Belastingdienst

BIJLAGE 1A

Belastingdienst / SSO Centrum voor facilitaire dienstverlening

NON-FUNCTIONAL REQUIREMENTS

IUC20-694 Assessment Tests

Behorende bij : IUC20-694 Openbare aanbesteding ‘Assessment Tests’

INHOUDSOPGAVE

Hoofdstuk 1. Doel van dit document ... 3

Hoofdstuk 2. Non-functionele eisen ... 4

2.1. Opbouw van de dienst ... 4

2.2. Wet- en regelgeving ... 5

2.3. Beveiliging ... 5

2.3.1. Overheidsbeleid ... 5

2.3.2. Verplichte Overheidsmaatregelen ... 6

2.3.3. Opdrachtgever specifieke eisen ... 7

2.4. Presentatie van de oplossing ... 8

2.5. Autorisatie en Authenticatie ... 8

2.6. Gegevens ... 9

2.6.1. Gegevens in rust ... 9

2.6.2. Gegevens in transitie ... 9

2.6.3. Verwerken van gegevens ... 9

2.6.4. Omgang met gegevens ... 10

2.6.5. Beveiliging van gegevens ... 10

2.6.6. Anonimiseren en pseudonimiseren van gegevens ... 10

2.7. Aansluitvoorwaarden ... 10

2.7.1. Richtlijnen Webapplicaties ... 10

2.7.2. Richtlijnen Webcamtest ... 11

2.7.3. Koppelingen ... 11

2.8. Bewaken van de Oplossing ... 11

2.9. Testen en Verifiëren van de Oplossing ... 11

Hoofdstuk 3. Beheer van de Oplossing ... 13

3.1. Service Level management ... 13

3.1.1. Service Level Agreement ... 13

3.1.2. Beschikbaarheid ... 13

3.2. Incident management ... 14

3.3. Helpdesk en Service window ... 14

3.4. Security management ... 14

3.5. Business Continuity management ... 15

3.6. Availability management ... 15

3.7. Service Level Rapportage ... 15

Hoofdstuk 4. Implementatie ... 16

Hoofdstuk 1. Doel van dit document

Dit document beschrijft de gunningseisen die de Aanbestedende dienst stelt aan Non-functionals in het kader van de Europese aanbesteding IUC20-694 "Assessment Tests". Dit document maakt integraal onderdeel uit van het beschrijvend document en is van toepassing wanneer u inschrijft op Perceel 1 en/of Perceel 2.

Non-functionals zijn eisen die aan een informatiesysteem (website/applicatie, dienst of product), gesteld worden. Deze eisen staan los staan van wat de gebruiker met het informatiesysteem wel of niet kan.

1.1. Eisen

De Aanbestedende dienst heeft geen voorkeur voor bepaalde Inschrijvers, noch voor bepaalde merken, types, fabricaten, herkomst e.d. Als er wordt gerefereerd aan bepaalde fabricaten, merken, typen, specifieke standaarden en dergelijke, dan dient dit te worden gelezen met de toevoeging "of daaraan gelijkwaardig".

Aan eisen moet worden voldaan. Het niet voldoen aan een eis betekent uitsluiting van verdere beoordeling en wordt de inschrijving terzijde gelegd (knock-out criterium).

Inschrijvers dienen te voldoen aan alle opgenomen eisen die de Aanbestedende dienst heeft geformuleerd ten aanzien van de te leveren prestatie. Eisen worden als volgt weergegeven:

EIS 1	**Gunningseisen** Aan een gunningseis moet worden voldaan op het moment van inschrijving. Als niet is voldaan aan een gunningseis dan wordt tot uitsluiting overgegaan.

