

Concept SLA

Deze template bevat een globale lijst met aandachtspunten die relevant zijn bij het opstellen van een Service Level Agreement (SLA). Het toesnijden op iedere gemeentelijke individuele praktijksituatie is ondoenlijk en er kan dan ook niet ingegaan worden op het afbreukrisico's die in uw specifieke situatie gelopen wordt. Op basis van het af te nemen product en/of dienst en eigen risicoafweging dient de gemeente te beslissen welke aandachtspunten uit deze template relevant zijn. Deze relevante aandachtspunten kunnen daarna door de gemeente gebruikt worden om de nieuwe SLA op te stellen of de SLA van de dienstleverancier te beoordelen. Het kan ook voorkomen dat bepaalde onderwerpen en/of detaillering niet in deze SLA worden beschreven maar in een ander document worden opgenomen zoals Dossier afspraken en Procedures (DAP, inkoopvoorwaarden, contract/overeenkomst of bewerkersovereenkomst. Denk hierbij aan kwantitatieve afspraken zoals aantal gebruikers. Deze aantallen kunnen in de loop van de tijd veranderen en hiervoor wil je niet telkens de SLA aanpassen.

Uit deze template zijn t.b.v. de aanbesteding van Gemeente Tilburg voor de Woo Publicatievoorziening ter vermijding van verwarring de onderdelen verwijderd die reeds elders beschreven zijn of niet relevant geacht worden in SLA afspraken tussen haar en Opdrachtnemer.

i. Versiebeheer/Wijzigingshistorie

Hier worden de wijzigingen op de SLA beschreven die zijn goedgekeurd en door wie.

ii. Distributielijst

Hier worden de functies/personen opgesomd die een afschrift dienen te ontvangen van deze SLA.

iii. Leeswijzer

Hier wordt beschreven hoe dit SLA het beste gelezen kan worden, afhankelijk van de functie/taak en achtergrondkennis van de lezer.

0. Positie SLA en gerelateerde documenten

Hier wordt de samenhang beschreven tussen het contract / de overeenkomst en de SLA en de relatie met documenten die mogelijk als bijlagen op de SLA zijn bijgevoegd.

1 Inleiding

Deze SLA beschrijft de door de dienstleverancier geleverde diensten en specificaties van de applicatie, systeem of dienst, zoals deze aan de gemeente wordt aangeboden.

1.1 Doel van de SLA

Doel van de SLA is bindende kwalitatieve en kwantitatieve afspraken te maken over de kwaliteitsparameters voor het te realiseren dienstenniveau en over de rapportage daarover, met als doel om de kwaliteit en uitvoering van de dienstverlening te monitoren en te verbeteren.

1.2 Vastlegging van partijen en goedkeuring

Hier worden de contactgegevens van zowel de vertegenwoordiger van de leverancier van de dienst (Opdrachtnemer) als van de afnemer (Opdrachtgever) vermeld. Dit zijn meestal de personen die goedkeuring geven aan de SLA en namens beide partijen de SLA ondertekenen.

- **Vertegenwoordiger leverancier**
Hier worden de contactgegevens van de vertegenwoordiger van de leverancier (Opdrachtnemer) van de dienst vermeld, meestal is dit de service level manager.
- **Vertegenwoordiger gemeente**
Hier worden de contactgegevens van de vertegenwoordiger van de gemeente (Opdrachtgever) vermeld.
- **Goedkeuring**
De goedkeuring van de SLA is de gezamenlijke verantwoordelijkheid van de gemeente en de Opdrachtnemer (service level manager).

1.3 Ingangs- en einddatum

Hier worden de ingangs- en einddatums van de SLA beschreven, tevens wordt aangegeven of er een (tussen)evaluatie plaatsvindt.

2 Governance

Governance is het proces waarbij de dienstverlening wordt bestuurd en gecontroleerd. Het belangrijkste aandachtspunt is de manier waarop wijzigingen en updates van een dienst worden beheerd. Of het wijzigingsverzoek nu afkomstig is van de gemeente die de dienst afneemt of van de dienstleverancier, maakt niet uit.

