Programma van Eisen en Wensen

Datawarehouse en Dashboards

Regio West-Brabant - Mobiliteitscentrum

Inhoud

1. Eisen

Legenda

Eis.x	**Korte omschrijving eis (harde eis)**
Eventuele korte toelichting bij de eis.	
Wens.x	**Korte omschrijving wens (geen harde eis, heeft de voorkeur)**
Eventuele korte toelichting bij de wens.	

1.1 Algemene technische eisen

E.1	**Inrichting volledig binnen Azure tenant opdrachtgever**
De gevraagde inrichting (Azure landingzone, datawarehouse, en Power BI) wordt binnen de tenant van Opdrachtgever ingericht. Dit omvat zowel de programmatuur als de data. Leverancier draagt zorg voor het beheer van de Azure inrichting.	
E.2	**De aangeboden oplossing door Opdrachtnemer wordt geleverd als een Software as a Service (SaaS) omgeving ('de SaaS-applicatie'), een cloudoplossing waarbij technisch beheer door Leverancier uitgevoerd wordt.**
E.3	**Op basis van het afgesloten contract garandeert Leverancier dat de SaaS-applicatie gedurende de contractperiode zal worden doorontwikkeld.**
Hieronder wordt, naast correctief en preventief onderhoud, ook verstaan dat binnen de SaaS-applicatie innovatief onderhoud wordt uitgevoerd om te blijven voldoen aan geldende wet- en regelgeving. Zie artikel 8 e.v. van de GIBIT.	
E.4	**Opdrachtnemer waarborgt dat de aangeboden Oplossing niet meer dan één major versie achterloopt ('neerwaartsecompatibiliteit') op de open standaarden van het Forum Standaardisatie (www.forumstandaardisatie.nl). Aanpassingen in de hierboven genoemde standaarden worden binnen 6 maanden door de Opdrachtnemer verwerkt nadat de aanpassingen als nieuwe standaard zijn gepubliceerd op genoemd forum of Gemma online. Daarnaast wordt de oude versie van de standaard nog minimaal 12 maanden ondersteund.**
E.5	**Er wordt minimaal een test- en productieomgeving beschikbaar gesteld, beiden inclusief alle in dit Programma van Eisen en wensen geëiste en later toegevoegde koppelingen. De testomgeving geeft te allen tijde een representatie van de productieomgeving en dient continu beschikbaar te zijn (ook tijdens en na de implementatieperiode).**
E.6	**De test- en productieomgeving hebben gescheiden datasets.**
E.7	**De testomgeving bevat relevante data van Opdrachtgever.**
E.8	**De testomgeving werkt geïsoleerd en is niet gekoppeld aan de productieomgeving. Ook biedt deze omgeving de mogelijkheid om o.a. nieuwe updates te testen.**
E.9	**De SaaS-applicatie beschikt over een webbased userinterface (dus géén Citrix of gelijkwaardige omgeving) zonder beperking van functionaliteit. En werkt in de laatste versie –1 van de browsers Edge, Chrome. Er zijn ook geen verdere**

	instellingen of installaties (op het client device en/of in de webbrowser) benodigd, met uitzondering van client certificaten.
E.10	**De SaaS-applicatie moet in meerdere tabbladen binnen de webbrowser gelijktijdig te openen zijn.**
E.11	**De Oplossing dient benaderbaar te zijn via een "fully qualified domain name" via een beveiligde verbinding.**
E.12	**De gebruikersinterface van de SaaS-applicatie is volledig Nederlands- of Engelstalig.**
E.13	**De Leverancier zorgt voor beschikbaarheid en continuïteit van de SaaS oplossing.**
De beschikbaarheid is minimaal 99,5% op jaarbasis. De maximale toelaatbare uitvalsduur (Recovery Time Objective (RTO)) is 1 uur tijdens kantoortijden (8.00 tot 18.00 uur).	
W.1	**De Leverancier garandeert adequate back-up- en restorevoorzieningen van de data binnen de SaaS-applicatie waarbij, in het geval een restore van data nodig is, de afgesproken dienstverlening binnen 1 uur kan worden gecontinueerd. Er mag sprake zijn van maximaal dataverlies (Recovery Point Objective (RPO)) van een (1) uur.**

