Bijlage 5 - Programma van Eisen

Nr.	Betreft	Algemene eisen
1.	Inschrijver heeft een geldige ISO9001, ISO27001 en ISAE3402 certificering en voert haar dienstverlening uit conform deze kwaliteitsnormen. Certificeringen worden jaarlijks extern geaudit.	
2.	Inschrijver is verplicht zich bij de uitvoering van haar werkzaamheden te houden aan geldende wet- en regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG).	
3.	Inschrijver gaat ermee akkoord dat een Verwerkersovereenkomst onderdeel is van de Overeenkomst, zie bijlage 9.	
4.	Inschrijver gaat ermee akkoord dat Nuffic - voordat de applicatie in gebruik wordt genomen - een standaard BIO-implementatie uitvoert. Hieronder vallen de volgende stappen: ▪ Een gap-analyse met als uitgangspunt beveiligingsniveau BBN2; ▪ Een risicoanalyse om mogelijke maatregelen te bepalen waardoor een acceptabel restrisico wordt bereikt.	

Nr.	Betreft	Eisen aan de dienstverlening
5.	De communicatie van de dienstverlening gedurende de looptijd van het contract is in het Nederlands.	
6.	Er is een helpdesk beschikbaar voor het melden van incidenten en bugs in de software.	
7.	De helpdesk is minimaal beschikbaar tussen 09:00 – 17:00 uur (Nederlandse kantooruren).	
8.	Inschrijver dient tijdens de contractperiode één (1) vast contactpersoon en één (1) vervangend contactpersoon op te geven met wie Nuffic tijdens kantooruren contact kan opnemen.	
9.	Periodiek (tenminste 1 keer per jaar) worden evaluatiemomenten over de geleverde dienstverlening ingepland.	
10.	Inschrijver gaat ermee akkoord dat na ingangsdatum van de Overeenkomst i.s.m. Nuffic een Service Level Agreement (SLA) worden uitgewerkt, waarbij de uitwerking van wens K 3 (Programma van Wensen) het uitgangspunt is. Onderdeel van de SLA is het gezamenlijk vaststellen van KPI's waar de dienstverlening op gemonitord zal worden. Nadat de KPI's zijn vastgesteld, zullen deze vanaf dat moment worden gemeten en besproken tijdens de evaluatiemomenten. De definitieve SLA is onderdeel van de Overeenkomst.	

Nr.	Betreft	Eisen aan performance en beschikbaarheid
11.	De wachttijd voor eindgebruikers bij schermwisselingen is aantoonbaar < 2 seconde per uitgevoerde beeldschermtransactie, bij concurrent gebruik van 20 gebruikers of minder. Dit bij voldoende bandbreedte en netwerkcapaciteit aan de gebruikerskant (buiten de invloedssfeer van Inschrijver).	

12.	De responsetijd voor online functionaliteit / transacties tijdens kantooruren ligt voor minimaal 95% aantoonbaar op <1 sec. Dit bij voldoende bandbreedte en netwerkcapaciteit aan de gebruikerskant (buiten de invloedssfeer van Inschrijver).
13.	Voor veelgebruikte reguliere rapportages en opvragingen wordt een goede responsetijd gevraagd van < 5 sec in aantoonbaar minimaal 95% van de gevallen. Dit bij voldoende bandbreedte en netwerkcapaciteit aan de gebruikerskant (buiten de invloedssfeer van Inschrijver).
14.	De applicatie is tijdens kantooruren en in piekperiode van 07:00 uur - 23:00 uur beschikbaar met een service level van minimaal 99,5%.

