticatie middels certificaten.	
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.	
Er is een totaaloverzicht beschikbaar van alle autorisaties van zowel de leverancier als de gemeente.	
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.	

Systeemsoftware die bij de leverancier in gebruik is, wordt up-to-date gehouden.	
Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig worden onmiddellijk gemeld aan en besproken met de Drechtsteden.	
Uw beleid 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.	
De leverancier verleent medewerking aan het uitoefenen van controle door of namens de gemeente op bewaring en gebruik van gegevens en dat hij zijn verplichting tot adequate beveiliging nakomt. Een bezwaar van de leverancier tegen een door de gemeente uit te voeren audit is niet acceptabel.	
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.	
De persoonsgegevens moeten encrypted worden opgeslagen conform ISO 27001/BIO. Het encrypten in het lifecycleproces van data gebeurt gedurende: - Creatie van data - Storage van data - Use van data - Share(delen)van data - Archive van data - Destroy van data.	
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.	
Inschrijver beschikt over een recent certificaat of verklaring van een auditor (maximaal 1 jaar oud), waaruit blijkt dat de volledige, voor de aanbieding relevante, omgeving voldoet aan ISO27001, ISO27002 (of gelijkwaardig), BIO en AVG standaarden.	
De Drechtsteden hebben een 'right to audit'.	
De aangeboden oplossing(en) maakt/maken gebruik van een autorisatiemodel op basis van rollen (Role Based Access Control (RBAC)). Hierbij kunnen medewerkers van de Drechtsteden meerdere rollen toegekend krijgen. De autorisatie rollen (RBAC) zijn bepalend voor de rechten van medewerkers van de Drechtsteden, waarbij toegang en ontsluiting, maar ook mutatie van gegevens afzonderlijk zijn vrij te geven of af te schermen per rol.	