1.2 Functionele eisen

1.2.1 Azure data framework inrichting, implementatie, en beheer

E.14	**Azure Landingzone moet in tenant van Opdrachtgever gerealiseerd worden**
E.15	**Gebruikmaken van de standaard beschikbare componenten binnen Microsoft Azure**
Opdrachtgever wil alleen gebruikmaken van de standaard beschikbare toepassingen binnen Microsoft Azure wat betreft de inrichting.	
E.16	**Inzicht in pay-per-use kosten van de gebruikte componenten in de Azure omgeving**
Actueel inzicht in de variabele kosten voor de beheerders van Opdrachtgever. Leverancier geeft advies met betrekking tot de inrichting van het DWH, de modules, en bijbehorende kosten.	
W.2	**Devops wordt gebruikt voor zowel de ontwikkeling als implementatie.**
Ontwikkeling gebeurt op basis van code of maakt gebruikt van Fabric. De omgeving kan hiermee gemigreerd worden indien nodig.	

1.2.2 Datawarehouse inrichting, implementatie, en beheer

E.17	**Moet test- en productieomgeving bevatten**
Er moeten een test en productieomgeving gerealiseerd worden. Inclusief alle in dit Programma van Eisen en wensen geëiste en later toegevoegde koppelingen. De testomgeving geeft te allen tijde	

een representatie van de productieomgeving en dient continu beschikbaar te zijn (ook tijdens en na de implementatieperiode).	
E.18	**Connecties met verschillende type bronnen en het ontsluiten van data daaruit**
Geautomatiseerd ontsluiten van verschillende bronnen, zie bijlage. Het vormgeven van datamodellen hoort ook bij de opdracht.	
E.19	**Beschrijving per type connectie**
Opleveren van documentatie van hoe de verschillende type connecties technisch en functioneel werken nadat deze zijn opgeleverd.	
E.20	**Bewaren van historische data**
Opdrachtgever moet in kunnen stellen welke en hoe lang data bewaard worden, voor het kunnen signaleren van trends en het kunnen doen van prognoses.	
E.21	**Oplevering documentatie over de inrichting van ETL processen**
Leverancier documenteert informatie over de ontwikkelde ETL processen en draagt deze over wanneer Opdrachtgever dit vraagt.	
E.22	**Dagelijks inzicht in de laadprocessen en actieve signalering**
Inzicht in wat wel en niet goed is gegaan, inclusief actieve signalering bij waarschuwingen en fouten gedurende de laadprocessen	
E.23	**Het technisch beheer van het datawarehouse ligt bij leverancier.**
Tijdens de trainingsfase worden de medewerkers van Opdrachtgever opgeleid omwel zelfstandig te kunnen monitoren of en welke data overkomen vanuit de bronapplicaties. Het beheer ligt echter bij leverancier. Leverancier verleent op verzoek van Opdrachtgever ondersteuning bij vragen, incidenten (issues) en wijzigingsverzoeken tijdens de beheerfase.	

1.2.3 PowerBI inrichting, implementatie, en beheer

E.24	**Moet test- en productieomgeving bevatten**
Er moeten een test en productieomgeving gerealiseerd worden. De testomgeving geeft te allen tijde een representatie van de productieomgeving en dient continu beschikbaar te zijn (ook tijdens en na de implementatieperiode).	
E.25	**DWH is gekoppeld aan PowerBI**
Het DWH is aan PowerBI gekoppeld zodat alle data uit het DWH met PowerBI gebruikt kunnen worden.	
E.26	**Gebruik PowerBI is inzichtelijk**
Actueel en historisch inzicht in het gebruik van de PowerBI dashboards. Beheerder van Opdrachtgever moet zelf kunnen instellen wie dit gebruik kan inzien.	
E.27	**PowerBI inrichten zodat bepaalde dashboards ook met externen gedeeld kunnen worden.**
Het moet mogelijk zijn om delen van dashboards te delen met gemeenten en andere organisaties. Idealiter is het mogelijk alleen de data relevant voor de desbetreffende klant te delen in eenzelfde	

dashboard. Leverancier richt PowerBI zo in dat dit mogelijk is. Opdrachtgever bouwt samen met Odprachtnemer de dashboards en zorgt zelf voor de autorisaties.	
E.28	**Leverancier leidt Opdrachtgever op zodat Opdrachtgever PowerBI kan beheren**
Tijdens de trainingsfase worden de medewerkers van Opdrachtgever opgeleid om zelfstandig PowerBI te beheren. Leverancier verleent op verzoek van Opdrachtgever ondersteuning bij vragen, incidenten (issues) en wijzigingsverzoeken tijdens de beheerfase.	

