BIJLAGE 5 – Programma van Eisen

In deze bijlage staan de gestelde eisen met betrekking tot de opdracht.

ALGEMENE EISEN

Eisen aan het in te zetten personeel

	Eis	Perceel		
1.	Het personeel dat betrokken is bij de uitvoering van de opdrachten voor ICTU heeft minimaal HBO-werk- en denkniveau, minimaal twee jaar werkervaring met het betreffende type werk en is Nederlandssprekend en -schrijvend.	1	2	3
2.	Personeel dat de opdrachten uitvoert voor ICTU dient te beschikken over een Verklaring omtrent Gedrag (VOG). ICTU stelt de VOG-aanvraag op, het personeel van opdrachtnemer vraagt de VOG aan. De kosten van de VOG zijn voor opdrachtnemer. De VOG wordt beschikbaar gesteld aan ICTU voorafgaande aan de start van de werkzaamheden.	1	2	3

Eisen aan de nadere overeenkomsten

	Eis	Perceel		
3.	Opdrachtnemer brengt altijd (100%) binnen vijf werkdagen na ontvangst van de offerteaanvraag een nadere offerte uit. De nadere offerte bevat minimaal: samenstelling van het team dat de opdracht uitvoert met een beknopt CV (max. 1 A4) van elk teamlid, de planning van de doorlooptijd van start tot eindrapportage en de kosten (in het geval van perceel 2 op basis van de in de raamovereenkomst opgenomen tarieven). Bij het uitvragen onder een mini-competitie onder perceel 2, dienen Opdrachtnemers binnen tien werkdagen na ontvangst van de offerteaanvraag een nadere offerte uit te brengen.	1	2	3
4.	ICTU kan de startdatum tot tien werkdagen van tevoren in een latere startdatum wijzigen tot een maximaal uitstel van 40 werkdagen. Indien ICTU de startdatum langer dan 40 werkdagen uit wil stellen kan dat alleen met wederzijdse goedkeuring.	1	2	3
5.	Opdrachtnemer wijkt niet van de in de definitieve nadere offerte vastgelegde einddatum af (behoudens een eventuele wijziging van de startdatum) tenzij ICTU hier schriftelijk toestemming voor geeft.	1	2	3

Eisen aan de toetsingskaders

	Eis	Perceel		
6.	De beveiligingsopdrachten dienen, tenzij anders aangegeven in de nadere offerteaanvraag, te toetsen: 1. dat het IT-systeem voldoet aan de Wet Computercriminaliteit en de Algemene Verordening Gegevensbescherming (AVG), 2. dat het IT-systeem voldoet aan de meest recente OWASP Top 10[1], de meest recente CWE/SANS TOP 25 Most Dangerous Software Errors[2], de meest recente NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties 2015[3], de meest recente Baseline Informatiebeveiliging Overheid[4], de meest recente NEN-EN-ISO/IEC 27001[5] en NEN-EN-ISO/IEC 27002[6] (allen voor zover van toepassing op het te onderzoeken IT-systeem), 3. dat het IT-systeem niet onbeschikbaar gemaakt kan worden met of zonder autorisatie (beschikbaarheid), 4. dat informatie niet kan worden ontsloten zonder autorisatie (vertrouwelijkheid), 5. dat informatie niet kan worden veranderd of vernietigd zonder autorisatie (integriteit), 6. dat geen informatie die een persoon of bedrijf identificeert kan worden achterhaald zonder autorisatie (privacy), 7. dat in voorgaande beveiligingsopdrachten geconstateerde bevindingen waarvan ICTU heeft aangegeven dat ze zijn verholpen, en die niet eerder zijn hertest, inderdaad zijn verholpen, 8. op bekende exploits (met een CVE ID), 9. op configuratiefouten in gebruikte standaardsoftware en op fouten in configuratiebestanden, 10. op het gebruik van beveiligingskaders en -plannen zoals binnen het project opgesteld, 11. op het correct gebruik van privileges voor het IT-systeem, conform de autorisatiematrix, 12. op het correct gebruik van logging door het IT-systeem, 13. steekproefsgewijs op beveiligingsaspecten zoals HTTP headers, special encodings, implicit variables, mixing languages, information leakage en input validation problems zoals client-side input validation, hidden form fields, command injection (e.g. SQL), cross-site scripting, cross-site request forgery, cross-origin resource sharing en cross-site tracing, 14. project-specifieke eisen toegevoegd in de offerteaanvraag.	1	2	