Nr.	Betreft	Functionele eisen FASE 1
15.	De applicatie is een standaard oplossing. Middels alleen configuratie wordt aan de gestelde eisen voldaan.	
16.	De dienst wordt als een SaaS oplossing aangeboden.	
17.	De voertaal in de (menu's van de) applicatie is Engels.	
18.	Begrotingen kunnen eenvoudig via een interface naar Unit4 ERP worden overgezet. Inschrijver is verantwoordelijk voor het realiseren van deze interface en neemt de kosten hiervoor op in het prijsinvulformulier.	
19.	Personeelsgegevens uit YouForce kunnen eenvoudig in de begrotingsapplicatie worden ingelezen.	
20.	Toegang tot gegevens kan per (groep) gebruikers worden geconfigureerd. Beperken van toegang tot de volgende gegevens moet mogelijk zijn: ▪ read-only of ook muteerrechten ▪ toegang tot een selectie van (deel)projecten ▪ toegang tot de medewerkers of functies van een team ▪ toegang tot begrotingsversies (read-only of ook muteerrechten)	
21.	Ingevoerde mutaties worden gelogd (audit trail). Gelogd wordt minimaal: wie heeft wat wanneer gewijzigd. Deze logging kan worden gebruikt voor een verschillenanalyse tussen twee begrotingsversies.	
22.	Er kunnen meerdere begrotingsversies worden gemaakt. Gebruikers kunnen eenvoudig schakelen tussen begrotingsversies.	
23.	Er kan zowel op projecten als deelprojecten worden begroot (Nuffic hanteert de termen Project en Workorder).	
24.	De formatiebegroting kan per medewerker en per functie worden ingevoerd.	
25.	De applicatie beschikt over functionaliteit om per combinatie Grootboekrekening/Project meerdere regels te registeren. Bijvoorbeeld de post licentiekosten van een Project kan worden geregistreerd middels meerdere regels (licentiekosten applicatie A, licentiekosten applicatie B, etc.) op dezelfde combinatie van Grootboekrekening/Project. Deze functionaliteit wordt gebruikt bij de invoer van materiele lasten en baten.	
26.	De applicatie beschikt over functionaliteit voor automatische berekening van uurtarieven per medewerker en per functie op basis van (ingelezen) personeelgegevens en andere data (bijvoorbeeld CAO). De gegenereerde tarieven kunnen handmatig per medewerker of functie worden overschreven.	

27.	De applicatie beschikt over functionaliteit om overhead volledig automatisch toe te rekenen o.b.v. totale kosten overhead in relatie tot verhoudingsgewijze directe loonkosten per project.
26.	De applicatie beschikt over functionaliteit om o.b.v. eigenschappen van een project een automatische batenberekening uit te voeren (bijvoorbeeld resultaatneutraal begroten: kosten + baten = 0).
27.	De applicatie beschikt over functionaliteit om controles op invoer en totalen uit te voeren: 1 op 1 relatie tussen omvang arbeidsovereenkomst en begrote uren op individueel werknemersniveau. (waarschuwing bij overschrijding).
28.	De applicatie beschikt over functionaliteit om controles op invoer en totalen uit te voeren: Een controle op de volledige doorbelasting van de overhead.
29.	De applicatie beschikt over functionaliteit om controles op invoer en totalen uit te voeren: Een controle op de toerekening van de generieke OCW-subsidie.
30.	De applicatie ondersteunt de eindgebruiker bij de invoer van budgetten door een gebruikersvriendelijke user interface en functionaliteit (zie paragraaf 1.2.3. van het Beschrijvend document voor de definitie van gebruiksvriendelijkheid).
31.	Er kan eenvoudig een (selectie van) projecten, medewerkers etc. worden gemaakt in invoerschermen en rapportages.
32.	De invoer of wijziging van een budget wordt direct doorgevoerd in schermen en rapportages. Doel is om snel en eenvoudig inzicht te verkrijgen in het effect van een invoer/wijziging van gegevens op de begroting van een team/project.
33.	De applicatie beschikt over Drill down functionaliteit in schermen en/of rapporten om van een bepaald aggregatieniveau in te zoomen naar onderliggende projecten/kostensoorten.
34.	De applicatie beschikt over eenduidige rapportages: Rapportages vanuit verschillende invalshoeken sluiten op elkaar aan.
35.	Rapportages kunnen naar Excel worden geëxporteerd.
36.	De applicatie beschikt over een rapport om per (groep van) project(en) te rapporteren over data van het begrotingsjaar T, begrotingsjaar T minus 1 en realisatie van jaar T minus 2.
37.	De applicatie beschikt over een detailrapportage per project met onderscheid tussen personele lasten (per medewerker/functie), materiele lasten, overhead en baten.
38.	De applicatie beschikt over een Exploitatie-/Managementrapportage: Een rapportage per Afdeling/Team met per project het totaal van personele lasten, materiele lasten, overhead en specificatie van baten.
39.	De applicatie beschikt over een rapportage per grootboekrekening (begrotingsjaar T vs jaar T minus 1) waarbij de grootboekrekeningen zijn gegroepeerd conform de indeling van de Verlies en Winstrekening.
40.	De applicatie beschikt over een rapportage (begrotingsjaar T) per grootboekrekening waarbij de grootboekrekeningen zijn gegroepeerd conform de indeling van de Verlies en Winstrekening inclusief (sub)totalen per afdeling.
41.	De applicatie beschikt over een rapportage met een verschillenanalyse tussen twee begrotingsversies.

