Bijlage 8 Non functionele eisen Source-to-Pay applicatie

Aanbestedende dienst	:	Gemeente Veenendaal
Kenmerk	:	23GV1001 TN428453
Datum	:	20 december 2023
Versie	:	Definitief

1.1 Algemeen

- De Oplossing wordt geleverd als Software as a Service (SaaS). Een SaaS-dienst is software die online beschikbaar gesteld wordt en technisch volledig onderhouden wordt door de Opdrachtnemer.
- De Oplossing wordt geleverd, gebruikt en onderhouden in de Nederlandse taal. (Gebruikers)documentatie wordt tevens in het Nederlands opgeleverd.
- Er wordt minimaal een acceptatie- n productieomgeving beschikbaar gesteld.
- De Oplossing voldoet aan vigerende wet- en regelgeving (onder andere Archiefwet, Algemene Verordening gegevensbescherming (AVG), BIO, Wet Modernisering Elektronisch Berichten Verkeer, tijdelijk besluit Digitale toegankelijkheid Overheid). En de leverancier zal ervoor zorgen dat de oplossing aan de relevante wetgeving blijft voldoen gedurende de looptijd van het contract.
- Op basis van het afgesloten contract garandeert de opdrachtnemer dat de oplossing, gedurende de contractperiode, doorontwikkeld zal worden zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief onderhoud, ook verstaan dat op de oplossing adaptief onderhoud wordt uitgevoerd om als opdrachtgever te blijven voldoen aan in de contractperiode geldende wet- en regelgeving en inspeelt op ontwikkelingen in de markt
- De oplossing heeft een heldere kostenstructuur, die beschreven is, zowel in de verschillende elementen als de wijze waarop de aantallen zijn gebaseerd (aantal inwoners, formatieplaatsen, users, devices, enzovoort).
- Leverancier van de applicatie en de hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van de applicatie en de gegevens vindt fysiek plaats in en in overeenstemming met de eisen van de Nederlandse wet- en regelgeving. Dit moet ook gelden voor de onderaannemer(s) en subverwerker(s) van de leverancier.
- De helpdesk van de Opdrachtnemer is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de Oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De Opdrachtgever bepaalt de initiële prioriteit van incidenten. Ten aanzien van de ondersteuning wil de Opdrachtgever de volgende prioriteitsbepaling en werkwijze hanteren. Hiermee gaat u akkoord.

Categorie	Omschrijving
1	De Oplossing is volledig niet bruikbaar (naar mening van de Opdrachtgever een Critical Problem).
2	De Oplossing is deels niet bruikbaar of deels niet bruikbaar voor meer dan 10% van de gebruikers (naar mening van de Opdrachtgever een Major Problem).
3	Kleine verstoringen (naar mening van de Opdrachtgever een Minor Problem)
4	Gebruikers/beheerdersvraag.

De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de Oplossing. De Opdrachtnemer maakt voor de Opdrachtgever inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.

Categorie	Reactietijd	Oplossing binnen
1	0-0.5 uur beantwoorden 24/7	Work-around binnen 4 uur Oplossing binnen 8 uur
2	1 uur (op werkdagen tussen 8.00 en 17.00 uur)	Work-around binnen 8 uur op werkdagen Oplossing binnen 48 uur op werkdagen
3	24 uur (op werkdagen tussen 8.00 en 17.00 uur)	Work-around binnen 2 werkdagen Oplossing in volgende reguliere versie

