

3.1 Software as a service & Architectuur

- 3.1 De gevraagde functionaliteit voor de financiële administratie en inkoop wordt geleverd in de vorm van een SAAS-oplossing, dus als een dienst waarbij zowel het runnen (operations) als het doorontwikkelen (development) door de leverancier wordt uitgevoerd. Het technisch beheer ligt volledig bij de leverancier. Er is geen sprake van klantspecifiek maatwerk.
- 3.2 Aangeboden applicaties/oplossingen zijn volledig web gebaseerd en daarmee onafhankelijk van het apparaat, besturingssysteem en locatie.
 - maken primair gebruik van standaard internetprotocollen (http en https) en poorten (80 en 443)
 - maken geen gebruik van (browser) plugins of add-ons
 - werken tenminste met de volgende browsers (laatste en één na laatste versie):
 - Chrome
 - Firefox
 - Internet Explorer (versie 10 en 11)
 - Edge
 - Safari (op mac OS/OSX en iOS)
- 3.3 De leverancier biedt aanbestedende dienst een gescheiden test- en productieomgeving aan. De testomgeving is bedoeld om aanbestedende dienst in de gelegenheid te stellen functionaliteit en integratieaspecten met andere applicaties te kunnen testen voorafgaand aan het in productie gaan van een nieuwe release. De data op deze testomgeving kan op aanvraag verversen en geleegd worden. Ook wordt verzocht om een tijdelijke trainingsomgeving voor de opleiding van beheerders en gebruikers voorafgaand aan de 'go live'.
- 3.4 Leverancier stelt een realtime leesreplica van de productiedatabase beschikbaar aan aanbestedende dienst op een locatie en databaseplatform naar keuze van leverancier. Koppeling zal via een databaselink gaan van een gangbare standaard, gebruik makend van een beveiligde verbinding. De primaire doelstelling van deze database is de beschikbaarheid van data voor rapportagedoeleinden. Om die reden levert leverancier ook de documentatie van het datamodel, zodat de data adequaat ontsloten kan worden.
- 3.5 Er is Single Sign On mogelijk voor gebruikers op basis van ADFS (Active Directory Federation Services) of Surfconext. Hierbij heeft realisatie via Surfconext de voorkeur. Two factor authentication wordt ondersteund.
- 3.6 Het datacentrum waar de SaaS oplossing wordt gehost bevindt zich in de Europese Unie.
- 3.7 Inschrijver moet beschikken over een systeem dat dataveiligheid aantoonbaar waarborgt, hetgeen kan worden aangetoond door een 27001 certificaat of een isae3402 verklaring.

3.2 Integratie & koppelingen

- 3.10 Alle, in de aangeboden applicaties/oplossingen, opgeslagen data is beschikbaar via een gestandaardiseerd, actueel en (near) realtime koppelvlak (zowel push als pull) in de vorm van een API/Webservice op basis van de-facto standaarden zoals SOAP/XML of REST/JSON.
- 3.11 De aangeboden API's/Webservices zijn goed gedocumenteerd en voorzien van duidelijke (eenduidige) terugkoppeling. Alle documentatie hieromtrent is beschikbaar voor de Aanbestedende Dienst.
- 3.12 In de communicatie van een nieuwe release van de applicatie worden ook eventuele aanpassingen aan het datamodel en/of de koppelingen expliciet beschreven.
- 3.13 De applicatie biedt de mogelijkheid om middels csv- en/of Excel bestanden (gegevens) in te lezen en/of gegevens te exporteren.
- 3.14 Geautomatiseerde User Provisioning wordt ondersteund, dat wil zeggen: Gebruikers(accounts) kunnen, via een koppeling met het Identity Management systeem van Aanbestedende Dienst, geautomatiseerd aangemaakt, gemuteerd, geblokkeerd en verwijderd/gearchiveerd worden.
- 3.15 De financiële applicatie is in staat zowel journaalposten (ingeval facturen elders worden opgemaakt en verstuurd) als factuurregels te verwerken (ingeval de facturen opgemaakt en verstuurd moeten worden vanuit de financiële applicatie).
- 3.16 Historische integriteit: gegevens worden vastgehouden en niet weggegooid. Bij mutatie wordt het huidige database record bewaard (inactief) naast het gewijzigde record (actief).

