## Bijlage Programma van Eisen

Onderdeel van het Programma van Eisen zijn de Aansluitvoorwaarden, PSA en Regionale Enterprise Architectuur, opgenomen als separate bijlagen.

## Inhoudsopgave



**Betreft: Gewijzigde versie t.a.v. Nota van Inlichtingen II d.d. 21 februari 2024**

## 1. Algemene Eisen

| Nr. | Omschrijving |
|---|---|
| **1.1** | Opdrachtnemer gaat akkoord met de voorwaarden benoemd in GIBIT 2020 en verwerpt daarmee de eigen voorwaarden. |
| **1.2** | (Technische) documentatie wordt continu up-to-date gehouden en de laatste versie wordt actief gedeeld met de Opdrachtgever. |
| **1.3** | Medewerkers van de Opdrachtnemer, die in enige mate toegang hebben tot de verzamelde gegevens, zijn gescreend op integriteit, waarbij de minimale eis is dat werknemer bij indiensttreding aan Opdrachtnemer een specifiek voor de functie geldende Verklaring omtrent Gedrag (VOG-verklaring) heeft overlegd, die bij indiensttreding niet ouder is dan 3 maanden. |

## 2. Oplossing

| Nr. | Omschrijving |
|---|---|
| **2.1** | Opdrachtnemer geeft aan dat de toegepaste oplossing geen merkbare belasting creëert op het netwerk van de Opdrachtgever. |
| **2.2** | Opdrachtnemer levert een high level design aan waarin koppelingen met interne en externe systemen en netwerkcomponenten uitgewerkt zijn. |
| **2.3** | Opdrachtnemer dient te specificeren welke netwerkprotocollen (w.o. StUF, rNLX, estder-API's, IPv4, IPv6, SFTP/FTPS etc.) en applicaties worden toegepast voor communicatie tussen endpoints en de toepassing. De netwerkprotocollen dienen versleuteld te zijn. |
| **2.4** | De Oplossing en dataopslag dienen zich te allen tijde fysiek op een locatie binnen de EER (Europese Economische Ruimte) te bevinden. |
| **2.5** | Vooraf geïdentificeerde medewerkers van Opdrachtgever dienen volledige toegang te hebben tot de Oplossing, teneinde zelf triage en analyse te kunnen uitvoeren en ter verkrijgen van additionele context in het geval van een security incident.<br>Toegangsbeheer is de verantwoordelijkheid van de Opdrachtgever. |
| **2.6** | Autorisatie dient geïmplementeerd te worden op basis van minimaal benodigde rechten. |
| **2.7** | Indien de oplossing een eigen identity store gebruikt, dan is deze toegankelijk voor provisioning door middel van standaard API calls.<br>De applicatie biedt de mogelijkheid om de actuele status van alle identiteiten op te vragen, ten behoeve van provisioning, reconciliatie en audit.<br><br>*Aanvulling NVI I d.d. 02-02-2024:*<br>Een API omgeving van de TOPdesk instance kan beschikbaar worden gesteld voor het realiseren van bovengenoemde koppeling. |
| **2.8** | Alle activiteiten van gebruikers en beheerders worden gelogd en zijn inzichtelijk voor Opdrachtgever wanneer daar om gevraagd wordt. |
| **2.9** | Alle accounts zijn herleidbaar naar een persoon, het delen van accounts is niet toegestaan. |
| **2.10** | Opdrachtgever kan verlangen dat technische details van een incident en de Oplossing worden gedeeld met Opdrachtgever of met een derde partij teneinde deze te analyseren en/of vast te kunnen stellen of herhaling aannemelijk is. Dit ontslaat Opdrachtnemer niet van haar verplichting tot eigen analyse. |
| **2.11** | Opdrachtnemer neemt de verantwoordelijkheid om passende connectoren te bieden om componenten die niet "out-of-the-box" kunnen worden aangesloten op de producten die Opdrachtnemer gebruikt in de Oplossing, alsnog aan te kunnen sluiten op de aangeboden Oplossing. |