4	24 uur (op werkdagen tussen 8.00 en 17.00 uur)	Antwoord binnen 1 week

1.2 Toegang en beschikbaarheid

- De Oplossing dient benaderbaar te zijn via een “fully qualified domain name” van de opdrachtnemer.
- De Oplossing beschikt over een webbased userinterface die zonder beperking van functionaliteit, benaderbaar is, door de laatste twee versies van de meest gangbare en ondersteunde browsers (Microsoft Edge, Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX, etc.). Uitzondering hierop is een plug-in voor kantoorautomatisering.
- Op werkdagen van 07.00 - 20.00 uur wordt de beschikbaarheid van alle geëiste omgevingen van de Oplossing voor minimaal 99% per maand (exclusief gepland onderhoud) gegarandeerd, voor de overige uren van de werkweek en het weekend wordt dit voor minimaal 99,0% per maand (exclusief gepland onderhoud) gegarandeerd. Er wordt uitgegaan van een beschikbaarheid van de verbinding vanuit de Opdrachtgever van 100%.
- Voor de Oplossing wordt een acceptabele performance voor circa 50 concurrent gebruikers gegarandeerd. Dit houdt in dat de resultaten van tenminste de volgende handelingen in de Oplossing binnen 3 seconden worden weergegeven (uitgaande van een schone internetverbinding):
  1. Het starten van een nieuwe transactie.
  2. Het accepteren van een transactie.
  3. Het verwerken van een transacte.
- De Opdrachtnemer garandeert adequate backup- en restorevoorzieningen van de Oplossing waarbij in geval van een gebeurtenis buiten de invloedsfeer van de Opdrachtnemer (bijvoorbeeld een ramp of incident) de afgesproken dienstverlening binnen 16 uur kan worden gecontinueerd in 85% van de gevallen en waarbij het verlies van gegevens maximaal 1 werkdag kan bedragen. Back-ups dienen minimaal 3 en maximaal 12 maanden bewaard te worden. Opdrachtnemer doet tenminste 2 restore testen per jaar en rapporteert dit aan de gemeente.
- De opdrachtnemer draagt aan het einde van de looptijd van het contract alle data (inclusief meta-data, geclassificeerd (Beschikbaarheid, Integriteit en Vertrouwelijkheid)) uit de oplossing in een origineel en duurzaam bestandsformaat, welke te importeren is binnen de nieuwe applicatie, kosteloos, over aan de aanbestedende dienst. Na bevestiging van overdracht wordt alle data van de systemen van de opdrachtnemer vernietigd. De opdrachtnemer levert een verklaring van vernietiging.
- De SaaS-oplossing moet beschikken over de mogelijkheid om een koppeling te maken voor het beschikbaar maken van de gegevens in de SaaS-oplossing ten behoeve van managementinformatie. Dit wordt ondersteund voor een ETL-proces, maar het biedt ook ondersteuning bijeen directe bevraging in het kader van managementinformatie (een Logisch Data Warehouse)
- De Opdrachtnemer levert 1 keer per kwartaal een rapportage aan met de resultaten m.b.t. de afgesproken KPI’s of geeft realtime inzicht.
- Escrow is vereist. De duurzaamheid van de Oplossing is gegarandeerd als de Oplossing niet langer ondersteund wordt door de Opdrachtnemer of de Opdrachtnemer niet langer in staat is om de Oplossing beschikbaar te stellen. Hierbij wordt de broncode en ook de werkende software (open source, escrow) beschikbaar gesteld of bestaat de mogelijkheid om het onderhoud en de ondersteuning voort te zetten bij een andere partij (exclusief de Opdrachtnemer en zuster-, dochter- en moedermaatschappijen).

1.3 Technologie en standaarden

- De oplossing heeft zich bewezen in de markt[1] en is gebaseerd op bewezen technologie.
- De oplossing voldoet aan de principes van de Gemma en de Common Ground of heeft dit op de planning staan om binnen 1 jaar te realiseren.
- Koppelingen op basis van rest API's en via een ESB of API Gateway (met uitzondering van key2financiën)
    - Minimaal voor operationele gegevens
    - Ook voor grotere dataleveringen voor bijvoorbeeld Management Informatie
- Binnen de Oplossing wordt de volgende standaard gehanteerd:
    - Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden. Voor het versturen en ontvangen van e-mails worden SPF, DKIM en DMARC toegepast. Voor het mailen vanuit de Oplossing wordt er gebruik gemaakt van STARTTLS 1.2, waarbij een DKIM-sleutel mogelijk is. Andere standaarden waar de oplossing aan moet voldoen met een 'secure connections', zijnde: DNSSEC, DANE en IPv4 en IPv6, HTTPS en HSTS verkeer. Hierop kan getoetst worden via www.internet.nl. Indien er gewerkt wordt met een certificaat of certificaten, dan worden alleen certificaten toegestaan van Trusted instanties.

1.3.1 De volgende standaarden zijn relevant:

Ades Baseline Profiles
De Advanced Electronic Signature (AdES) standaard voorziet in het digitaal tekenen van documenten met een geavanceerde of gekwalificeerde digitale handtekening.

Digikoppeling
Digikoppeling realiseert geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgende gegevensuitwisseling, op basis van vier koppelvlakstandaarden (DK ebMS standaard voor meldingen tussen informatiesystemen, DK WUS standaard voor de bevraging van informatiesystemen, DK GB standaard voor de uitwisseling van grote berichten, of REST API om gegevens veilig uit te wisselen volgens het REST principe).

Digitoegankelijk (EN 301 549 met WCAG 2.1)
Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor mensen met permanente, tijdelijke of situationele functiebeperkingen. Zo krijgt iedereen dezelfde toegang tot overheidsinformatie.
Let op: per 1 juli 2018 zijn overheidsorganisaties wettelijk verplicht om Digitoegankelijk (EN 301 549 en WCAG 2.1) te gebruiken voor de toegankelijkheid van websites en mobiele applicaties. Kijk voor meer informatie.

