Bijlage 16
Generiek PvE ICT-middelen

Let op: Indien Inschrijver niet kan instemmen met een wens (zie nummer 25 en/of 27) uit deze bijlage**,** biedt Inschrijver voor de betreffende wens een alternatief aan. Inschrijver dient een **beschrijving van het alternatief (free format)** in te dienen bij zijn Inschrijving. Indien geen beschrijving is toegevoegd wordt Inschrijver geacht in te stemmen met deze wensen.

1.1 Identity & Access Service

Nr.	Omschrijving	Eis/wens
1	Voor toegang tot de software/voorziening wordt uitsluitend gebruikgemaakt van persoonsgebonden inlognaam en wachtwoord. Dit geldt voor zowel eindgebruikers en beheerders als voor de Opdrachtnemer.	Eis
2	Access Management vindt plaats op basis van groepen. - Gebruikersgroepen (op basis van profielen) - Afdelingen (op basis van profielen)	Eis
3	Ondersteuning van de rechtenstructuur is mogelijk op basis van een Windows Active Directory-omgeving (LDAPs compliant). Binnen de VRFGV wordt gebruik gemaakt van AGDLP.	Eis
4	Gebruikers (inclusief functioneel beheerders) binnen de VRFGV hebben beperkte gebruikersrechten; geen power-user of local adminrechten en de software kan daarmee omgaan.	Eis
5	Software mag uitsluitend onder een serviceaccount draaien. Een serviceaccount is onderdeel van een AD-domain en heeft zo min mogelijk privileges. Serviceaccounts worden nooit voorzien van Domain Adminrechten. De benodigde rechten voor deze serviceaccount dienen te worden gespecificeerd door de Opdrachtnemer.	Eis
6	Opdrachtnemer heeft niet rechtstreeks toegang tot de data, zonder hiervoor toestemming te hebben gekregen van de VRFGV. Wijzigingen aangebracht door de Opdrachtnemer zijn controleerbaar.	Eis

1.2 SaaS

Nr.	Omschrijving	Eis/wens
7	Nieuwe versies of releases van de software zullen dezelfde interfacespecificatie hebben als hun voorganger en zullen altijd volledig compatibel zijn met de hulpprogramma's, software en databestanden die door de VRFGV worden gebruikt in combinatie met de software. Dit betekent dat deze hulpprogramma's, software en databestanden niet	Eis

	hoeven te worden gewijzigd of omgebouwd als er een nieuwe versie of release van de software wordt uitgevoerd.	
8	Indien Opdrachtnemer er voor kiest om in plaats van een nieuwe versie of releases een andere software uit te brengen en te stoppen met onderhoud op de bij de VRFGV in gebruik zijnde software, dan kan de VRFGV aanspraak maken op het onverkort nakomen van het onderhoud dan wel op een gebruiksrecht op de nieuwe versie of release zonder meerkosten.	Eis
9	Indien en voor zover Opdrachtnemer software van derden al of niet in combinatie met de eigen software aan de VRFGV ter beschikking stelt, zullen, voor wat betreft die software, dezelfde voorwaarden gelden als in dit PvE gesteld.	Eis
10	Om de ICT-omgeving van de VRFGV beheersbaar en op het goede beveiligingsniveau te houden volgt de VRFGV het Microsoft Support Lifecycle-beleid. Opdrachtnemer zal zich confirmeren aan dit Microsoft Support Lifecycle-beleid.	Eis
11	Indien de Overeenkomst eindigt, doet Opdrachtnemer op eerste verzoek van de VRFGV datgene wat noodzakelijk is om een andere partij de Overeenkomst voort te laten zetten.	Eis
12	De VRFGV heeft de mogelijkheid om gebruikers/users tijdelijk of definitief op te zeggen indien deze gebruikers geen gebruik maken van de software. Dit zal moeten gebeuren met een opzegtermijn van 1 maand. Vanaf dat moment wordt betaling van de bedragen opgeschort voor de periode dat de gebruiker(s) geen gebruik maken van de software. De eventueel vooraf betaalde onderhoudsbetalingen worden met terugwerkende kracht gecrediteerd.	Eis
13	Opdrachtnemer is niet gerechtigd het gebruik van de SaaS-dienst door technische maatregelen te belemmeren of te blokkeren, behalve nadat Opdrachtnemer de VRFGV in gebreke heeft gesteld ten aanzien van een aan de VRFGV toerekenbaar tekortschieten in de nakoming van haar verplichtingen uit de Overeenkomst.	Eis

1.3 Beheer, Service en Onderhoud

Nr.	Omschrijving	Eis/wens
14	Functioneel beheer (incl.gebruikersbeheer) dient plaats te kunnen vinden met behulp van een gebruikersaccount dat beschikt over beperkte beheersrechten.	Eis

