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. Het eigendom van de data ligt te allen tijde bij de Drechtsteden	
2. Inschrijver zal na gunning een incident response procesketen met de Drechtsteden inrichten en testen.	
3. 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 / BIG / BIR / AVG / GIBIT.	
4. 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	
5. 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.	
6. 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.	
7. Er is een totaaloverzicht beschikbaar van alle autorisaties van zowel de leverancier als de gemeente.	
8. 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	
9. Systeem en applicatiesoftware die bij de leverancier in gebruik is, wordt up-to-date gehouden.	
10. Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig worden onmiddellijk gemeld aan en besproken met de Drechtsteden.	
11. Uw beleid voor informatiebeveiliging is onderdeel van het kwaliteitsbeleid van de organisatie. Het is aantoonbaar in een ISAE3000 type 2 verklaring of ISO27001 of vergelijkbare certificeringen.	
12. 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.	
13. De Drechtsteden hebben een 'right to audit'	
14. In het beleid behoort te zijn vastgesteld dat een centrale organisatiestructuur gebruikt wordt voor het beheren van netwerken (onder andere Local Area Network (LAN) en Virtual Local Area Network (VLAN)) en zo veel mogelijk van de hardware en softwarecomponenten daarvan.	

15. Organisaties behoren hun netwerken te beveiligen op basis van richtlijnen voor ontwerp, implementatie en beheer.	
16. 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.	
17. 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.	
18. 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.	
19. 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).	
20. 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.	
21. Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	
22. Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	
23. Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruiken van bedrijfsmiddelen te verminderen.	
24. Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.	
25. Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	

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.