DNSSEC
DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.

HTTPS en HSTS
HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser).

[1] Onder bewezen in de markt verstaat de Gemeente Veenendaal dat de oplossing bij meerdere vergelijkbare organisaties naar tevredenheid in gebruik is en dat jaarlijkse nieuwe klanten gebruik gaan maken van de oplossing.

Let op: per 1 juli 2023 zijn overheidsorganisaties wettelijk verplicht om HTTPS en HSTS te gebruiken voor beveiligen van publiek toegankelijke websites en webapplicaties. Kijk voor meer informatie.

IPv6 en IPv4
IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren.

NL GOV Assurance profile for OAuth 2.0
NL GOV Assurance profile for OAuth 2.0 zorgt ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige plaatsvindt.

RPKI
Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routering negeren.

SAML
SAML standaardiseert federatieve (web)browser-gebaseerde single-sign-on (SSO). Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.

security.txt
security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.

TLS
TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

1.4 Archivering
Mits de oplossing is bedoeld voor archivering van documenten:

- De oplossing is geschikt voor de duurzaam toegankelijke opslag van documenten. Dat wil zeggen:
  - Er is toegangsautorisatie mogelijk op meerdere niveaus.
  - Het is mogelijk om met behulp van metadata de bewaartermijnen te hanteren.
  - Documenten zijn te delen met behulp van koppelingen, zonder te resulteren in kopietjes van het document.
  - Er is versiebeheer van documenten beschikbaar.
  - Het is mogelijk om met behulp van metadata classificaties mee te geven.
  - Het is mogelijk om op basis van de archiefwet vernietigingslijsten op te stellen.

1.5 Privacy en security

- **Code Hardening Vereisten:**
  a. **Input Validatie:** De SaaS-applicatie moet inputvalidatie implementeren op alle invoervelden om SQL-injecties, cross-site scripting (XSS) en andere invoergebaseerde aanvallen te voorkomen.
  b. **Buffer Overflow Bescherming:** De code moet bescherming tegen bufferoverloopaanvallen bevatten, zoals stack en heap overflows.

c. **Authenticatie en Autorisatie:** Sterke authenticatie- en autorisatiemechanismen moeten worden geïmplementeerd om ongeoorloofde toegang tot gegevens en functies te voorkomen.
d. **Beveiligde Communicatie:** Alle communicatie tussen de SaaS-applicatie en gebruikers moet versleuteld zijn via HTTPS.
e. **Beveiligde configuratie:** Gevoelige configuratiegegevens, zoals wachtwoorden en sleutels, moeten veilig worden opgeslagen en mogen niet hard-coded zijn.
f. **Patch Management:** Er moet een proces zijn voor het regelmatig bijwerken van de applicatie en alle afhankelijke bibliotheken om bekende beveiligingslekken te dichten.
Code Auditing Vereisten:
a. **Onafhankelijke Code Audit:** Een onafhankelijke derde partij moet periodieke beveiligingscode-audits uitvoeren om potentiële beveiligingsrisico's te identificeren en te rapporteren.
b. **Geautomatiseerde Scans:** Regelmatige geautomatiseerde scans met beveiligingshulpmiddelen moeten worden uitgevoerd om bekende kwetsbaarheden op te sporen.
c. **Compliance met Beveiligingsstandaarden:** De code moet worden beoordeeld en gevalideerd tegen relevante beveiligingsstandaarden. Hiervoor dient de meest relevante ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC gehanteerd te worden.
d. **Rapportage en Herstel:** De aanbieder moet gedetailleerde rapporten verstrekken met geïdentificeerde kwetsbaarheden en een plan voor herstel.
Documentatie en Transparantie:
a. De aanbieder moet volledige documentatie verstrekken van de code-audits en code hardeningmaatregelen.
b. De aanbieder moet transparantie bieden over hun beveiligingspraktijken, inclusief incidentresponsprocedures.
Bewustwording en Training:
a. Het personeel dat betrokken is bij het ontwikkelen en onderhouden van de SaaS-applicatie moet regelmatig worden getraind op het gebied van beveiligingsbewustzijn.
Toegang en Controle:
a. Beheer van toegangsrechten: Er moeten strikte beheersmaatregelen zijn voor toegangsrechten tot de code en gegevens van de applicatie.
b. Logging en Monitoring: Er moet een adequaat log- en monitoringsysteem zijn om verdachte activiteiten te detecteren.