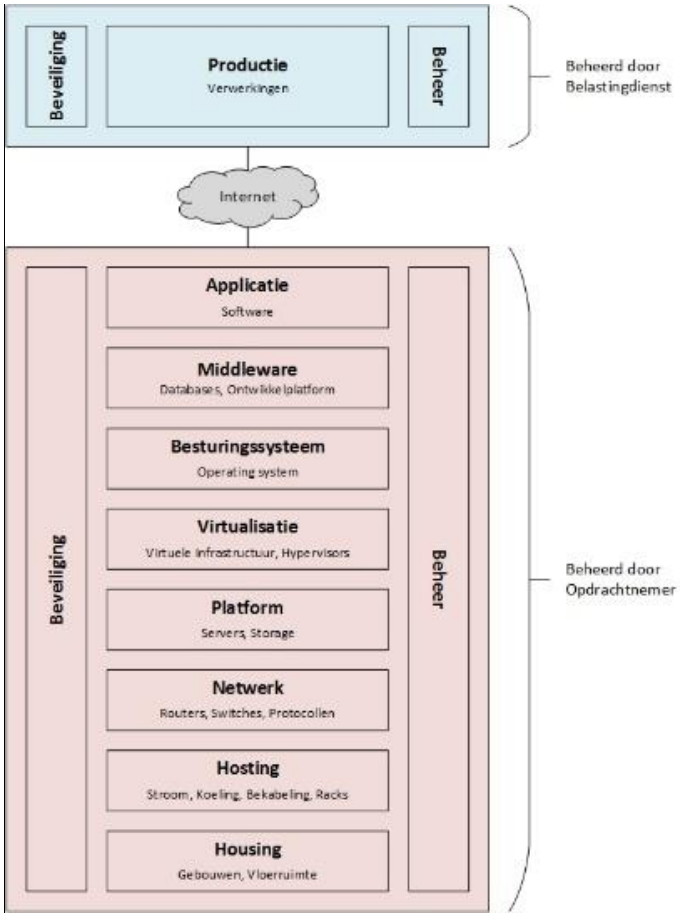
UE 1.	**Uitvoeringseisen** Voorwaarden waar opdrachtnemer zich bij de uitvoering van de opdracht aan dient te houden zijn uitvoeringseisen. De uitvoeringseisen zijn opgenomen in dit document. Door het indienen van een inschrijving gaat u onvoorwaardelijk akkoord met het voldoen aan de uitvoeringseisen gedurende de uitvoering van de overeenkomst.

Hoofdstuk 2. Non-functionele eisen

2.1. Opbouw van de dienst

De Oplossing voor perceel 1 'Psychologische instrumenten', is een SaaS-oplossing. Voor perceel 2 'Programmeerproeve' heeft Inschrijver de keuze om een SaaS-oplossing of een standalone oplossing aan te bieden.

Ten aanzien van de SaaS-oplossing is de verdeling in verantwoordelijkheidsgebieden tussen Opdrachtnemer en Opdrachtgever opgenomen in de onderstaande Figuur 1:



Figuur 1 - Opbouw van de dienst

Indien Inschrijver voor perceel 2 een standalone functionaliteit aanbiedt, is de Opdrachtnemer verantwoordelijk voor het beschikbaarstellen van de benodigde apparatuur en software.

De Opdrachtgever wil dat de Oplossing uit één geheel bestaat en dat te allen tijde de Opdrachtnemer verantwoordelijk is voor alle in de Aanbestedingsstukken gestelde eisen van de Oplossing. Dit laat onverlet dat de Opdrachtnemer delen van de Oplossing kan en mag uitbesteden aan derden.

EIS 1	De Opdrachtnemer levert per aangeboden Assessment test de Oplossing als één integraal werkend systeem.

2.2. Wet- en regelgeving

De Opdrachtgever hecht veel belang aan de beveiliging van Gegevens en heeft de taak en de verantwoordelijkheid om er voor te zorgen dat Gegevens nooit in onbevoegde handen vallen of kunnen vallen.

De Opdrachtnemer dient alle passende en nodige maatregelen te hebben getroffen en te treffen om de Opdrachtgever in staat te stellen deze taak uit te voeren en haar verantwoordelijkheid te kunnen nemen.

Een belangrijk kader in de te nemen beveiligingsmaatregelen is de vigerende wetgeving en standaarden ten aanzien van ICT-beveiliging en privacy.

EIS 2	De Oplossing voldoet aan de algemene vigerende wet- en regelgeving, waaronder en niet beperkt tot de Algemene Verordening Gegevensbescherming (AVG). Partijen zullen voldoen aan hun respectievelijke verplichtingen onder de van toepassing zijnde wet- en regelgeving ter bescherming van persoonsgegevens (zoals de Algemene Verordening Gegevensbescherming) met betrekking tot alle persoonsgegevens die bij de uitvoering van deze Overeenkomst worden verwerkt.

EIS 3	De verplichtingen in onderhavige bijlage gelden niet alleen voor Opdrachtnemer, maar ook voor de eventuele onderaannemer(s). Opdrachtnemer verplicht zich er hierbij toe deze verplichtingen met de onderaannemer(s) vooraf schriftelijk overeen te komen en de naleving ervan te controleren.

2.3. Beveiliging

De Opdrachtgever is gehouden aan de Baseline Informatiebeveiliging Overheid (BIO versie 1.04). Dit overheidsbeleid is gebaseerd op de ISO27001 en de ISO27002 en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde verplichte overheidsmaatregelen.

Daarnaast stelt de Opdrachtgever zelf ook beveiligingseisen, de zogenaamde Opdrachtgever specifieke eisen. De eisen worden in deze paragraaf verder toegelicht.