| | |
|---|---|
| **2.12** | Voor beveiligingsfuncties wordt alleen gebruik gemaakt van cryptografie volgens voorschriften en moderne richtlijnen zonder wijzigingen. De Oplossing gebruikt alleen cryptografische algoritmen die ECRYPT (ECRYPT - CSA, "D5.4 Algorithms, Key Size and Protocols Report," 2018) aanbeveelt als geschikt voor nieuwe of toekomstige systemen. Sleutels zijn minstens zo lang als dit ECRYPT-rapport aanbeveelt voor gebruik op korte termijn. |
| **2.13** | Opdrachtnemer is verantwoordelijk voor het opleveren en actueel houden van de High Level Design en Low Level Design documentatie en het veiligstellen van configuratiebestanden en stelt deze op verzoek van Opdrachtgever voor implementatie beschikbaar. De designs worden afgestemd met de architecten van de Opdrachtgever en worden actueel gehouden.<br><br>*Aanvulling NVI I d.d. 02-02-2024:*<br>AD dient goedkeuring te geven op wijzigingen op HLD en LLD documenten. Aanpassing op HLD en LLD vanuit AD, dan zal Inschrijver hierbij betrokken worden. |
| **2.14** | De Oplossing is geïntegreerd in de Microsoft tenant van Opdrachtgever. |
| **2.15** | De Oplossing moet in staat zijn om real-time eventcorrelatie te bieden tussen multi-vendor-technologieën voor ten minste het systeem en de applicatie. |
| **2.16** | De Oplossing moet in staat zijn om op patronen gebaseerde correlatieregels te bieden in plaats van een regel voor elke mogelijke exploit. |
| **2.17** | Opdrachtnemer draagt zorg voor de koppeling tussen de Oplossing en het interne Incident Managementsysteem van Opdrachtgever (TOPdesk). |
| **2.18** | De Oplossing dient 7x24 uur monitoring te faciliteren, waarbij fysiek toezicht op de monitoring plaatsvindt binnen de normale kantooruren in Nederland. Het wordt verwacht dat er tijdens kantooruren door gekwalificeerde specialisten analyses worden uitgevoerd. In de avond- en nachtelijke uren als ook in het weekend mag een combinatie van geautomatiseerde monitoring met piketdienst worden toegepast. |
| **2.19** | Opdrachtnemer levert een High Level Design, passend bij de architectuur van de Opdrachtgever, waarin de samenhang is beschreven tussen de (MDR) Oplossing van Opdrachtnemer en de componenten binnen het landschap waarop gemonitord wordt. |
| **2.20** | Opdrachtnemer adviseert Opdrachtgever over de vereiste Use Cases en connectoren. |
| **2.21** | Opdrachtgever wordt eigenaar van de Oplossing, de geleverde Use Cases, Rapportage templates en connectoren welke opgeleverd worden. |
| **2.22** | *Vervalt, vervangen door hoofdstuk 8* |
| **2.23** | De Oplossing dient plaats- en tijdonafhankelijk toegankelijk te zijn voor medewerkers van Opdrachtgever. |
| **2.24** | Alle data van Opdrachtgever is logisch gescheiden van overige klanten van Opdrachtnemer, de security en performance worden niet beïnvloed door andere gebruikers van de dienst. |
| **2.25** | Data protection is een vereiste, data wordt niet gedeeld/doorverkocht aan derde partijen. |
| **2.26** | Data in rust is versleuteld op basis van bewezen technologie. |
| **2.27** | Data in transport is versleuteld op basis van bewezen technologie. |
| **2.28** | Opdrachtnemer draagt zorg voor de continuïteit van de dienst, alsmede voor een vooraf gedeeld Exit-plan bij beëindiging van de dienstverlening. |
| **2.29** | Opdrachtnemer draagt zorg voor het up-to-date houden van de relevante certificeringen van haar organisatie en medewerkers en verstrekt daarover jaarlijks updates aan de Opdrachtgever. |
| **2.30** | *Eis aangepast:*<br>Opdrachtnemer onderhoudt Opdrachtgever specifieke use cases (alerts). Deze use cases worden door de Opdrachtnemer in samenwerking met het securityteam van |

| | |
|---|---|
| | Opdrachtgever opgesteld. Dit omvat in ieder geval: configuratie van alerts, integratie van benodigde databronnen, validatie (testen) en de ontwikkeling, uitvoering en onderhoud van incident response playbooks. |