2.1 Verlenging en beëindiging

Afspraken over het verlengen van de looptijd en het beëindigen van de SLA en tevens afspraken over het voortijdig beëindigen van de SLA (exitprocedure/-strategie). De beschrijving van de exitprocedure is te vinden in het Dossier Afspraken en Procedures (DAP).

- **Beëindigingsproces**
Het beëindigingsproces vindt plaats wanneer de gemeente die de dienst afneemt of de dienstleverancier, ervoor kiest om de overeenkomst te ontbinden. Het beëindigingsproces dient een stappenplan te bevatten dat de gemeente in staat stelt om de gemeentelijke gegevens binnen een aangegeven tijdsperiode veilig te stellen voordat de dienstleverancier de gemeentelijke gegevens uit systemen van de dienstleverancier wist (inclusief back-ups, hiervoor geldt mogelijk een ander tijdschema).

2.2 Ontbinding en garanties

Beschrijving van de ontbindende voorwaarden. Maar ook de garanties met betrekking tot de overdracht en vernietiging van gegevens.¹ Bijvoorbeeld het langdurig niet halen van de afgesproken dienstenniveaus.

¹ Zie ook paragraaf 5.1 in dit document.

2.3 Wijzigingsproces van het SLA

Wijzigingen op de in het SLA vastgelegde regelingen, prestaties en rapportages kunnen zowel een incidenteel² als een blijvend (structureel)³ karakter hebben.

Wijzigingen op de SLA worden in het SLA-overleg tussen de beslissingsbevoegde vertegenwoordigers van de gemeente en dienstleverancier (service level manager) afgestemd. Wanneer één van de partijen aanleiding ziet om wijzigingen in het SLA aan te brengen, doet deze partij hiertoe een schriftelijk voorstel aan de andere partij. Vervolgens treden de partijen hierover in overleg. Een tussentijdse aanpassing van het SLA verkrijgt rechtskracht na overeenstemming en ondertekening door de daartoe bevoegde vertegenwoordigers van beide partijen.

3 Dienstverlening, doelen en resultaten

3.1 Dienstverlening

Aard van de uitbestede activiteiten of de ingekochte of geleverde goederen/diensten.

- **Belang van de dienst**
Hier worden specifieke functionaliteiten met betrekking tot de dienst beschreven. Deze specifieke functionaliteiten kunnen van essentieel belang zijn vanuit het perspectief van de gemeente, om gebruik te maken van deze dienst.
- **Identificatie van essentiële componenten**
Hier wordt onder andere de essentiële hard- en software beschreven, maar ook de gemeentelijke (vitale) bedrijfsfuncties die door de dienst ondersteund worden. Deze informatie kan verkregen worden uit een door de gemeente uitgevoerde baselinetoets BIO, diepgaande risicoanalyse of classificatie van informatie verkregen informatie.
- **Vitale bedrijfsfuncties, processen en activiteiten**
Hier worden de vitale gemeentelijke bedrijfsfuncties, processen en activiteiten die door de (ICT-)dienst ondersteund worden beschreven. Hierbij is input van de gemeente uiteraard onontbeerlijk. De gemeente geeft aan de dienstleverancier aan wat voor hen van belang is. Hier wordt ook vermeld of er (bijzondere) persoonsgegevens worden verwerkt.
- **Overige essentiële zaken**
Hier wordt onder andere het (laten) testen van de dienst en de controle op de beveiligingsmaatregelen beschreven. In de SLA dient dan ook vastgelegd te worden welke beveiligingsmaatregelen vereist zijn, dat deze door de dienstleverancier getroffen zijn en worden nageleefd, en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. Ook dient beschreven te zijn hoe die beveiligingsmaatregelen door de dienstleverancier te controleren zijn (bijvoorbeeld audits en penetratietests) en hoe het toezicht is geregeld.
- **Business impact bij verlies van de dienst**
Hier wordt de business impact beschreven bij verlies van de dienst op basis van de resultaten van de uitgevoerde baselinetoets BIO of de handreiking classificatie.