3.3 Datamanagement & Security

- 3.19 De applicatie voldoet aan 'Juridische Normenkader Cloudservices Hoger Onderwijs' 2016.
- 3.20 De leverancier vrijwaart Aanbestedende dienst van virussen, malware, worms en andere softwarematige attacks.
- 3.21 Aangeboden applicaties/oplossingen zijn beschermd tegen tenminste de OWASP top 10 kwetsbaarheden.
- 3.22 De leverancier hanteert gangbare beveiligingsmiddelen, zoals beveiligde verbindingen en beveiliging op toegang tot database en toegang tot back-ups, om te voorkomen dat derden ongeoorloofd toegang krijgen tot gegevens van Aanbestedende dienst.
- 3.23 De leverancier stelt Aanbestedende dienst z.s.m. op de hoogte indien er een 'data breach' is opgetreden waar Aanbestedende dienst gegevens bij betrokken zijn geweest (zie relevante EU-wetgeving) of een ander security probleem dat mogelijk van invloed is op het Aanbestedende dienst. Leverancier geeft hierbij het actieplan aan.
- 3.24 De leverancier sluit na definitieve gunning een Escrow-overeenkomst af, waarin geregeld wordt dat applicatie en data ingeval van insolventie toegankelijk blijven.
- 3.25 Binnen de applicatie worden door middel van rollen privacygevoelige gegevens afgeschermd (wet op de privacy persoonsgegevens).
- 3.26 In geval van een calamiteit is het maximale dataverlies één (1) minuut.
- 3.27 Leverancier garandeert de integriteit van gegevens onder alle omstandigheden.
- 3.28 Leverancier garandeert de vertrouwelijkheid van gegevens onder alle omstandigheden.
- 3.29 Er is een back-up-, disaster- en recoveryprocedure aanwezig, gedocumenteerd, getest, en operationeel.
- 3.30 Historische integriteit: gegevens worden vastgehouden en niet weggegooid. Bij mutatie wordt het huidige database record bewaard (inactief) naast het gewijzigde record (actief).
- 3.31 Mutaties die een gebruiker in het systeem doet kunnen worden vastgelegd, waarbij wordt gedocumenteerd wie wanneer wat heeft gecreëerd/gewijzigd/verwijderd. Hiervoor is audittrail rapportage beschikbaar.

3.4 Performance

- 3.34 De responsetijd van de webpagina's en operationele rapporten mag niet meer dan één (1) seconde zijn tijdens normale productionele belasting. Hierbij mag worden aangenomen dat het client apparaat (pc/laptop) en netwerk geen beperkende factor zijn.
- 3.35 De leverancier sluit na definitieve gunning een Escrow-overeenkomst af, waarin geregeld wordt dat applicatie en data ingeval van insolventie toegankelijk blijven.
- 3.36 Er is een back-up-, disaster- en recoveryprocedure aanwezig, gedocumenteerd, getest, en operationeel.
- 3.37 Het genereren van rapporten mag geen nadelige impact hebben op de genoemde performance eisen.
- 3.38 Voor 80% van de rapporten geldt dat ze binnen één minuut gegenereerd zijn.

3.5 Beschikbaarheid

- 3.41 Aangeboden applicatie/oplossing en bijbehorende beheerprocedures zijn ontworpen uitgaande van een minimale gegarandeerde beschikbaarheid van 99,8%.

3.6 App

- 3.44 Indien een app wordt meegeleverd dan is deze tenminste beschikbaar voor:
 - iOS
 - Android