## 3. Implementatie

| Nr | Omschrijving |
|---|---|
| **3.1** | Opdrachtnemer is volledig eindverantwoordelijk voor de aan Opdrachtgever aangeboden dienstverlening en fungeert als enige aanspreekpunt hieromtrent. |
| **3.2** | Bij de implementatie van de Oplossing levert de Opdrachtnemer training/begeleiding aan de leden van het security-team van Opdrachtgever om de relevante delen van de Oplossing en ondersteunende tooling in scope van de aangeboden dienst te gebruiken. |
| **3.3** | *Eis aangepast:*<br>De Opdrachtnemer moet de eerste implementatie (11 use cases) afgerond hebben binnen 4 maanden na start implementatie en mits benodigde informatie tijdig wordt aangeleverd door AD. |
| **3.4** | *Eis aangepast:*<br>Opdrachtnemer biedt volledige en kosteloze medewerking aan maximaal 2 audits per jaar die vanuit Opdrachtgever uitgevoerd worden op de Oplossing. |
| **3.5** | Opdrachtnemer draagt zorg dat de inspanningen aan de zijde van Opdrachtnemer en Opdrachtgever evenredig verdeeld zijn. |

## 4. Documentatie, Processen en Communicatie

| Nr. | Omschrijving |
|---|---|
| **4.1** | Alle (schriftelijke en mondelinge) communicatie tussen Opdrachtnemer en Opdrachtgever vindt plaats in het Nederlands. In het geval van specialistische ondersteuning is Engelstalige communicatie (na overeenstemming met Opdrachtgever) toegestaan.<br><br>*Aanvulling NVI I d.d. 02-02-2024:*<br>Daarbij geldt dat tactisch en strategisch overleg in het Nederlands plaatsvindt. Operationele communicatie mag in het Engels worden gedeeld. |
| **4.2** | De aangeboden Oplossing dient 24x7 detectie te kunnen uitvoeren. |
| **4.3** | *Vervalt, vervangen door hoofdstuk 8* |
| **4.4** | *Vervalt, vervangen door hoofdstuk 8* |
| **4.5** | Opdrachtnemer verzorgt de schriftelijke verslaglegging van alle projectoverleggen (met uitzondering van de operationele overleggen, hier volstaat een actie- en besluitenlijst) en levert deze binnen vijf werkdagen na het overleg bij Opdrachtgever digitaal aan. Opdrachtgever geeft een reactie op het verslag binnen vijf werkdagen aan Opdrachtnemer. |
| **4.6** | Opdrachtnemer biedt Opdrachtgever de mogelijkheid om ticketinformatie en false positives uit te wisselen middels een geautomatiseerde koppeling tussen de beide IT Service Management tools via een REST API. |
| **4.7** | *Vervalt, vervangen door hoofdstuk 8* |
| **4.8** | Een security event/incident wordt geregistreerd in het ticketsysteem van Opdrachtnemer via geautomatiseerde koppeling(en). Deze registratie moet volledig en actueel zijn. Opdrachtgever verwacht dat dit event minimaal aan de volgende eisen voldoet:<br>• Internet Protocol adres, numeriek label gekoppeld aan elk device geconnect aan het netwerk;<br>• Fully Qualified Domain Name, mits gerelateerd aan een webpagina;<br>• Configuration Item (CI): iedere computer, device, software, of service in de CMDB;<br>• Locatie waar het incident is gedetecteerd; |