1.3 Eisen informatiebeveiliging

E.29	**De opslag van data vindt plaats binnen de Europese Economische Ruimte (EER)**
E.30	**In de Overeenkomst zal worden beschreven op welke fysieke locaties de data van Opdrachtgever wordt/is ondergebracht. Zowel productie-omgeving als back-up.**
E.31	**Indien Leverancier gebruik maakt van meerdere sub-verwerkers, dient Leverancier deze sub-verwerkers te benoemen en aan te geven welke rol zij in de keten hebben. Deze sub-verwerkers dienen ook aan de gestelde eisen met betrekking tot informatieveiligheid te voldoen, zoals die aan opdrachtnemer gesteld zijn.**
E.32	**De volgende risicovolle situaties zijn niet toegestaan zonder expliciete goedkeuring van Opdrachtgever:** **- Gebruik maken van een back-up dienst (al dan niet van derden) waarbij niet 100% zeker is dat de data binnen de Europese Economische Ruimte (EER) blijft.** **- Gebruik maken van beheerdiensten van partijen gevestigd buiten de EER.** **- Hergebruik van gemeentelijke data voor test- en acceptatiedoelen, zonder expliciete schriftelijke toestemming van Opdrachtgever.** **- Opslag van gemeentelijke data buiten de beveiligde omgeving, bijvoorbeeld op laptops van medewerkers om 'even' wat te testen, fouten te zoeken etc.** **Op voorhand zal Opdrachtgever geen toestemming geven voor deze situaties. Indien Leverancier aan één van bovenstaande risico's voldoet, dient hij dit kenbaar te maken via de Nota van inlichtingen.**
E.33	**De fysieke locaties van waar de SaaS-applicatie wordt gehost is beveiligd tegen toegang door onbevoegden. De locatie is adequaat – minimaal naar marktstandaarden -beveiligd tegen onheil van buitenaf, waaronder in ieder geval weersomstandigheden en vandalisme. Indien er sprake is van opslag van data bij een extern datacenter is dat datacenter NEN-ISO/IEC 27001 gecertificeerd of anderszins gecertificeerd.**
E.34	**De SaaS oplossing ondersteunt Roll Based Access Control (RBAC). Rechten hangen aan rollen en gebruikers worden gekoppeld aan rollen.**
E.35	**Gebruikers dienen alleen de gebruikerinterfaces/-menu's en onderliggende gegevens te zien waarvoor zij zijn geautoriseerd. Denk hierbij aan het principe 'need to know /least privileged'.**
E.36	**Er dient een totaaloverzicht (op elk moment en direct) beschikbaar te zijn van autorisaties van zowel Leverancier als Opdrachtgever verdeeld naar gebruikers per rol en autorisaties per rol (in het kader van de audittrail).**

E.37	**De SaaS-Applicatie en daarmee samenhangende diensten Leverancier stellen Opdrachtgever in staat om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO).**
E.38	**Leverancier moet een geldend ISO 27001 certificaat inclusief Verklaring van Toepasselijkheid of een ISAE 3402 SOC type II certificaat overleggen, of vergelijkbaar.**
E.39	**Leverancier behoudt deze certificering gedurende de gehele contractperiode en toont jaarlijks, d.m.v. een extern auditrapport, aan dat de informatiebeveiliging van de oplossing is gewaarborgd.**
E.40	**Alle software (front-end en back-end) behorend tot de (cloud)dienst is volgens relevante standaarden beveiligd, conformeert zich telkens aan de laatst bekende beveiligingsinzichten en is blijvend van voldoende kwaliteit. Richtlijnen van de Autoriteit Persoonsgegevens (AP), Nationaal Cyber Security Centrum (NCSC), Informatiebeveiligingsdienst voor gemeenten (IBD), Forum Standaardisatie en Open Web Application Security Project (OWASP) zijn hierbij normstellend.**
E.41	**Leverancier dient gebruik te maken van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen (Hardenen van systemen bestaat uit verschillende stappen om een gelaagde bescherming te bieden. Met behulp van antivirus, -spyware, -spam en -phishing software, regelmatig installeren van de laatste patches van Opdrachtnemer, het uitschakelen van onnodige software en diensten leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillende is te misbruiken). Hardening is een continu proces. Opdrachtnemer levert halfjaarlijks bewijsmiddelen op dat hardening wordt toegepast (conform SLA).**
E.42	**Er dient altijd gebruik gemaakt te worden van beveiligde internetverbindingen.**
E.43	**Gegevens die van en naar de SaaS-applicatie getransporteerd worden, in welke vorm dan ook, dienen beveiligd te worden door middel van encryptie. Hierbij dient gebruik te worden gemaakt van het SSL-protocol op basis van TLS 1.2 of beter of gelijkwaardig.**
E.44	**De versleutelde verbindingen worden voorzien van een SSL-certificaat en indien noodzakelijk PKIO certificaten. Hierbij wordt er te allen tijde gebruik gemaakt van een door de opdrachtgever vertrouwde certificaat autoriteit.**
E.45	**De opslag van gegevens op de servers dient versleuteld te gebeuren waarbij minimaal gebruik wordt gemaakt van AES-256.**
E.46	**Emailverkeer dat namens Opdrachtgever plaatsvindt (intern danwel extern) voldoet blijvend aan aanvullende beveiligingsmaatregelen als DNSSEC, SPF, DKIM, DMARC, STARTTLS en DANE. Leverancier definieert en valideert de SPF-, DKIM- en DMARC-records van het domein van Opdrachtgever conform de actuele configuratie van Opdrachtgever. Leverancier zorgt ervoor dat de partijen, die e-mailberichten ontvangen van Opdrachtgever, kunnen valideren dat deze emailberichten inderdaad van Opdrachtgever afkomstig zijn. Leverancier deelt daartoe tenminste de publieke sleutel van het DKIM sleutelpaar én de "selector" in de vorm van een TXT-record (voorkeur) of CNAME-record met Opdrachtgever zodat Opdrachtgever deze aan haar DNS-dienst kan koppelen.**
E.47	**Leverancier dient minimaal (1) maal per jaar een penetratie test uit te voeren. Een samenvatting van de rapportage hiervan is door de Opdrachtgever opvraagbaar.**