² Bij deze wijzigingen gaat het om een eenmalige, kortstondige afwijking van de inhoud van het SLA, waarbij het SLA als zodanig niet wijzigt.

³ Een wijziging is structureel wanneer ten gevolge van deze wijziging de inhoud van het SLA verandert.

3.2 Gebruiksresultaat

Beschrijving van het gewenste gebruiksresultaat, hier worden de kwalitatieve en kwantitatieve afspraken voor het te realiseren dienstenniveau beschreven.

3.3 Garanties

Beschrijving van de gewenste resultaten in termen van garanties, hier worden de kwalitatieve en kwantitatieve afspraken voor het te realiseren dienstenniveau beschreven.

3.4 Kwaliteit

Hier worden de kwaliteitsnormen, certificeringen et cetera beschreven waaraan de dienstleverancier dient te voldoen.

3.5 Dienstverleningstijden

Hier worden de afspraken met betrekking tot de beschikbaarheid van de dienst vastgelegd.

- **Support (service-/helpdesk)**
Support is de dienstverlening die door dienstleverancier wordt geleverd om incidenten, problemen en vragen van de gemeente af te handelen. Hier worden afspraken met betrekking tot reactie- en oplostijden vastgelegd.
- **Beschikbaarheid van de dienst (uptime)**
Beschikbaarheid is de eigenschap dat de dienst toegankelijk en bruikbaar is op het moment dat de gemeente gebruik wil maken van de dienst. Beschikbaarheid is een belangrijke dienstniveaudoelstelling, want het beschrijft of de dienst daadwerkelijk gebruikt kan worden. Het is belangrijk om de beschikbaarheid van de dienst vast te stellen in combinatie met het belang van beschikbaarheid van de specifieke toepassing voor uw gemeente.
- **Onderhoud**
Hier worden de afspraken met betrekking tot het onderhoud van de dienst vastgelegd. De uitvoering van onderhoudswerkzaamheden kan tot gevolg hebben dat de dienst niet beschikbaar is voor gebruik door de gemeente.
- **Uitzonderingen op beschikbaarheid dienstverlening**
Hier worden de afspraken met betrekking tot de uitzonderingen op de beschikbaarheid van de dienstverlening vastgelegd.
- **Stand-by**
Hier worden de afspraken met betrekking tot de stand-by dienstverlening vastgelegd.

3.6 Ondersteuning

Hier worden de afspraken met betrekking tot het vereiste niveau van ondersteuning (support) vastgelegd. Denk hierbij aan toegang tot systemen door de technisch beheerders van de dienstleverancier/-verlener (beheerders) maar ook aan de gemeentelijke functioneel beheerders en (eind)gebruikers. Tevens dienen afspraken vastgelegd te worden met betrekking tot de beveiliging.

- **Locaties/Ruimtes**
Hier worden de afspraken vastgelegd over vanaf welke locaties/ruimtes ondersteuning kan worden geboden.
- **Soorten gebruikers**
Hier worden de afspraken vastgelegd over welke soorten en het aantal gebruikers dat van de dienst gebruik gaat maken. Groepen/gebruikers die toegang tot de dienst worden toegekend. Maak het gebruik van een bandbreedte mogelijk (minimaal en maximaal aantal gebruikers).
- **Soorten infrastructuur**
Hier worden de afspraken vastgelegd over welke soorten infrastructuur worden ondersteund.