2.3.1. Overheidsbeleid

De Opdrachtnemer is niet direct gehouden aan de Baseline Informatiebeveiliging Overheid omdat dit stelsel geldt voor overheidspartijen, zoals de Belastingdienst. Echter, de Opdrachtnemer dient de Opdrachtgever in staat te stellen om haar verantwoordelijkheid te kunnen nemen.

Door ISO 27001 certificering kunt u deels aantonen dat u voldoet aan het overheidsbeleid op het gebied van informatiebeveiliging ten aanzien van de Oplossing. Het stelt de Opdrachtgever in staat om aan een deel van haar verplichten ten aanzien van de BIO te voldoen.

EIS 4	Op het moment dat de Opdrachtgever de Oplossing accepteert om in Productie te nemen, is de Opdrachtnemer voor het leveren van de dienst ISO 27001 of gelijkwaardig gecertificeerd en blijft dit voor ten minste de duur van de Raamovereenkomst. De Opdrachtnemer toont dit aan door de Statement of Applicability te overleggen, uitgevoerd door een geaccrediteerd instituut.

2.3.2. Verplichte Overheidsmaatregelen

Naast de ISO 27001 of gelijkwaardige certificering zijn een aantal maatregelen vanuit de Baseline Infomatiebeveiliging Overheid (BIO versie 1.04) ook voor de Opdrachtnemer verplicht. Het betreft:

Nr.	Control	Maatregel
6.1.2.1	Scheiding van taken	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
9.2.5.1	Beoordeling van toegangsrechten van gebruikers	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.
9.2.5.2	Beoordeling van toegangsrechten van gebruikers	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.
9.4.1.1	Beperking toegang tot informatie	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.
9.4.1.2	Beperking toegang tot informatie	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
9.4.3.1	Systeem voor wachtwoordbeheer	Als er geen gebruik wordt gemaakt van Two factor authentication is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een Account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.
9.4.4.1	Speciale systeemhulpmiddelen	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.
12.4.2.1	Beschermen van informatie in logbestanden	Er is een overzicht van logbestanden die worden gegenereerd.
12.4.2.3	Beschermen van informatie in logbestanden	Er is een (onafhankelijke) interne Audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.
12.4.2.4	Beschermen van informatie in logbestanden	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident.
12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.
13.2.3.1	Elektronische berichten	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.
15.1.2.4	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd. In onderhavige aanbesteding wordt de Algemene Rijksinkoopvoorwaarden 2018 (ARIV-2018) gehanteerd.

Tabel 1 - Verplichte overheidsmaatregelen

EIS 5	De Opdrachtnemer voldoet aan de overheidsmaatregelen zoals gespecificeerd in Tabel 1.

2.3.3. Opdrachtgever specifieke eisen

Aanvullend op de ISO27001- of gelijkwaardige certificering en een aantal maatregelen uit de BIO wil de Opdrachtgever dat de Opdrachtnemer aan een aantal specifieke Eisen voldoet.

EIS 6	De Opdrachtgever heeft het recht om één keer per jaar een A&P test te laten uitvoeren om de beveiliging te testen. De Opdrachtgever contracteert hierbij zelf een onafhankelijk bureau dat de testen uitvoert. Opdrachtnemer en de Opdrachtgever besluiten gezamenlijk de scope van de A&P test. Mochten partijen er niet gezamenlijk uit komen, dan neemt de Opdrachtgever de uiteindelijke beslissing hierover. A&P tests zijn enkel toetsend en vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer. De kosten van de uitvoering van deze test zijn voor rekening van de Opdrachtgever. Opdrachtnemer werkt kosteloos mee aan A&P testen. Bevindingen uit A&P testen dienen op kosten van Opdrachtnemer opgelost te worden. De resultaten van de testen worden gedeeld met Opdrachtnemer. Bij het bespreken van de bevindingen worden indien van toepassing afspraken gemaakt over de oplostijden en de aansluitende hertest. De aansluitende hertest na de eerste gedane A&P test is voor rekening van de Opdrachtnemer.

De Opdrachtgever wil de mogelijkheid hebben om nieuwe kwetsbaarheden te detecteren en vast te stellen dat bestaande Kwetsbaarheden zijn opgelost. Dit is aanvullend op de eisen t.a.v. de andere A&P tests.