| | |
|---|---|
| | • Korte beschrijving van de analyse en bijbehorende voorgestelde acties die worden verwacht van de oplosgroep aan wie het event wordt toegewezen;<br>• Volledige beschrijving van alle acties die worden verwacht van de oplosgroep aan wie het event wordt toegewezen.<br>*Aanvulling NVI I d.d. 02-02-2024:*<br>Er worden geen CMDB gegevens uit de TOPdesk omgeving van AD ingelezen in het ticketsysteem van Opdrachtnemer. Wel dient in het ticketsysteem opgeslagen te worden op welke IP adres een event verschijnt. Er volgt nog overleg met onze privacy officers om te bepalen welke info (user id, werkplek id) wel/niet in het ticketsysteem van Inschrijver mag worden opgeslagen. |
| **4.9** | Opdrachtnemer biedt Opdrachtgever optimaal support om False Positives zo spoedig te voorkomen in het voorkomen van nieuwe False Positives om via deze werkwijze de relevantie en kwaliteit van de detectie adequaat en correct te houden. |
| **4.10** | Preventief onderhoud vindt altijd plaats tijdens een, minimaal, 3 maanden vooraf overeengekomen onderhoudsvenster. |
| **4.11** | Opdrachtnemer zal toestaan dat Opdrachtgever reguliere kwetsbaarhedenanalyses (vulnerability scans) en penetratietesten uitvoert op de Oplossing, waarbij Opdrachtgever voorafgaand met Opdrachtnemer afstemming heeft over scope en tijdstip. |
| **4.12** | Opdrachtnemer dient voor Opdrachtgever een real-time dashboard te implementeren waarin op hoofdlijnen de uitkomsten van de dienstverlening voor Opdrachtgever inzichtelijk is. Hierbij dienen minimaal het aantal security incidenten, mogelijke cyberaanvallen, trendrapportages en uitkomsten van Use Cases te worden weergegeven in een overzichtelijk scherm. |
| **4.13** | De Opdrachtnemer levert capaciteit, wanneer nodig, om snelle response uit te voeren naar aanleiding van een security incident of dreiging. |
| **4.14** | Opdrachtnemer is volledig verantwoordelijk voor het lifecycle management en de periodieke updates en upgrades van componenten die onderdeel zijn van de dienst. |
| **4.15** | Opdrachtgever dient direct geïnformeerd te worden zodra er (mogelijk) een aanval wordt voorbereid op Opdrachtgever of de gehele sector Lokale Overheid. Opdrachtnemer adviseert en ondersteunt Opdrachtgever in het nemen van mitigerende maatregelen. |
| **4.16** | Opdrachtnemer dient kennisborging en -deling minimaal op het gebied van domeinspecifieke, technologische, organisatorische kennis en ervaringen welke relevant is voor de (toekomstige) dienstverlening aan Opdrachtgever te borgen. |
| **4.17** | Opdrachtnemer dient een Service Continuity Plan beschikbaar te stellen die de continuïteit van de dienstverlening waarborgt en voldoet aan minimaal de volgende aspecten:<br>• Het periodiek testen en evalueren van het Service Continuity Plan;<br>• Het onderhouden van het Service Continuity Plan (bijvoorbeeld door veranderingen in de onderliggende infrastructuur of productportfolio van de dienstverlening). |
| **4.18** | Binnen zes weken na ondertekening levert de Opdrachtnemer een volledig Dossier Afspraken en Procedures (DAP) met als voorwaarden dat AD tijdig de benodigde informatie aanlevert. De Opdrachtnemer blijft gedurende de contractperiode de penvoerder van het betreffende document. |
| **4.19** | Opdrachtnemer escaleert informatiebeveiligingsincidenten tijdig. Tijdige afhandeling en mitigerende acties zijn belangrijk. Het beste is als er op basis van ‘early warnings en/of ‘indicators of compromise’ proactief opgetreden kan worden. |
| **4.20** | Opdrachtnemer rapporteert op een begrijpelijke manier, rekening houdend met de verschillende doelgroepen. Door middel van het security dashboard wordt real-time gerapporteerd aan het securityteam van De Connectie. |
| **4.21** | De Opdrachtnemer maakt gebruik van het Azure Sentinel platform van AD om operationeel monitoring uit te voeren. Dit mag/kan direct of indirect door middel van een applicatie-, rapportage- of BI-schil. |

## 5. Prijsmodel

| Nr | Omschrijving |
|---|---|
| **5.1** | Het ingevulde Prijsmodel dient een weergave te zijn van de totale kosten van de Inschrijving, wat inzicht geeft in de TCO van deze dienst gedurende 4 jaar, inclusief de implementatie. Dat wil zeggen alle kosten nodig om invulling te geven aan de offerteaanvraag (inclusief alle bijlagen) zijn meegenomen bij het invullen van het prijsmodel. |
| **5.2** | Het Prijsmodel dient volledig te zijn ingevuld. Een onvolledig ingevuld prijsmodel kan leiden tot uitsluiting van verdere deelname. Een prijsmodel is volledig ingevuld als alle blauwe velden: relevante informatie over de prijscomponenten, prijzen, "n.v.t." of 0 (nul) bevatten. Andere door Opdrachtnemer aangebrachte wijzigingen in het prijsmodel kunnen leiden tot uitsluiting van verdere deelname. |
| **5.3** | De opgegeven prijzen zullen gedurende de gehele duur van de overeenkomst gehandhaafd worden. Jaarlijks kunnen de prijzen worden geïndexeerd o.b.v. de indexatierichtlijn in GIBIT 2020. |
| **5.4** | Bij verlenging van de overeenkomst zullen de prijzen gehandhaafd blijven. Bij verlenging geldt dezelfde mogelijke indexering o.b.v. GIBIT 2020.<br><br>*Aanvulling NVI I d.d. 02-02-2024:*<br>Met verlengen doelt Opdrachtnemer op de optionele verlengingsjaren (2x2 jaar) zoals genoemd in het Aanbestedingsdocument. |
| **5.5** | Opdrachtnemer vult op basis van de Kengetallen en zijn ervaringscijfers een prijs per eenheid in, en legt deze vast in een aanname waarin de directe relatie tussen Kengetallen en ervaringscijfers en prijs per eenheid is vastgelegd. |
| **5.6** | De Implementatiekosten zijn fixed price. De Implementatiekosten zijn gebaseerd op Implementatie-aanpak van de Opdrachtnemer zoals vastgelegd met begrote uren. |
| **5.7** | De Implementatiekosten zijn maximaal 30% van de Inschrijfprijs. |
| **5.8** | Opdrachtgever is geen kosten verschuldigd aan Opdrachtnemer voor de retransitie en het onderhouden van het Exit-plan. |