1.4 Informatiebeveiliging en Privacy

Nr.	Omschrijving	Eis/wens
15	Opdrachtnemers die persoonsgegevens verwerken van de VRFGV dienen ISO27001 / NEN-7510 gecertificeerd te zijn. Voor andere Opdrachtnemers geldt dat zij werken conform deze richtlijnen en/of andere best practices voor informatiebeveiliging. Bij andere best pratices dan ISO de bron vermelden. Verzoek aan de Opdrachtnemer om een kopie van de certificaten en Verklaring van Toepasselijkheid te verstrekken.	Eis
16	De VRFGV legt de afspraken tussen verantwoordelijke en verwerker omtrent het omgaan met persoonsgegevens vast in een verwerkersovereenkomst. Afhankelijk van de	Eis

	informatie waar een derde toegang toe verkrijgt en afhankelijk van de wijze waarop door een derde partij gegevens kunnen worden bewerkt wordt een verwerkersovereenkomst afgesloten. De VRFGV hanteert daarvoor het verwerkersovereenkomst-format zoals opgesteld door de VNG. Opdrachtnemer verklaart hierbij bereid te zijn deze verwerkersovereenkomst, incl. bijlagen en met de nodige inhoudelijke gegevens te beoordelen en te ondertekenen (eventueel na overleg met de VRFGV).	
17	De Opdrachtnemer dient mee te werken aan risicoanalyses en Data Privacy Impact Assessments (DPIA) indien de VRFGV hierom vraagt.	Eis
18	Bij de ontwikkeling van software door de Opdrachtnemer worden Security & Privacy by design als basisprincipes aangehouden. Privacy by Design is een eis uit de AVG.	Eis
19	Alle servers en (standalone) clients dienen voorzien te kunnen worden van end-point protection software	Eis
20	Van de uitgevoerde handelingen (wie, wat, wanneer) op alle niveau's (bijvoorbeeld: transactieniveau en stambestandniveau) dient logging te worden bijgehouden.	Eis
21	De logging kan na vastlegging niet meer worden aangepast.	Eis
22	Alle persoonsinformatie dient versleuteld te worden als deze wordt opgeslagen, alsmede wanneer deze getransporteerd wordt over een netwerk. De encryptiestandaard is ten minste AES-256 of complexer.	Eis
23	De software biedt bescherming tegen de in de OWASP-Top10 van 2017 en 2021 benoemde bedreigingen.	Eis
24	Bij de software wordt een Security Baseline of vergelijkbaar verstrekt, waarin onderwerpen zijn opgenomen, zoals: (parameter) die het veilig gebruik van de software aanstuurt met best practice settings; standaardgebruikers en wachtwoorden die in de software aanwezig zijn en die verwijderd moeten worden of gebruikers waarbij ten minste het default password moet worden aangepast; good/best practices t.a.v. de inrichting en het gebruik van verschillende OTA-omgevingen; welke richtlijnen moeten in acht worden gehouden bij het kopiëren van omgevingen; de instellingen die de logging aansturen; de beveiliging van de logtabellen; de beveiliging van de onderliggende database; veilige instellingen voor het OS; hoe datacommunicatie tussen de [software/hardware] en andere toepassingen veilig is in te regelen; good/best practices t.a.v. de autorisatie-inrichting. De security baseline dient zo concreet mogelijk en eenvoudig toetsbaar te zijn tijdens een audit.	Eis
25	De Opdrachtnemer biedt de mogelijkheid om de toets aan de security baseline geautomatiseerd te laten uitvoeren of beter, de security baseline (configureerbaar) kan worden afgedwongen.	Wens
26	De dienst die geboden wordt biedt ransomware-protectie	Eis
27	De VRFGV kan, voordat in productie wordt gegaan, een penetratietest uitvoeren op de software. Een penetratietest is een test waarin pogingen worden gedaan om in te breken op de software. De bevindingen die hieruit voortvloeien en die betrekking hebben op de software van Opdrachtnemer zullen door Opdrachtnemer opgepakt en uitgevoerd worden, zonder additionele kosten, zodat de software voldoet aan de relevante maatstaven.	Wens
28	Opdrachtnemer maakt alleen gebruik van (ISO 27001 gecertificeerde) Europese onderaannemers voor bijvoorbeeld hosting in een datacentrum.	Eis

29	Opdrachtnemer heeft indien relevant gelijkstrekkende verwerkersovereenkomsten afgesloten met zijn onderaannemers. Een kopie van de verwerkersovereenkomsten dient beschikbaar gesteld te worden aan de VRFGV.	Eis
30	Opdrachtnemer heeft adequate processen ingericht voor autorisatie, authenticatie en wachtwoordbeleid voor zijn medewerkers, die waarborgen dat alleen bij-de-VRFGV-bekende gebruikers toegang hebben tot de gegevens van de VRFGV.	Eis
31	Bij het aanbieden van een externe inlogmogelijkheid wordt een vulnerabilityscan uitgevoerd vanaf het internet. Geconstateerde hoogkritische lekken worden door de Opdrachtnemer direct verholpen voordat de portal (weer) in productie gaat.	Eis
32	Onveilige protocollen (zoals oa HTTP/FTP/Telnet) waarvoor een veilig alternatief bestaat zijn niet toegestaan.	Eis
33	Beveiligingsupdates worden gedurende de gehele levensduur van het systeem beschikbaar gesteld en worden uitgevoerd als onderdeel van de support gedurende de levensduur van het de software.	Eis
34	Er worden geen onpersoonlijke accounts toegestaan/de default aanwezige accounts zijn uit te schakelen.	Eis
35	Opdrachtnemer kan een SOC-2 type 2 dan wel ISAE3402-assurancerapport overleggen over de ICT-dienstverlening.	Eis