EIS 7	De Opdrachtgever heeft het recht om Vulnerability scans op de Oplossing uit te laten voeren door het Security Operation Center (SOC) van de Opdrachtgever. Opdrachtnemer zorgt ervoor dat het SOC de benodigde toegang heeft om deze scan uit te voeren. De Bevindingen worden indien nodig gedeeld en besproken met de Opdrachtnemer. Gevonden kwetsbaarheden worden op eigen kosten opgelost door Opdrachtnemer. Opdrachtnemer werkt kosteloos mee aan de Vulnerability scans die door de Opdrachtgever wordt uitgevoerd. Vulnerability scans vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer.

EIS 8	Kwetsbaarheden worden gekwalificeerd doormiddel van het Common Vulnerability Scoring System 3.0 (CVSS 3.0). Kritische bevindingen (Critical) dienen per direct te worden weggenomen door de Opdrachtnemer. Voor hoge risicobevindingen (High risk) geldt dat deze binnen uiterlijk een maand zijn weggenomen door de Opdrachtnemer.

	Voor kwetsbaarheden die geclassificeerd zijn als Gemiddeld en Laag worden termijnen van respectievelijk drie en zes maanden gehanteerd (Comply). Indien er gegronde redenen zijn om een kwetsbaarheid geclassificeerd als Gemiddeld of Laag, niet te verhelpen dient de Opdrachtnemer hiervoor een motivatie op te leveren (Explain) aan de Opdrachtgever en deze motivatie voor akkoord te laten verklaren door de Opdrachtgever. Opdrachtnemer draagt de kosten voor het wegnemen van de risico's.

EIS 9	De Opdrachtgever heeft het recht om minimaal 1 keer per jaar een Audit uit te laten voeren om de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de Oplossing te toetsen. De Opdrachtgever kiest hierbij zelf welk onafhankelijk bureau de Audit uitvoert. De resultaten van de Audit worden, in de vorm van een Third Party Memorandum, gedeeld met Opdrachtnemer. Bij het bespreken van de bevindingen worden afspraken gemaakt over de te nemen vervolgstappen. De Opdrachtnemer werkt kosteloos mee aan de te nemen vervolgstappen.

2.4. Presentatie van de oplossing

Eis 10 en 11 geldt enkel bij een SaaS-oplossing. Indien Inschrijver voor perceel 2 een stand-alone oplossing (op locatie) aanbiedt, waarbij Inschrijver zelf devices regelt waarop de testen gemaakt worden gelden Eis 10 en Eis 11 niet.

EIS 10	De oplossing dient een 'zero-client footprint' te hebben. Dat wil zeggen er is, naast een webbrowser, geen additionele software, browser-plugin of additionele hardware nodig op de gebruikersapparaten om alle gevraagde functionaliteit van de Oplossing te kunnen benaderen.

EIS 11	De Oplossing is apparaat-onafhankelijk te gebruiken op gangbare gebruikersapparaten die over een webbrowser beschikken. De volledige functionaliteit van de Oplossing wordt ondersteund door de vier meest gangbare webbrowsers. Op het moment van publicatie zijn dat: Google Chrome, Microsoft Edge, Mozilla Firefox en Apple Safari. De Oplossing ondersteunt minimaal de huidige versie en de voorgaande versie van de webbrowsers welke nog actief worden ondersteund door de leverancier van de webbrowser.

2.5. Autorisatie en Authenticatie

EIS 12	Indien de Oplossing gebruik maakt van een API-koppeling met een ander systeem, wordt deze API-koppeling altijd geauthenticeerd op basis van een veilige en geaccepteerde methode (zoals certificaten of een complexe UserID/Password-combinatie. Hierbij is eenduidigheid t.a.v. het ontwerp van de API gedefinieerd. Voorbeelden: • Standaardisatie: https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules • Protocol: OAuth2.0

2.6. Gegevens

2.6.1. Gegevens in rust

Opdrachtgever kent voorschriften t.a.v. locatie waar de gegevens worden opslagen.

EIS 13	Gegevens van de Opdrachtgever worden binnen de Europese Unie / Europese Economische Ruimte (EU/EER) opgeslagen. Gedurende de levenscyclus van de Gegevens, blijven deze Gegevens binnen de EU/EER.

EIS 14	Opdrachtnemer zal geen persoonsgegevens doorgeven of laten doorgeven door diens aannemers of onderaannemers naar landen buiten de EU/EER zonder de uitdrukkelijke voorafgaande schriftelijke toestemming van de Opdrachtgever. Zodra er nieuwe regelgeving is op het gebied van persoonsgegevens, zullen partijen in overleg treden en de overeenkomst op dit punt aanvullen zodat deze overeenkomst niet afwijkt van de geldende regelgeving.

2.6.2. Gegevens in transitie

EIS 15	Opdrachtnemer dient gebruik te maken van versleuteling voor de uitwisseling van informatie tussen de Oplossing en andere partijen. Versleuteling van de Gegevens geschiedt met een door National Institute of Standards and Technology (NIST) of Nationaal Cyber Security Centrum (NCSC) aanbevolen encryptie-algoritmes van bij voorkeur 256 bits.