## 6. Privacy & Security

| Nr | Omschrijving |
|---|---|
| **6.1** | Opdrachtnemer stemt ermee in dat de persoonsgegevens die worden verwerkt en opgeslagen door de dienstverlening vallen onder de verantwoordelijkheid en daarmee zeggenschap van Opdrachtgever. |
| **6.2** | Opdrachtnemer stemt ermee in dat alleen false positives zonder persoonsgegevens gebruikt mogen worden voor het verbeteren van de dienstverlening. |
| **6.3** | Opdrachtnemer stemt ermee in dat specifieke instellingen en/of configuraties van Opdrachtgever vallen onder (intellectueel) eigendom van Opdrachtgever. |
| **6.4** | Opdrachtnemer moet (oudere) versies van eventueel gebruikte algoritmes vastleggen en deze ter beschikking stellen op het moment dat daar een gerechtvaardigd verzoek voor komt.<br><br>*Aanvulling NVI I d.d. 02-02-2024:*<br>Gerechtvaardigde verzoeken zijn o.a. audits en forensisch onderzoek. Opdrachtgever dient de nodige informatie te voorzien als hiervan uit deze redenen vraag voor is.<br>Opdrachtgever bedoelt met algoritmes de gebruikte monitoring en detectie instellingen. |
| **6.5** | Opdrachtnemer past de principes van Security by Design en Privacy by Design toe door de Security Officers en Privacy Officers van Opdrachtgever te betrekken bij het configureren van de dienstverlening voor Opdrachtgever. |

## 7. Retransitie (Exitplan)

| Nr | Omschrijving |
|---|---|
| **7.1** | Gedurende de retransitie wordt de dienstverlening door Opdrachtnemer tegen gelijkblijvende voorwaarden en serviceniveaus geleverd als voorafgaand aan de retransitie. |
| **7.2** | Opdrachtnemer levert één (1) maand voor einde van de Overeenkomst aan Opdrachtgever een overzicht van alle verzamelde gegevens van de Opdrachtgever voortkomend uit de geleverde dienstverlening. Opdrachtnemer draagt op verzoek van Opdrachtgever de verzamelde gegevens – waaronder informatie over de meest recente versies van Use Cases en het kunnen detecteren van afwijkend gedrag binnen de infrastructuur van de Opdrachtgever - over aan Opdrachtgever. |
| **7.3** | Opdrachtnemer vernietigt na overleg met Opdrachtgever aan het eind van de Overeenkomst alle informatie die Opdrachtnemer tijdens het leveren van de dienstverlening heeft verzameld over Opdrachtgever. Tevens wordt een bewijs van vernietiging aangeleverd. |
| **7.4** | Opdrachtnemer vernietigt alle datadragers van de monitoringvoorziening op locatie bij Opdrachtgever, zodra deze van de locatie worden verwijderd. Deze vernietiging voert Opdrachtnemer uit conform NIST SP800-88 of vergelijkbaar. Het certificaat wordt overhandigd aan Opdrachtgever. |