E.48	**Op verzoek van Opdrachtgever dient Leverancier mee te werken aan een penetratietest op de SaaS-applicatie.**
E.49	**Opdrachtgever moet in de logging terug kunnen zien wie de laatste wijziging omtrent datamutatie heeft uitgevoerd.**
E.50	**De logging biedt voldoende inzicht in de bijhouding, uitwisseling, en selecties van gegevens om het gebruik van een gegeven door een applicatie te kunnen achterhalen en hierop te signaleren of acteren.**

Onderdelen die minimaal in de logging opgenomen dienen te zijn:

- Gebruikerslogging
  - Datum/tijd van actie
  - Gebruikersnaam of gebruiker ID
  - Uitgevoerde handeling
  - Object waarop de handeling werd uitgevoerd
  - Handelingen van gebruikers met speciale bevoegdheden

- Systeemlogging
  - Opgetreden fouten (error log)
  - (Poging tot) ongeautoriseerde toegang
  - (Poging tot) wijziging van beveiligingsinstellingen

In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, etc.). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de Opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts).

E.51	**De SaaS-applicatie moet bovenstaande systeem logging beschikbaar stellen aan de SIEM oplossing van de opdrachtgever. Denk hierbij bijvoorbeeld aan het uitlezen van de logging van de SaaS-applicatie via een API.**

Wanneer Leverancier zelf een SIEM oplossing heeft draaien, is dit ook voldoende.

E.52	**Logging wordt minimaal een half jaar bewaard voor eventueel onderzoek.**

1.4 Eisen Privacy

E.53	**Bewaartermijnen kunnen ingericht worden**
W.3	**Faciliteiten om recht op dataportabiliteit te kunnen accomoderen als dit wordt ingeroepen.**
E.54	**De infrastructuur, de geleverde dienst en organisatie van de Opdrachtnemer voldoen aan de voorwaarden genoemd in de Algemene verordening Gegevensbescherming (AVG) en de uitvoeringswet algemene verordening Gegevensbescherming (UAVG)**
E.55	**In de Oplossing zijn functionaliteiten opgenomen voor de privacy officers, om aan drie AVG taken invulling te geven: 1) transparantie van gegevens, 2) recht op inzage en 3) gegevensminimalisatie.**