- **Malware-detectievereisten:**
  Realtime Detectie:
  De SaaS-dienst moet beschikken over realtime malware-detectie die bestanden en netwerkverkeer bewaakt op verdachte activiteiten.
  Handtekeninggebaseerde Detectie:
  De malware-detectie moet gebruikmaken van handtekeninggebaseerde technieken om bekende malware te identificeren.
  Gedragsanalyse:
  De dienst moet gedragsanalyse gebruiken om ongebruikelijke activiteiten en verdacht gedrag van programma's te detecteren.
  Heuristische Analyse:
  De malware-detectie moet heuristische analyse uitvoeren om nieuwe, niet eerder bekende malware te identificeren.
  Automatische Updates:
  De malware-detectiecomponent moet regelmatig automatische updates ontvangen om de malware-handtekeningen en detectiemethoden up-to-date te houden.

Malware-verwijderingsvereisten:
Automatische Verwijdering:
De SaaS-dienst moet in staat zijn om gedetecteerde malware automatisch te verwijderen of in quarantaine te plaatsen.
Handmatige Verwijderingsmogelijkheid:
De dienst moet beheerders de mogelijkheid bieden om malware handmatig te verwijderen als dat nodig is.
Rapportage en Logging:
De applicatie moet gedetailleerde rapporten genereren over gedetecteerde malware, inclusief de acties die zijn ondernomen, en deze logs moeten beschikbaar zijn voor beheerders.
Herstelprocedures:
Er moeten duidelijke procedures worden vastgesteld voor het herstellen van gegevens en systemen die zijn getroffen door malware-infecties.
Systeemhersteloptie:
De SaaS-dienst moet de mogelijkheid bieden voor systeemherstel naar een schone staat in geval van ernstige malware-infecties.

Algemene Vereisten:
Regelmatige Beveiligingsupdates:
De aanbieder van de SaaS-applicatie moet regelmatig beveiligingsupdates en patches uitbrengen om bekende kwetsbaarheden te verhelpen.
Periodieke Audits:
Periodieke beveiligingsaudits moeten worden uitgevoerd om de effectiviteit van de malware-detectie en -verwijdering te beoordelen.
Naleving van Beveiligingsnormen:
Daar waar van toepassing is de geboden oplossing en werkt de achterliggende organisatie conform de vereisten van de meest actuele versie van de BIO (Baseline Informatieveiligheid Overheid).
Incidentresponsplan:
De aanbieder moet een gedetailleerd incidentresponsplan hebben en dit beschikbaar stellen aan de gemeente.

Naleving van Beveiligingsstandaarden:
Het organisatieonderdeel dient ISO 27001 gecertificeerd te zijn en met name dat deel van de organisatie dat zich bezig houdt met de ontwikkeling en beheer van de applicatie. Dit dient te blijken uit de VVT.

- De aanbieder werkt actief mee en verleent toegang tot die onderdelen waar auditinginformatie over gevraagd wordt, als de opdrachtgever een audit wil (laten) uitvoeren.
- De aanbieder beschermt de service en de gegevens tegen toegang door andere gebruikers op hetzelfde systeem.
- De Oplossing beschikt over een authenticatiemechanisme op basis van Azure Active Directory. Hierbij wordt gebruik gemaakt van beproefde standaarden voor federatie/Single Sign On, zoals authenticatie (MFA) via de Azure Active Directory, hebben gebruikers door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van de aangeboden Oplossing, uiteraard voor zover ze daartoe zijn geautoriseerd. Bij gebruik van de Oplossing dient gebruik gemaakt te worden van 2-factor authenticatie.
- De Oplossing beschikt over een niet-muteerbare audit-trail/logging waarbij automatisch ook records managementacties worden vastgelegd. Met daarin minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een gebruiker; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.

Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. In het geval van een, door de Opdrachtgever gedefinieerd, veiligheidsincident dient de logging omtrent dit incident minimaal drie jaar opvraagbaar te zijn.

- Er wordt bij de aanbesteding meegewerkt aan het opstellen van een DPIA en aan het opnieuw uitvoeren van de DPIA als de gegevens, die verwerkt worden, wijzigen. Een DPIA is nodig als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de gegevens verwerkt wordt. Dit wordt uitgevoerd in samenwerking van de Privacy Officer van de gemeente Veenendaal. Onacceptabele risico's dienen te worden opgelost.
- De aanbieder heeft een actueel Disaster Recovery plan en is bereid dit te overleggen als de opdrachtgever hierom vraagt.
- De integriteit van data blijft gewaarborgd door bedrijfskritische data van gemeente Veenendaal aantoonbaar te scheiden van andere klanten.