2.6.3. Verwerken van gegevens

EIS 16	Opdrachtnemer zal zonder de uitdrukkelijke voorafgaande schriftelijke goedkeuring van de Opdrachtgever slechts persoonsgegevens verwerken voor zover noodzakelijk is voor het uitvoeren van de Raamovereenkomst. Opdrachtnemer zal geen persoonsgegevens verplaatsen of doorgeven aan bedrijven of bedrijfsonderdelen, gevestigd in territoria buiten de EU/EER, of in derde landen, zonder de uitdrukkelijke voorafgaande schriftelijke goedkeuring van de Opdrachtgever. In het specifieke geval dat de Opdrachtgever goedkeuring geeft aan verplaatsing van persoonsgegevens buiten de EU/EER, met inachtneming van het in de vorige volzin gestelde, zal Opdrachtnemer de daaraan verbonden verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG) nakomen, waaronder het aangaan van EU Model Clauses met de verwerkende identiteit buiten de EU.

EIS 17	Opdrachtnemer garandeert dat alle data en persoonsgegevens die in verband met de uitvoering van de Raamovereenkomst door Opdrachtnemer ten behoeve van de Opdrachtgever zijn verwerkt, zullen worden vernietigd na beëindiging van de Raamovereenkomst.

EIS 18	Op verzoek van de Opdrachtgever worden bij beëindiging van de Raamovereenkomst, Gegevens van de Opdrachtgever binnen een van te voren afgesproken aantal dagen ter beschikking gesteld, in een voor de Opdrachtgever bruikbaar van te voren afgesproken digitaal formaat. Aanlevering gebeurt via een beveiligde verbinding. De Opdrachtgever levert hiervoor een beveiligde dienst. De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele- en technische beschrijving dat in de toekomst een datamigratie naar een

	nieuwe Oplossing kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.

2.6.4. Omgang met gegevens

EIS 19	Behalve wanneer de Opdrachtgever uitdrukkelijk anders bepaalt of voor zover Opdrachtnemer hiertoe wettelijk verplicht is, zal Opdrachtnemer geen data en of persoonsgegevens aan enige andere partij bekendmaken, anders dan aan medewerkers en betrokken onderaannemers voor wie een dergelijke bekendmaking noodzakelijk is om de gecontracteerde dienstverlening uit te voeren, en uitsluitend in de mate waarin het nodig is voor een daartoe bevoegde partij. Indien Opdrachtnemer ten gevolge van een wettelijke verplichting data en of persoonsgegevens aan een andere partij bekend moet maken, zal Opdrachtnemer dit (indien toegestaan) van tevoren met de Opdrachtgever bespreken. Opdrachtnemer zal geen persoonsgegevens gebruiken voor eigen doeleinden anders dan noodzakelijk voor de uitvoering van de Raamovereenkomst.

EIS 20	Opdrachtnemer zal naar beste vermogen meewerken aan alle redelijke procedures en processen betreffende de omgang met persoonsgegevens die de Opdrachtgever aan Opdrachtnemer heeft bekendgemaakt.

2.6.5. Beveiliging van gegevens

EIS 21	Opdrachtnemer draagt zorg voor alle redelijke technische en organisatorische maatregelen om vernietiging van of schade aan data of persoonsgegevens te voorkomen, inclusief maar niet beperkt tot de betrouwbaarheid van werknemers die toegang hebben tot deze data of persoonsgegevens. Opdrachtnemer heeft tenminste de als normaal geldende standaardsystemen en procedures ingericht om de veiligheid en vertrouwelijkheid van data en persoonsgegevens te beschermen tegen bedreigingen en gevaren van deze data en persoonsgegevens en tegen niet geautoriseerde toegang tot of gebruik van deze data en persoonsgegevens.

2.6.6. Anonimiseren en pseudonimiseren van gegevens

Het anonimiseren en/of pseudonimiseren van informatie heeft een positief effect op de zwaarte van de beveiligingseisen. De Opdrachtgever hecht daarom veel waarde aan het kunnen anonimiseren en/of pseudonimiseren van persoonsgegevens.

EIS 22	De Oplossing ondersteunt slechts het gebruik van ge-anonimiseerde- en/of gepseudonimiseerde gegevens bij verzending en opslag voor het uitvoeren van de gevraagde functionaliteit vanuit het Assessment-portaal. Voor Perceel 2 geldt deze eis alleen wanneer de Oplossing als een SaaS-oplossing wordt aangeboden en gebruik wordt gemaakt van koppeling met het assessmentportaal.