Nr.	Betreft	Functionele eisen FASE 2
42.	Realisatiedata (actuals en openstaande Purchase Orders) uit Unit4 ERP kunnen eenvoudig via een interface in de applicatie worden ingelezen. Inschrijver is verantwoordelijk voor het realiseren van deze interface en neemt de kosten hiervoor op in het prijsinvulformulier.	
43.	Er kan zowel een jaarbegroting als een meerjarenbegroting worden ingevoerd.	
44.	De applicatie beschikt over forecasting functionaliteit om op basis van begrotingsdata en actuele realisatiedata een eindejaarsverwachting te maken.	
45.	De applicatie beschikt over functionaliteit om what-if-scenario's door te rekenen (bijvoorbeeld effect van generieke (loon)wikkeling).	
46.	De applicatie beschikt over een rolling forecast rapportage van begrotings- én realisatiedata van (begrotings)jaar T en T minus 1.	
47.	De applicatie beschikt over een rapportage waarin het resultaat van een what-if scenario naast de begrotings- en realisatiedata wordt gepresenteerd.	

Nr.	Betreft	Eisen aan privacy
48.	Inschrijver garandeert dat zij de vertrouwelijkheid van Nuffic data beschermt.	
49.	De informatie van Nuffic moet conform de Privacy wetgeving worden opgeslagen en behandeld.	
50.	Gegevens in rust of in bewerking (incl. backups) blijven binnen EU grenzen	
51.	Persoonsgegevens worden verwijderd op verzoek van de betreffende persoon. Dit gebeurt onmiddellijk en uiterlijk binnen een maand.	
52.	Inschrijver verwijdert op verzoek van Nuffic data van Nuffic op veilige wijze in geval van opzegging van het product, na de verplichte bewaarperiode en geeft een verklaring af dat de gegevens zijn vernietigd.	
53.	Voordat apparatuur en media worden afgevoerd dienen de opgeslagen gegevens te worden verwijderd op niet meer te recoveren wijze.	

Nr.	Betreft	Technische eisen en eisen aan informatiebeveiliging
54.	Middels het indienen van een Inschrijving conformeert Inschrijver zich aan het informatiebeveiligingsbeleid zoals bijgevoegd in Bijlage 14.	
55.	De omgeving van Nuffic is afgeschermd op het netwerk van andere klanten.	
56.	Gegevens mogen niet voor andere doeleinden gebruikt worden zonder toestemming van Nuffic.	
57.	Inschrijver faciliteert op verzoek van Nuffic data overdracht in een open standaard vorm bij beëindiging van activiteiten voor Nuffic.	
58.	Toegangsautorisatie tot de applicatie verloopt via Azure AD. Inschrijver is verantwoordelijk voor het realiseren van de koppeling met de Azure-omgeving van Nuffic en neemt de kosten hiervoor op in het prijsinvulformulier. Er mogen geen gegevens worden opgeslagen uit Azure AD.	
59.	Inschrijver zal vooraf informatie verstrekken als er risico's zijn die de dienstverlening beïnvloeden.	
60.	Inschrijver informeert Nuffic tijdig over onderhoud en storingen. Onderhoud wordt ingepland zodat de overlast voor Nuffic wordt geminimaliseerd.	
61.	Bij storingen of verminderde beschikbaarheid van een dienst rapporteert schriftelijk over de reden en maatregelen.	

62.	De autorisatie van gebruikers binnen de applicatie vindt plaats op basis van een door Nuffic opgestelde autorisatiematrix.
63.	Inschrijver past functiescheiding toe in systemen van Nuffic en voorkomt conflicterende rollen.
64.	Inschrijver stelt op verzoek toegangsrechten van haar personeel en operator logs gerelateerd aan Nuffic omgevingen beschikbaar. In productie omgevingen heeft Inschrijver alleen de noodzakelijke toegangsrechten voor het beheer.
65.	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek. Met systeemhulpmiddelen wordt bedoeld: hulpmiddelen die de continuïteit en het onderhouden van het systeem bevorderen, zoals applicaties en tools die helpen bij zaken als, Identificatie, authenticatie, autorisatie, tools die helpen bij logging en monitoring etc.
66.	Een logregel bevat minimaal: a. de gebeurtenis; b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c. het gebruikte apparaat; d. het resultaat van de handeling; e. een datum en tijdstip van de gebeurtenis.
67.	De beschikbaarheid van de loginformatie wordt gewaarborgd voor de periode van maximaal één (1) jaar.
68.	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
69.	In het back-up beleid staan minimaal de volgende eisen: a. Dataverlies bedraagt maximaal 28 uur. b. Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.
70.	Security incidenten en inbreuken op de privacy worden zo spoedig mogelijk en tenminste op de dag van ontdekking aan de Security Manager van Nuffic gemeld en aan uw contactpersoon bij Nuffic gemeld. Op verzoek van Nuffic worden relevante logs beschikbaar gesteld. In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. Nuffic wordt geïnformeerd over welke maatregelen Inschrijver treft en nog gaat treffen.
71.	Publiekelijk beschikbare web applicaties en API's gerelateerd aan de dienst zijn beveiligd. Verbindingen worden gemaakt op basis van sterke wachtwoorden (zie hiervoor) en versleutelde verbindingen.
72.	Nuffic is eigenaar van data. Inschrijver zal het intellectueel eigendom van Nuffic respecteren.
73.	Inschrijver informeert Nuffic over belangrijke versie upgrades. Inschrijver houdt bestaande technologieën die Nuffic gebruikt beschikbaar. Wanneer zulke technologie wordt uitgefaseerd, zal dit met een overgangsperiode gebeuren.