[1] https://owasp.org/Top10/
[2] https://www.sans.org/top25-software-errors
[3] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
[4] https://bio-overheid.nl
[5] https://www.nen.nl/nen-en-iso-iec-27001-2023-nl-314206
[6] https://www.nen.nl/nen-en-iso-iec-27002-2022-nl-304509

	Eis	Perceel		
7.	De onderhoudbaarheidsopdrachten dienen, tenzij anders aangegeven in de nadere offerteaanvraag: 1. te toetsen dat de software voldoet aan de meest recente SIG/TÜViT Evaluation Criteria Trusted Product Maintainability[7], de IFSQ standaarden (level 1 en 2)[8] en NEN-ISO/IEC/IEEE 42010[9], 2. te toetsen dat in voorgaande onderhoudbaarheids-opdrachten geconstateerde bevindingen waarvan ICTU heeft aangegeven dat ze zijn verholpen, en die niet eerder zijn getoetst, inderdaad zijn verholpen, 3. de broncode steekproefsgewijs te onderzoeken op onderhoudbaarheidsaspecten die niet (geheel) geautomatiseerd kunnen worden bepaald, zoals naamgeving, leesbaarheid, inline documentatie, gebruik van design patterns en testbaarheid, 4. project-specifieke eisen toegevoegd in de offerteaanvraag te toetsen.			3

Eisen aan de uitvoering van de opdrachten

	Eis	Perceel		
8.	Opdrachtnemer meldt bevindingen met een CVS-score[10] van 7 ("high") of hoger direct na constatering mondeling en elektronisch aan de contactpersonen van ICTU die in de offerteaanvraag zijn genoemd.	1	2	
9.	Bij penetratietesten en vulnerabilityscans informeert opdrachtnemer de contactpersonen van ICTU die in de offerteaanvraag zijn genoemd dagelijks over start en einde van de werkzaamheden en de betrokken IP-adressen.		2	
10.	Opdrachtnemer spreekt de bevindingen door met ICTU tijdens een validatiesessie waarin opdrachtnemer de geconstateerde bevindingen, inclusief per bevinding een initiële beoordeling van de ernst, toelicht. ICTU geeft vervolgens feedback op de geconstateerde bevindingen en de beoordeling van de ernst. Opdrachtnemer stelt na deze feedback gehoord te hebben de bevindingen en de ernst van de bevindingen vast en neemt dit op in de rapportage.	1	2	3
11.	Elektronische vergaderingen met ICTU vinden altijd plaats met behulp van Microsoft Teams.	1	2	3
12.	Opdrachtnemer biedt een beveiligde omgeving aan voor ontvangst van documenten en informatie. Binnen deze omgeving hebben alleen degenen die direct bij de uitvoering van de opdracht betrokken zijn toegang tot de ingediende stukken.	1	2	3

[7] https://www.softwareimprovementgroup.com/wp-content/uploads/SIG-TUViT-Evaluation-Criteria-Trusted-Product-Maintainability-Guidance-for-producers.pdf
[8] http://www.ifsq.org/standards.html
[9] https://www.nen.nl/NEN-Shop/Norm/NENISOIECIEEE-420102011-en.htm
[10] https://nvd.nist.gov/vuln-metrics/cvss

	Eis	Perceel		
13.	Opdrachtnemer verwijdert aantoonbaar binnen 3 maanden na oplevering van de definitieve rapportage alle door ICTU aangeleverde informatie, te weten broncode en softwaredocumentatie, van haar systemen.	1	2	3