E.56	**Opdrachtgever eist voor aanvang van implementatie dat er een verwerkersovereenkomst wordt ingevuld en ondertekend conform het VNG model standaard verwerkersovereenkomst.**
E.57	**Op verzoek van Opdrachtgever dient de Opdrachtnemer een Data Protection Impact Assessment aan te leveren aan de opdrachtgever en indien die niet beschikbaar is mee te werken aan het uitvoeren (DPIA) op de SaaS-applicatie. Dit moet gebeuren voordat de applicatie echte persoonsgegevens bevat.**
E.58	**Opdrachtnemer heeft een bewustwordingscampagne voor het personeel van de eigen organisatie met betrekking tot de toepasselijke beleidsregels, processen en procedures.**
W.4	**Opdrachtnemer geeft hier blijk aan voorgaande eis door twee (2) bewijsstukken aan te leveren waaruit blijkt dat er actief aan bewustwording op deze thema's wordt voldaan.**
E.59	**Opdrachtnemer verleent alle benodigde assistentie wanneer zich een inbreuk in verband met persoonsgegevens (datalek) voordoet (ex artikel 33 en 34 AVG).**
E.60	**Opdrachtnemer meldt een (vermoeden van) inbreuk binnen 24 uur aan Opdrachtgever.**
E.61	**Een verwijderverzoek voor een dossier moet binnen 7 dagen worden afgerond.**
E.62	**De verwijdering/anonimisering van persoonsgegevens vindt op een aantoonbare wijze plaats.**
E.63	**Indien Leverancier gebruik maakt van meerdere sub-verwerkers, dient Leverancier met deze sub-verwerkers een sub-verwerkersovereenkomst te hebben.**

1.5 Functioneel/technisch beheer

E.64	**Dagelijkse functionele beheertaken kunnen worden uitgevoerd, zonder dat dit invloed heeft op de werking van de SaaS-applicatie voor de overige gebruikers en op andere ICT oplossingen.**
E.65	**Gebruikers kunnen ingelogd blijven en volledig gebruik blijven maken van de SaaS-applicatie tijdens dagelijkse functionele beheertaken.**
E.66	**Autorisaties dienen middels een beheerinterface gebruiksvriendelijk te kunnen worden geconfigureerd.**
W.5	**De beheerder dient zelf de logging en auditrail(rapportages) in te kunnen instellen.**
E.67	**De beheerder dient efficiënt en flexibel in te spelen op wijzigingen in werkprocessen. Dit houdt in dat de beheerder workflows snel aan kan passen.**
E.68	**De beschikbaarheid en ondersteuning van de SaaS-applicatie is binnen de contractperiode gegarandeerd.**
E.69	**Het systeem- en technisch beheer dient geheel verzorgt te worden door Leverancier. Technisch applicatiebeheer betreft de werkzaamheden die nodig zijn voor het waarborgen van de ononderbroken goede werking van de SaaS-oplossing.**
E.70	**Er dient op geen enkele wijze sprake te zijn van inlogmogelijkheden voor Leverancier of diens voor deze opdracht in te zetten derden (backdoor) waar Opdrachtgever niet van op de hoogte is. Toegang tot de omgeving gaat altijd na overleg vooraf.**
E.71	**Alle wijzigingen/updates worden door Leverancier altijd eerst getest voordat deze in productie worden genomen.**
E.72	**Opdrachtgever wenst inzicht te hebben in de wijziging(en) die in een release zijn opgenomen. Leverancier informeert Opdrachtgever op actieve wijze over releases.**

1.6 Eisen gegevensbeheer

E.73	**Metadatering**
De bronnen zijn voorzien van metadatering, zoals eigenaar, versiebeheer, frequentie van updates	
E.74	**De data zijn en blijven eigendom van Opdrachtgever**

1.6.1. Archivering en vernietiging

W.6	**Applicatie/systeem voldoet aan de geldende Archiefwet en daaruit vloeiende regelingen (o.a. de NEN-ISO 16175)**
W.7	**Applicatie/systeem voldoet aan TMLO/MDTO**
E.75	**Bij een export kan de metadata in een gangbaar machinaal leesbaar bestandsformaat meegeleverd worden, zoals XML.**

1.6.2 Integratie en koppelingen

E.76	**Alle bronnen uit de bijlage 'Te ontsluiten bronnen' worden ontsloten en datamodellen worden opgemaakt.**
E.77	**De SaaS-applicatie moet koppelen met de Azure Active Directory van Opdrachtgever.**
E.78	**De SaaS-applicatie moet Single Sign On ondersteunen in relatie tot de Azure Active Directory.**
E.79	**De SaaS-applicatie moet 2 factor authentication ondersteunen.**
E.80	**Alle data van de SaaS-applicatie moet via een beveiligde database verbinding kunnen worden toegevoegd, opgevraagd, gemuteerd en worden verwijderd.**

1.7 Trainingen, kennisoverdracht, en documentatie

E.81	**Inrichting, gebruik, en beheer van de componenten binnen het Azure dataframework**
Toegespitst op eigen situatie + geschreven documentatie	
E.82	**Inrichting, gebruik, en beheer van het DWH**
Toegespitst op eigen situatie + geschreven documentatie	
E.83	**Inrichting, beheer, en gebruik van koppelingen met verschillende bronnen en de laadprocessen**
Toegespitst op eigen situatie + geschreven documentatie	
E.84	**Oplevering van een beschrijving van de geïmplementeerde architectuur**
Een beschrijving van de gebruikte componenten, waar mogelijk visueel ondersteund door tekeningen.	