74.	Inschrijver informeert Nuffic over veranderingen in beveiligingsprocedures, substantiële wijzigingen in het beveiligingsbeleid, beveiligingsstatus en beveiligingsvereisten.
75.	Informatie over technische kwetsbaarheden van applicatie behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
76.	De applicatie wordt jaarlijks door Inschrijver gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.
77.	Het verzenden van mail voor alle domeinen dient altijd via Office 365 te gebeuren.
78.	Gevoelige data wordt versleuteld opgeslagen. Ongeautoriseerde toegang en opslag van onversleutelde gevoelige informatie is niet mogelijk.
79.	Er wordt standaard via ssllabs.com een controle gedaan op de configuratie van de webserver. Er dient tenminste een A beoordeling te worden gehaald.
80.	Webapplicaties dienen te voldoen aan de laatste OWASP. Specifiek voor webapplicaties gelden een aantal beveiligingsricio's. Voordat de webapplicatie in gebruik wordt genomen dient de externe softwaredienstverlener aan te tonen welke maatregelen zijn genomen om de OWASP Top 10 te beheersen: Deze maatregelen dienen per OWASP Top tien punt aangegeven en toegelicht te worden, en gebaseerd te zijn op "how do I prevent ….." van het document "OWASP Top 10: the Ten Most Critical Web Applications Security Risks" / The OWASP Foundation.
81.	Vertrouwelijke gegevens mogen enkel verzonden worden door ze tijdens de gehele transportketen over het internet te beveiligen met een actueel versleutelingalgoritme. Voor webverkeer is dit HTTPS (certificaat, TLS, minimale CSR sleutellengte van 2048 bits). Verzenden van vertrouwelijke gegevens via e-mail is niet toegestaan.
82.	Vertrouwelijke en persoonsgegevens mogen slechts binnen een beschermde database worden opgeslagen, verwerkt en beheerd en niet daarbuiten.
83.	Indien programmatuur, hardware, wordt ontwikkeld of getest dient dit te gebeuren op een van de productieomgeving gescheiden (acceptatie)test- en ontwikkelomgeving (OTAP). De ontwikkel- en testomgeving zijn bij Inschrijver.
84.	Testgegevens moeten worden beveiligd en beheerd. Het gebruik van een identieke kopie van productie databases met gevoelige gegevens (waaronder persoonsgegevens) moet worden vermeden.
~~85.~~	~~Van een extern opgeslagen database dienen de actuele keys en andere ontsleutelingsinformatie beschikbaar te worden gesteld aan de Security manager.~~
86.	Inschrijver zal vooraf informatie verstrekken over het risico op inbeslagname, terminatie van de provider, lock-in risico en verandering in eigendom Inschrijver.

Nr.	Betreft	Eisen aan de tarieven en facturatie
85.	Voor de realisatie van fase 1 en 2 + de licentiekosten voor één (1) jaar hanteert Nuffic een maximum budget van € 125.000 (exclusief BTW). Hierbij is het uitgangspunt voor het aantal gebruikers als volgt: ▪ Budgethouders: 35 ▪ Controllers: 5 ▪ Functioneel beheerders: 2	
86.	Facturatie vindt plaats onder vermelding van het inkooporder nummer.	
87.	Inschrijver verstuurt één factuur per inkooporder.	
88.	Facturen worden digitaal, in PDF formaat verstuurd aan facturen@nuffic.nl	