2.7. Aansluitvoorwaarden

2.7.1. Richtlijnen Webapplicaties

EIS 23	De Oplossing voldoet aan de beveiligingsrichtlijnen voor webapplicaties. Zie https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.

2.7.2. Richtlijnen Webcamtest

EIS 24	Voordat een kandidaat de Webcamtest uitvoert, wordt de kandidaat schriftelijk, via een pop up waarin een leesbevestiging moet worden gegeven, op het volgende geattendeerd: • De kandidaat wordt bewust gemaakt van het feit dat men in een digitale omgeving zit, die kwetsbaar kan zijn voor cyberdreigingen; • De kandidaat wordt bewust gemaakt van de omgeving waarin de Webcamtest gebruikt wordt (meeluisteren door derden, de fysieke ruimte die in beeld komt, afsluiten van het gesprek na afronding); • De kandidaat wordt bewust gemaakt van het feit dat wat besproken wordt in principe openbaar zou kunnen worden.

EIS 25	Voordat een kandidaat de Webcamtest uitvoert, wordt de kandidaat schriftelijk het volgende geadviseerd: • Maak gebruik van een vertrouwd en beveiligd wifinetwerk; • Zorg voor een actuele virusscanner; • Houd je systemen up-to-date: installeer updates zodra deze door de leverancier beschikbaar worden gesteld; • Wees extra alert op phishingmail.

2.7.3. Koppelingen

De Oplossing zal in staat moeten zijn om te koppelen met oplossingen van derden die geen onderdeel zijn van de Oplossing. Dit moet het mogelijk maken om in de toekomst gegevens tussen andere autonome systemen en de Oplossing uit te kunnen wisselen.

EIS 26	Alle relevante API's van de Oplossing ten aanzien van koppelingen en gegevensuitwisseling met andere autonome systemen van derden (indien van toepassing) zijn gedocumenteerd. Deze API-documentatie is actueel, correct en wordt op verzoek beschikbaar gesteld aan de Contractmanager van de Opdrachtgever.

De API-documentatie geeft inzicht in de koppelbaarheid en de Beveiliging daarvan.

2.8. Bewaken van de Oplossing

De Opdrachtgever wil zicht krijgen op afwijkingen om herstelacties te kunnen formuleren.

EIS 27	De oplossing wordt door Opdrachtnemer continu gemonitord op beveiligingsaspecten, Capaciteit, Performance en Beschikbaarheid.

2.9. Testen en Verifiëren van de Oplossing

De Opdrachtgever behoudt zicht het recht voor de eisen te toetsen middels een Verificatie.

EIS 28	De Opdrachtgever heeft het recht na voorlopige Gunning alle eisen in de aanbestedingsdocumenten te toetsen m.b.v. een Verificatie.

Voor in productiename van de Oplossing wordt een Acceptatietest door de Opdrachtgever uitgevoerd. Er kan worden getest op alle eisen uit de aanbestedingsdocumenten.

EIS 29	De Opdrachtgever behoudt zich het recht voor om vóór in productiename eisen en wensen uit de aanbestedingsdocumenten te testen in een Acceptatietest. Opdrachtnemer dient hieraan kosteloos mee te werken.

	De bevindingen van de Acceptatietest worden door de Opdrachtnemer opgelost voordat door de Opdrachtgever kan worden overgegaan tot het in productienemen van de Oplossing. Tenzij dit anders met de Opdrachtgever is overeengekomen.

De Opdrachtgever wil voorkomen dat er enkel op basis van de A&P test van de leverancier een kwetsbare Oplossing naar productie wordt gebracht.

EIS 30	De Opdrachtgever behoudt zich het recht voor om een A&P-test uit te voeren als onderdeel van de Acceptatietest vóór in Productiename van de Oplossing. Opdrachtnemer dient hieraan kosteloos mee te werken. Kwetsbaarheden met de classificatie critical of high (conform CVSS 3.0) worden door de Opdrachtnemer opgelost voordat door de Opdrachtgever overgegaan kan worden tot het in productienemen van de Oplossing.

De Opdrachtgever wil voorkomen dat er in testomgevingen van de Opdrachtnemer Persoonsgegevens uit de Productieomgeving worden gebruikt.

EIS 31	Bij het testen van de Oplossing mag geen gebruik worden gemaakt van naar Natuurlijke Personen herleidbare gegevens. Indien het voor het testen van de Oplossing noodzakelijk is om gegevens te gebruiken die herleidbaar zijn naar individuen dienen acceptabele beveiligingsmaatregelen te zijn getroffen en dienen deze door Opdrachtgever te zijn goedgekeurd.