## 8. SLA \ Dienstverlening

| Nr | Omschrijving |
|---|---|
| **8.1** | Na gunning volgen afspraken wie penvoerder van de SLA wordt. Indien Opdrachtnemer een eigen SLA heeft, dan dient deze bij inschrijving meegestuurd te worden inclusief gekenmerkt welke onderdelen afwijken van de eisen uit deze aanbesteding. Voorwaarde is dat de eigen SLA minimaal voldoet aan de gestelde eisen. |
| **8.2** | De aangeboden oplossing dient gedurende de looptijd van het contract, inclusief de optionele verlengingstermijnen, ondersteund en onderhouden te worden met inachtneming van het Overeengekomen gebruik (de Applicatie Specifieke eisen en wensen).<br><br>Mochten functionaliteiten van het Overeengekomen gebruik in toekomstige updates komen te vervallen, dan verwittigd Opdrachtnemer twee (2) maanden voorafgaand aan de update Opdrachtgever van deze wijziging.<br><br>Het is aan Opdrachtgever te beslissen om de vervallen functionaliteit (beperken van het Overeengekomen gebruik) te accepteren of niet.<br><br>Indien Opdrachtgever niet akkoord is met het vervallen van die functionaliteit, zal de laatst geaccepteerde versie gebruikt blijven worden waarbij Opdrachtnemer gedurende de volledige looptijd van het contract, inclusief de optionele verleningstermijnen die versie zal ondersteunen en zorgdragen dat die versie blijft voldoen aan regel- en wetgeving, inclusief het verzorgen van security patches. |
| **8.3** | Indien functionaliteiten in toekomstige updates komen te vervallen, verwittigd Opdrachtnemer twee (2) maanden voorafgaand aan de update Opdrachtgever van deze wijziging.<br>Bij het vervallen van (delen van) functionaliteiten in toekomstige updates is het aan Opdrachtgever om te besluiten om de nieuwe versie niet in gebruik te nemen en door te blijven werken met de laatst geaccepteerde versie die op dat moment in gebruik is. |

<table>
<tr><td></td><td>Opdrachtnemer zal gedurende de lopende contractperiode inclusief de optionele verlengingsjaren de laatst geaccepteerde versie blijven ondersteunen en zorgdragen dat die versie blijft voldoen aan regel- en wetgeving, inclusief het verzorgen van security patches.</td></tr>
<tr><td>8.4</td><td>Opdrachtnemer levert per kwartaal onderstaande rapportages aan Opdrachtgever:<br>Effectiviteit van de Use Cases:<br>• Adviezen voor nieuwe Use Cases;<br>• Gewijzigde / Toegevoegde use cases over afgelopen periode;<br>• Overzicht uitgevoerde werkzaamheden/updates (RFC’s), inclusief percentage 1e keer succesvol;<br>• Trends;<br>• Relevantie (wereldwijde) bedreigingen/ontwikkelingen in de markt;<br>• Security incidenten:<br>  ○ Afgesloten meldingen\events<br>  ○ Overzicht aantal meldingen die een incident worden<br>  ○ Status openstaande meldingen<br>  ○ Overzicht meldingen die afgesproken SLA normen overschreden hebben (verhouding tov totaal afgesloten meldingen)<br>  ○ Behaalde Responsetijden<br>  ○ Behaalde Oplostijden<br>• Beschikbaarheid MDR oplossing</td></tr>
<tr><td>8.5</td><td>De Servicedesk van Opdrachtnemer heeft een telefonische bereikbaarheid minimaal tijdens kantoortijden (ma t/m vrij 08.00 - 18.00).</td></tr>
<tr><td>8.6</td><td>Opdrachtnemer garandeert 24/7 een beschikbaarheid van de MDR oplossing van minimaal 99,9%. Opdrachtgever is zelf verantwoordelijk voor het beschikbaar zijn voor dat deel van de oplossing dat draait in de omgeving van Opdrachtgever.</td></tr>
<tr><td>8.7</td><td>Opdrachtnemer gaat akkoord met de onderstaande escalatiematrix.
<table>
<tr><th>Escalatie niveau</th><th>Rol Opdrachtgever</th><th>Rol Opdrachtnemer</th></tr>
<tr><td>1</td><td>Operationeel Verantwoordelijke</td><td>Operationeel Verantwoordelijke</td></tr>
<tr><td>2</td><td>Operationeel Verantwoordelijke<br>Contract- Leveranciersmanager</td><td>Operationeel Verantwoordelijke</td></tr>
<tr><td>3</td><td>Operationeel Verantwoordelijke<br>Contract- Leveranciersmanager<br>Contracteigenaar</td><td>Operationeel Verantwoordelijke<br>Teamleider Operationeel Verantwoordelijke</td></tr>
<tr><td>4</td><td>Contract- Leveranciersmanager<br>Contracteigenaar<br>Manager ICT</td><td>Operationeel Verantwoordelijke<br>Teamleider Operationeel Verantwoordelijke<br>Management</td></tr>
</table></td></tr>
<tr><td>8.8</td><td>Opdrachtnemer initieert een overleg op escalatieniveau 2 indien in de afgelopen kalendermaand de afgesproken normen m.b.t. de dienstverlening zoals genoemd in de gestelde eisen niet werden gehaald. In het overleg zal Opdrachtnemer en toelichting geven waarom de norm niet gehaald werd.<br><br>Opdrachtnemer maakt en deelt een verslag van dit overleg.</td></tr>
<tr><td>8.9</td><td>Opdrachtnemer initieert een overleg op escalatieniveau 3 indien in twee (2) achtereenvolgende maanden afgesproken normen m.b.t. de dienstverlening zoals genoemd in de gestelde eisen niet werden gehaald en levert voorafgaand aan dit gesprek een verbeterplan aan.<br>Het overleg inclusief het verbeterplan wordt binnen een kalendermaand na constatering van de tweede maand overschrijding ingepland.<br>Opdrachtnemer maakt en deelt een verslag van dit overleg.</td></tr>
</table>