E.85	Vorm van training en kennisoverdracht
De opdrachtgever hanteert het principe ‘leren door te doen’. Opdrachtnemer neemt daarom de BI-ontwikkelaar mee in het gehele proces van de inrichting van PowerBI. Het Doel is dat de BI-ontwikkelaar uiteindelijk zelfstandig de PowerBI omgeving kan beheren en verder kan ontwikkelen.	

1.8 Service Level Agreement (SLA)

E.86	**Leverancier beschikt over een Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning ter ondersteuning bij onderhavige opdracht. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan.**
E.87	**De helpdesk van Leverancier levert zowel telefonische ondersteuning als ondersteuning via e- mail en/of een web-portaal/kennisbank.**
E.88	**De helpdesk dient op werkdagen telefonisch bereikbaar te zijn tussen 09.00 en 17.00 uur. Voor ondersteuning door de helpdesk (eerste lijn) van de Opdrachtnemer worden geen aanvullende kosten in rekening gebracht. Daarnaast is er een noodnummer beschikbaar voor calamiteiten.**
W.8	**Leverancier geeft inzicht in tickets die door andere klanten zijn aangemeld zodat opdrachtgever daarin kan zoeken om het probleem zelf op te lossen.**
E.89	**Beveiligingsincidenten worden zo snel als mogelijk gemeld aan de Opdrachtgever, maar niet later dan 24 uur na ontdekking van het incident.**
E.90	**De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de SaaS-applicatie volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). Opdrachtgever bepaalt prioriteit van incidenten. T.a.v. ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:** **1. De SaaS-applicatie is volledig niet beschikbaar (naar mening van de Opdrachtgever een Critical Problem)** **2. De SaaS-applicatie is deels niet beschikbaar of deels niet beschikbaar 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.**
E.91	**In relatie tot E99, Reactietijd binnen:** **• Prio 1: 0-1/2 uur beantwoorden (24/7) Work-around binnen 4 uur, oplossing binnen 8 uur.** **• Prio 2: 2 uur beantwoorden (Op werkdagen tussen Work-around binnen 8 uur op werkdagen, 9.00 en 17.00 uur) Oplossing binnen 48 uur op werkdagen** **• Prio 3: 4 uur beantwoorden (Op werkdagen tussen Work-around binnen 2 werkdagen, 9.00 en 17.00 uur) Oplossing in volgende reguliere versie** **• Prio 4: 8 uur beantwoorden (Op werkdagen tussen Antwoord binnen 1 week 9.00 en 17.00 uur)** **De prioritering wordt door Opdrachtgever bepaald.**
E.92	**De helpdesk draagt tevens zorg voor het relateren van incidenten aan reeds bekende problemen m.b.t. de SaaS-applicatie. Leverancier maakt voor 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.**

E.93	**Op aanvraag van Opdrachtgever dient er een overzicht te kunnen worden aangeleverd over de beschikbaarheid van de SaaS-applicatie en het aantal helpdeskcalls waarbij de doorlooptijd inzichtelijk is.**
E.94	**Onderhoudstijden van Leverancier worden ingepland buiten werktijden. Gepland onderhoud vindt derhalve plaats op avonden, weekenden of op nationale feestdagen.**
E.95	**Werkzaamheden door Leverancier worden altijd minimaal veertien (14) kalenderdagen van tevoren gecommuniceerd.**
E.96	**Een uitzondering op de vaste onderhoudstijden (inclusief communicatie) zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn, informatieveiligheidsincidenten en rampen.**
E.97	**Er vinden periodiek (ieder kwartaal) account- en evaluatiegesprekken plaats. Hierin worden onder andere de KPI's, dienstverlening, roadmap van Leverancier en eventuele ontwikkelingen besproken.**

Bijlage 1
Te ontsluiten bronnen

Systeem	Leverancier
Careernet	Careernet
Flexwestbrabant	Netive
ERPx	Unit4
Youforce	Visma Raet
Diverse Excelschema’s opgeslagen in Sharepoint of Onedrive	

DIt betreft een niet limitatieve lijst, die aan verandering onderhevig kan zijn.