Hoofdstuk 3. Beheer van de Oplossing

3.1. Service Level management

3.1.1. Service Level Agreement

De Opdrachtgever sluit met de Opdrachtnemer een Service Level Agreement (SLA) af, aangaande de te leveren Oplossing. De SLA bevat een beschrijving van de vastgestelde normen in de vorm van Service levels.

EIS 32	De Opdrachtgever sluit bij de start van de contractfase (binnen 3 weken na ondertekening van de Raamovereenkomst) met Opdrachtnemer een Service Level Agreement (SLA), op basis van een standaard (zie eis 33) SLA die wordt gehanteerd voor het leveren van de gevraagde Oplossing. Opdrachtnemer levert na de bezwaarperiode de SLA op ter ondertekening.

3.1.2. Beschikbaarheid

EIS 33	**Perceel 1:** De Oplossing voldoet minimaal aan de volgende Service Levels m.b.t. de beschikbaarheid van de Oplossing: • 7*24 uur openstelling van de gehele Oplossing voor gebruik door de Opdrachtgever; • Norm: beschikbaarheid van 99% per maand (= maximaal 7,20 uur downtijd per maand); • Beschikbaarheid is exclusief downtime bij implementaties van wijzigingen ten aanzien van de Oplossing op verzoek van de Opdrachtnemer. <u>Berekening van Beschikbaarheid</u> • Berekening Beschikbaarheid: (gerealiseerd aantal uren Beschikbaarheid/overeengekomen uren Beschikbaarheid) * 100%, • Overeengekomen aantal uren Beschikbaarheid = aantal uren Openstellingstijden – (aantal uren gepland Technisch Beheer en Onderhoud en/of maintenance tijdens Openstelling), • Gerealiseerd aantal uren Beschikbaarheid = overeengekomen aantal uren Beschikbaarheid – som van de Oplostijden van prio 1 Incidenten. **Perceel 2:** Indien de Oplossing als een SaaS-oplossing wordt aangeboden, voldoet de Oplossing minimaal aan de volgende Service Levels m.b.t. de beschikbaarheid van de Oplossing: • 7*24 uur openstelling van de gehele Oplossing voor gebruik door de Opdrachtgever; • Norm: beschikbaarheid van 99% per maand (= maximaal 7,20 uur downtijd per maand); • Beschikbaarheid is exclusief downtime bij implementaties van wijzigingen ten aanzien van de Oplossing op verzoek van de Opdrachtnemer. Indien de Oplossing als standalone functionaliteit wordt aangeboden, is de Opdrachtnemer verantwoordelijk voor de beschikbaarheid van de benodigde apparatuur en software. <u>Berekening van Beschikbaarheid</u> • Berekening Beschikbaarheid: (gerealiseerd aantal uren Beschikbaarheid/overeengekomen uren Beschikbaarheid) * 100%,

	• Overeengekomen aantal uren Beschikbaarheid = aantal uren Openstellingstijden – (aantal uren gepland Technisch Beheer en Onderhoud en/of maintenance tijdens Openstelling), • Gerealiseerd aantal uren Beschikbaarheid = overeengekomen aantal uren Beschikbaarheid – som van de Oplostijden van prio 1 Incidenten.

3.2. Incident management

Kandidaten melden incidenten altijd bij het backoffice van het team Assessments van de Opdrachtgever. De Opdrachtgever meldt incidenten vervolgens bij Opdrachtnemer. Voor Perceel 2 geldt dat kandidaten incidenten tevens aan de begeleider op locatie mogen melden, indien van toepassing.

EIS 34	Incidenten mogen alleen door medewerkers van het backoffice van het team Assessments van de Opdrachtgever gemeld worden bij Opdrachtnemer. Gebruikers mogen incidenten nooit direct bij Opdrachtnemer melden. Voor Perceel 2 geldt dat kandidaten incidenten wel aan de begeleider van Opdrachtnemer ter plekke mogen melden.

EIS 35	De Oplossing stelt de Gebruiker op ieder moment van de test informatie (telefoonnummer) ter beschikking, waarmee de Gebruiker het team Assessments van de Opdrachtgever tijdens reguliere openingstijd (zie eis 38) op de hoogte kan stellen van een incident.