<table>
<tr><td>8.10</td><td>Opdrachtnemer initieert een overleg op escalatieniveau 4 indien gestelde termijnen of overige afspraken uit overeengekomen verbeterplannen niet gehaald (kunnen) worden.</td></tr>
<tr><td>8.11</td><td>Opdrachtnemer garandeert dat 95% van uitgevoerde werkzaamheden/updates (RFC's) in één (1) keer correct opgeleverd worden.</td></tr>
<tr><td>8.12</td><td>Het staat Opdrachtgever vrij om in incidentele gevallen (max 5x per kalenderjaar) aan een melding een hogere prioriteit toe te kennen dan volgens de prioriteitenbepaling van toepassing zou zijn.</td></tr>
<tr><td>8.13</td><td>Opdrachtnemer garandeert dat op 95% van gedetecteerde security events\incidenten tijdig wordt gemeld (meldtijd).</td></tr>
<tr><td>8.14</td><td>Opdrachtnemer garandeert dat 95% van de gedetecteerde security events\incidenten tijdig een advies geleverd wordt om het probleem op te lossen of de gevolgen ervan te minimaliseren (oplostijd).</td></tr>
<tr><td>8.15</td><td>Opdrachtnemer gaat akkoord met onderstaande prioriteitenmatrix:
<table>
<tr><td>Prio 1 – Kritiek</td><td>• Risico 80% of meer van de dienstverlening aan de burgers is niet mogelijk of;<br>• Verwachte uitval van (een deel van) de informatievoorziening langer dan 8 uur of;<br>• Reële kans dat er negatieve berichtgeving over Inschrijver of haar partners in de landelijke pers gepubliceerd wordt of;<br>• Risico dat grote hoeveelheden gevoelige data lekt of onherstelbaar beschadigd raakt.</td></tr>
<tr><td>Prio 2 – Hoog</td><td>• Risico dat 60%-79% van de dienstverlening aan burgers niet mogelijk is of;<br>• Verwacht uitval van (een deel van) de informatievoorziening bedraagt 4-8 uur of;<br>• Reële kans dat er negatieve berichtgeving over Inschrijver of haar partners in de regionale pers gepubliceerd wordt of;<br>• Risico dat grote hoeveelheden gevoelige data lekt of beschadigd raakt.</td></tr>
<tr><td>Prio 3 – Medium</td><td>• Risico dat 40%-59% van de dienstverlening aan burgers niet mogelijk is of vertraagd verloopt of;<br>• Verwacht uitval van (een deel van) de informatievoorziening bedraagt 1-4 uur of;<br>• Reële kans dat er negatieve berichtgeving over Inschrijver of haar partners in de gemeentelijke pers gepubliceerd wordt of;<br>• Risico dat gevoelige data lekt of beschadigd raakt.</td></tr>
<tr><td>Prio 4 – Laag</td><td>• Risico dat (een deel) van de dienstverlening aan burgers vertraagd verloopt of;<br>• Verwacht uitval van (een deel van) de informatievoorziening bedraagt < 1 uur;</td></tr>
</table>
</td></tr>
</table>

