Eisen en Informatiebeveiliging (Soft- en Hardware)

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.

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 27001en 27002 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 backups (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 de BIO en de AVG.	
10. 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.	
11. Bij datacommunicatie voor bestandsuitwisseling en voor de user interface wordt gebruik gemaakt van minimaal TLS 1.2 en cliënt- en servercertificaat technologie User -> SaaS min. TLS 1.2 en	

enkelvoudig geldig certificaat. LAN <--> SaaS: Tweezijdig authenticatie middels certificaten.	
12. 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.	
13. Er is een totaaloverzicht beschikbaar van alle autorisaties van zowel de leverancier als de gemeente.	
14. 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.	
15. Systeemsoftware die bij de leverancier in gebruik is, wordt up-to-date gehouden.	
16. Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig worden onmiddellijk gemeld aan en besproken met de Drechtsteden.	
17. 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.	
18. 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.	
19. 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.	
20. 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.	
21. 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.	
22. 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.	
23. Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	
24. Cryptografische toepassingen voldoen aan passende standaarden.	
25. Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	
26. Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Alleen beveiligingsmechanismen. Overige zaken zie SLA eisen.
27. Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	
28. Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	
29. De effectiviteit van de richtlijnen voor de netwerkbeveiliging behoort periodiek getoetst en geëvalueerd te worden.	
30. De naleving van een, volgens het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliancy-toetsen).	
31. Ten behoeve van het huisvesting IV-beleid behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	
32. Het management van huisvesting IV behoort diensten te leveren volgens een Diensten Niveauovereenkomst (DNO)/Service Level Agreement (SLA).	
33. Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	
34. De stakeholder van huisvesting IV behoort een beheersorganisatie te hebben ingericht waarin de processtructuur, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.	
35. Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.	

36. Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	
37. In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	
38. De organisatie moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	
39. Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	
40. De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	
41. Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	
42. Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruiken van bedrijfsmiddelen te verminderen.	
43. Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.	
44. Voor autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen beschikbaar zijn, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten.	
45. Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er procedures te zijn vastgesteld.	
46. Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	
47. Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	
48. De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	
49. De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	
50. 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.	

Attentie: Bovenstaand programma van Eisen en Wensen is in beginsel een vertrekpunt van basiseisen die worden gesteld. Let er dus op dat het mogelijk is dat er aanvullende eisen van toepassing zullen zijn en dat bovenstaande lijst niet 100% sluitend is.