3.3. Helpdesk en Service window

EIS 36 De Opdrachtnemer voldoet minimaal aan de volgende normen:

Omschrijving	Indicator	Norm
Openstelling Helpdesk Opdrachtnemer	Reguliere Openingstijd	Maandag t/m Vrijdag 08:00 – 17:00 Nederlandse tijd
	Stand-by Openingstijd service desk voor melden Prio 1 Incidenten	7*24 uur
Monitoring en alerting	Opdrachtnemer heeft een monitoring en alerting proces ingericht om direct (binnen 2 klokuren, conform reactietijd Prio1) te kunnen handelen in geval van Incidenten en (dreigende) verstoring van de beschikbaarheid van de oplossing	7*24 uur

3.4. Security management

EIS 37	Beveiligingsincidenten zijn incidenten die een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van de data in informatieverwerkende systemen hebben. Beveiligingsincidenten dienen door de Opdrachtnemer altijd als volgt te worden geclassificeerd: • Impact: Hoog • Urgentie: Hoog Onder Beveiligingsincidenten worden in ieder geval de onderstaande incidenten bedoeld: • (Poging tot) Cyberinbraak;

	• Responsible Disclosure; • Common Vulnerability en Exposures (CVE) en Security Notes en NCSC-kennisgevingen; • Bevindingen A&P-test.

EIS 38	Opdrachtnemer informeert de Opdrachtgever onmiddellijk wanneer er een beveiligingsincident wordt geconstateerd of redelijkerwijs verwacht, ten aanzien van de data en/of persoonsgegevens van de Opdrachtgever. Opdrachtnemer zal in dat geval tevens de omvang van het incident aangeven alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. Dit onverminderd de wettelijke verplichting van Opdrachtnemer, als verwerkingsverantwoordelijke, om datalekken te melden bij de Autoriteit Persoonsgegevens.

EIS 39	Een beveiligingsincident wordt altijd per direct opgevolgd met een actie van de Opdrachtnemer.

3.5. Business Continuity management

EIS 40	De oplossing voldoet aan onderstaande eisen betreffende de Operationele continuiteit in geval van een Calamiteit (crisis): • Recovery Time Objective (RTO): De Oplossing is binnen 48 klokuren weer volledig functioneel beschikbaar; • Recovery Point Objective (RPO): Er is maximaal 24 klokuren verlies van Gegevens toegestaan. Voor Perceel 2 geldt dat deze eis enkel van toepassing is als de Oplossing aangeboden wordt als SaaS-oplossing.

3.6. Availability management

EIS 41	De Oplossing heeft een Maintenance Mode (Sorry-pagina), waarmee de Gebruiker op de hoogte wordt gesteld van de onbeschikbaarheid. In geval van Geplande niet-beschikbaarheid wordt de Gebruiker geïnformeerd over de duur van de onbeschikbaarheid. Voor Perceel 2 geldt dat deze eis enkel van toepassing is als de Oplossing aangeboden wordt als SaaS-oplossing.

3.7. Service Level Rapportage

EIS 42	Opdrachtnemer levert ieder kwartaal een Service Level Rapportage op aan de Contractmanager van de Opdrachtgever. De Opdrachtgever verwacht van de Service Level Rapportage dat hierin minimaal de onderstaande aspecten meegenomen zijn: • KPI Performance; • KPI overzicht Beschikbaarheid; • KPI opgeloste Incidenten binnen SLA en buiten SLA; • KPI opgeloste Beveiligingsincidenten binnen SLA en buiten SLA; • Status, voortgang en afhandeling van openstaande en opgeloste vragen, Incidenten, Problems en verbetervoorstellens; • Datum A&P-testen; • Datum ISO-certificering (of gelijkwaardige certificering).

Hoofdstuk 4. Implementatie

Let op! Dit hoofdstuk is enkel van toepassing op Perceel 1.

De Opdrachtnemer dient de leiding te nemen bij de Implementatie van de Oplossing. Om inzicht te krijgen op welke wijze de Opdrachtnemer de Implementatie uit gaat voeren, wordt tijdens de implementatiefase een Plan van Aanpak gevraagd dat door de Opdrachtgever wordt beoordeeld.

EIS 43	Inschrijver levert bij zijn Inschrijving een Plan van Aanpak voor de Implementatie van de Oplossing.

EIS 44	Opdrachtnemer heeft een resultaatverplichting voor het gebruiksklaar opleveren van de Oplossing conform de implementatieplanning zoals bedoeld in EIS 43. Het in Gebruik nemen van de Oplossing vindt plaats na Acceptatie van de Oplossing door de Opdrachtgever.

EIS 45	Het door Inschrijver in te dienen Plan van Aanpak, vormt de basis voor de wijze waarop de Oplossing wordt geimplementeerd. Het Plan van Aanpak zal binnen 2 weken na het ondertekenen van de Raamovereenkosmt tussen Opdrachtnemer en de Opdrachtgever worden besproken en vastgesteld. Pas nadat er akkoord is van de Opdrachtgever zal worden gestart met het uitvoeren van de Implementatie.