**8.16**

| Prioriteit | Registratie melding [1]) | Melding ri. Opdrachtgever | Telefonisch ri. Opdrachtgever |
|---|---|---|---|
| 1 – Kritiek<br>• Meldtijd [2])<br>• Oplostijd [3]) | √<br>< 5 minuten<br>< 1 klokuur | √<br>< 15 minuten<br>< 1 klokuur | √<br>< 15 minuten<br>< 1 klokuur |
| 2 – Hoog<br>• Meldtijd [2])<br>• Oplostijd [3]) | √<br>< 5 minuten<br>< 4 klokuren | √<br>< 30 minuten<br>< 4 klokuren | √<br>< 30 minuten<br>< 4 klokuren |
| 3 – Medium<br>• Meldtijd [2])<br>• Oplostijd [3]) | √<br>< 5 minuten<br>< 8 klokuren | √<br>< 1 uur<br>< 8 klokuren | |
| 4 – Laag<br>• Meldtijd [2])<br>• Oplostijd [3]) | √<br>< 5 minuten<br>< 5 werkdagen | √<br>< 1 werkdag<br>< 5 werkdagen | |

[1]) Opdrachtgever heeft het registeren van een melding in het Service Desk Systeem van Inschrijver of ander registratiesysteem lager gezet dan de communicatie met Opdrachtgever zodat getoetst kan worden of de gestelde normen v.w.b. de communicatie met Opdrachtgever gehaald worden. Indien Inschrijver dit op een andere manier kan aantonen, dan kunnen daar na gunning nadere afspraken over gehad.

[2]) Onder Meldtijd (response) wordt verstaan: De tijd vanaf detectie van een mogelijk incident door Inschrijver inclusief de tijd benodigd voor het bepalen van de impact van het mogelijke incident (triage).

[3]) Onder Oplostijd wordt verstaan: De tijd vanaf detectie van een mogelijk incident door Inschrijver inclusief triage en analyse en het leveren van een advies om het risico op te lossen of de gevolgen ervan te minimaliseren (mitigerende maatregelingen).

| | |
|---|---|
| **8.17** | Opdrachtnemer levert uiterlijk 1 november een releasekalender met alle geplande releases t.b.v. Innovatief onderhoud voor het komende kalenderjaar. |
| **8.18** | Opdrachtnemer levert uiterlijk 1 november een releasekalender met alle geplande releases t.b.v. Preventief onderhoud voor het komende kalenderjaar. Onvoorzien Preventief (niet kritisch) onderhoud wordt minimaal 14 werkdagen vooraf gecommuniceerd met Opdrachtgever. |
| **8.19** | Bijgewerkte applicatie- of systeemdocumentatie wordt binnen 5 werkdagen opgeleverd door Opdrachtnemer. |
| **8.20** | 1x per kwartaal vindt er een Operationeel overleg plaats tussen Opdrachtnemer en Opdrachtgever.<br><br>Doelstelling: Bespreken samenwerking. |
| **8.21** | 2x per jaar vindt er een Tactisch overleg plaats tussen Opdrachtnemer en Opdrachtgever.<br><br>Doelstelling: Bespreken samenwerking en geleverde prestatie. Vanuit dit overleg kunnen aanpassingen in de SLA en/of DAP plaatsvinden. |
| **8.22** | 1x per jaar vindt er een Strategisch overleg plaats tussen Opdrachtnemer en Opdrachtgever.<br><br>Doelstelling: Afstemming roadmap Opdrachtnemer en Opdrachtgever. Benen op Tafel sessie. Lange termijn visie bespreken. |

| | |
|---|---|
| **8.23** | Op verzoek maximaal 2x per jaar vindt er (kosteloos) een Technische / Innovatie / Informatie / Adviessessie plaats tussen Opdrachtnemer en Opdrachtgever.<br><br>Doelstelling: Toelichting op technische ontwikkeling binnen het product of in de markt. |
| **8.24** | Na gunning werkt Opdrachtnemer mee aan het invullen van een verantwoordelijkheden matrix. |

| Verantwoordelijkheden Matrix | | | | |
|---|---|---|---|---|
| **Taak** | **Opdrachtgever (De Connectie)** | **Opdrachtgever (Gemeente)** | **Opdrachtnemer** | **Toelichting** |
| **Beheer gebruiksrechten** | | X | | |
| **Backup-/Recovery** | X | | | |
| **Aanmelden Incidenten** | | | | |
| **Rapporteren over Incidenten** | | | X | |
| **Netwerk & Connectivity** | | | | |
| **Inrichten koppelvlakken** | | | | |
| **...** | | | | |