Eisen aan de rapportages

	Eis	Perceel		
14.	Een rapportage in de Nederlandse (of indien met ICTU zo afgestemd, in de Engelse) taal bevat minimaal de volgende meta-informatie: managementsamenvatting, versienummer, status, datum, inhoudsopgave, verklarende woordenlijst, wijzigingsgeschiedenis, namen van alle betrokkenen.	1	2	3
15.	De managementsamenvatting bevat minimaal de beoordeling van de beveiligbaarheid (perceel 1 en 2) of onderhoudbaarheid (perceel 3), de belangrijkste bevindingen en de belangrijkste aanbevelingen.	1	2	3
16.	Een rapportage bevat minimaal de volgende inhoudelijke informatie: de beoordeelde eisen, richtlijnen en standaarden (inclusief versienummer), een lijst van bevindingen met unieke identificatie en een lijst met aanbevelingen met unieke identificatie.	1	2	3
17.	De bevindingen zijn naar CVS-score[10] geclassificeerd. Per bevinding zijn alle locaties aangegeven waar de bevinding is geconstateerd, bijvoorbeeld de bronbestanden of de URLs.	1	2	
18.	De bevindingen zijn naar ernst geclassificeerd (bijvoorbeeld: hoog risico/medium risico/laag risico). Per bevinding zijn alle locaties aangegeven waar de bevinding is geconstateerd, bijvoorbeeld de bronbestanden, klassenamen, methodenamen en/of regelnummers.			3
19.	In de rapportage worden de bevindingen met een CVS-score[10] van 7 (“high”) of hoger geanalyseerd, waarbij aangegeven wordt welke (rest)bedreigingen aanwezig zijn, hoe groot de kans is dat dit optreedt en welke gevolgschade gelopen zou kunnen worden.	1	2	
20.	In de rapportage worden de belangrijkste bevindingen (bijvoorbeeld hoog risico) geanalyseerd, waarbij aangegeven wordt hoe groot de kans is dat deze nadelig zijn voor het onderhoud van de software en welke gevolgen het niet verhelpen zou kunnen hebben.			3
21.	Voor iedere aangetroffen bevinding dient de rapportage een aanbeveling te bevatten hoe de bevinding te verhelpen, dan wel de invloed te beperken. Tenzij anders overeengekomen met ICTU geldt dat voor bevindingen met een laag risic CVS-score lager dan 4.0 geen aanbevelingen hoeven worden aangedragen.	1	2	3
22.	Bevindingen en aanbevelingen zijn in de rapportage wederzijds traceerbaar. Dat wil zeggen dat voor elke aanbeveling duidelijk is welke bevindingen de aanbeveling zal oplossen of verbeteren en dat voor elke bevinding duidelijk is welke aanbevelingen de bevinding zal oplossen of verbeteren.	1	2	3

	Eis	Perceel		
23.	Opdrachtgever levert de rapportage digitaal aan in PDF. Daarnaast levert de opdrachtnemer de bevindingen in CSV-formaat. De CSV bevat per bevinding minimaal de beschrijving van de bevinding, de unieke identificatie van de bevinding, de ernst, de eventuele andere classificaties, de locaties waar de bevinding is geconstateerd, bijvoorbeeld de bronbestanden inclusief pad en regelnummer(s) of de URLs inclusief parameters.	1	2	3
24.	De concept-rapportage is in minimaal 95% van de gevallen gereed binnen vijf werkdagen na de validatiesessie. De opdrachtnemer verwerkt het reviewcommentaar van ICTU op het concept binnen vijf werkdagen tot een definitieve rapportage.	1	2	3
25.	ICTU behoudt zich het recht voor om zelfstandig te bepalen wie de rapportages mag inzien.	1	2	3

Eisen aan de tarieven en facturatie

	Eis	Perceel		
26.	Opdrachtnemer stuurt binnen één maand na versturen van de definitieve rapportage van een opdracht de factuur voor de uitgevoerde werkzaamheden zoals overeengekomen in de Nader Overeenkomst. Indien de factuur meer- of minderwerk bevat dient de goedkeuring daarvan door ICTU als bijlage bij de factuur meegezonden te worden.	1	2	3

Eisen aan contractmanagement

	Eis	Perceel		
27.	Minimaal één keer per jaar vindt er tussen de contracteigenaar van ICTU en opdrachtnemer een strategisch overleg plaats. Hierin komen tenminste aan de orde: evaluaties van de werkwijze en resultaten van de uitgevoerde opdrachten, relevante ontwikkelingen binnen beide partijen, nakomen van (proces)afspraken en verbeteracties door partijen en verwachtingen over opdrachten voor de komende periode.	1	2	3
28.	Minimaal één keer per kwartaal vindt tactisch overleg tussen de contractmanager van ICTU en opdrachtnemer plaats. Hierin komen tenminste aan orde: kwaliteit van de dienstverlening, klanttevredenheid over recente opdrachten, verbeteracties n.a.v. recente opdrachten en voortgang van eventueel eerder afgesproken verbeteracties.	1	2	3
29.	Opdrachtnemer vraagt na elke opdracht de klanttevredenheid over de uitgevoerde opdracht uit bij de contactpersonen van ICTU die in de offerteaanvraag zijn genoemd.	1	2	3