3.7 (verwijderd)

3.8 Wijzigingen

Hier worden afspraken vastgelegd over het indienen van wijzigingsverzoeken door de gemeente. Te denken valt aan de verschillende categorieën wijzigingen die daarbij worden onderkend, evenals criteria voor indeling van deze categorieën en per onderkende wijzigingscategorie de tijd die geldt voor het doorvoeren van de betreffende wijziging, de wijze waarop (belangrijke) wijzigingen binnen de ICT-organisatie impact kunnen hebben voor de gebruikersorganisatie van de gemeente en de wijze waarop over wijzigingen wordt gerapporteerd.

Er dienen ook afspraken met leveranciers worden vastgelegd over:

- dat de leverancier een wijzigingsbeheerproces uitvoert en dat het wijzigingsbeheerproces bij de leverancier en bij de exploitatieorganisatie van de gemeente op elkaar zijn afgestemd, dit geldt in het bijzonder voor de wederzijdse wijzigingskalenders.
- welke categorieën wijzigingen de leverancier autonoom binnen zijn eigen wijzigingsbeheerproces mag doorvoeren, en over welke wijzigingen afstemming met het wijzigingsbeheerproces van de gemeente plaatsvindt.
- welke eisen door de gemeente worden gesteld aan de informatievoorziening over de wijzigingen bij de leverancier.

3.9 Eigendom

Hier wordt beschreven wie de eigenaar is van de gegevens, software en hardware. Hier kunnen ook afspraken met betrekking tot de intellectuele eigendomsrechten worden beschreven.

4 Communicatie tussen gemeente en dienstverlener

Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken dienstenniveaus en het doorvoeren van veranderingen en verbeteringen (bijvoorbeeld vastgelegd in verbeterplannen), is regelmatig overleg op diverse organisatieniveaus noodzakelijk. Er wordt vastgelegd wanneer gestructureerd overleg plaatsvindt, wie er aan dit overleg deelnemen en wie bij beide partijen verantwoordelijk zijn voor de onderlinge relatie. Tevens wordt een overzicht opgenomen van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten. Een nadere concretisering van deze overlegvormen is opgenomen in het Dossier Afspraken en Procedures (DAP). Denk hierbij aan tijdstippen of aanleidingen voor overleg en de betrokken personen bij overleg.

4.1 Verantwoordelijke contactpersoon gemeente

Hier worden de contactgegevens van de verantwoordelijke contactpersoon van de gemeente weergegeven. Dit kan dezelfde persoon zijn als die bij paragraaf 1.2 maar dit kan ook een operationeel / procesmanager zijn.

4.2 Verantwoordelijk (klant) manager leverancier

Hier worden de contactgegevens van de service level manager (zie paragraaf 1.1) of de (klant) manager verantwoordelijk voor het leveren van de dienst van de leverancier weergegeven.

4.3 Dienstrapportages

Hier wordt de inhoud en frequentie (interval) van de rapportage beschreven die door de dienstleverancier worden opgeleverd. Als gemeente dient u zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de afgenomen dienstverlening.

4.4 Uitzonderingen en klachten

Hier worden de procedures voor de behandeling van uitzonderingen en klachten beschreven. Bijvoorbeeld gegevens die moeten worden opgenomen in formele klachten, afgesproken responstijden en de escalatie procedure. De procedure voor de behandeling van uitzonderingen en klachten is te vinden in het Dossier Afspraken en Procedures (DAP).

- **Communicatie in geval van escalaties**
Aangaande de dienstverlening welke buiten de afgesproken dienstenniveaus valt, kan geëscaleerd worden. Bijvoorbeeld: Eindgebruikers dienen altijd eerst de help-/servicedesk (escalatie niveau 1) te bellen. Overige partijen binnen de gemeente kunnen vanuit hun functie contact opnemen met hun counterpart bij de dienstleverancier. De escalatieprocedure is te vinden in het DAP en geeft onder andere aan welke personen betrokken zijn bij escalaties en welke afwijkende clausules gelden ten opzichte van het SLA (bijvoorbeeld met betrekking tot het verlenen van extra ondersteuning door de dienstleverancier).
- **Communicatie in geval van geschillen**
Beschrijving van het feit wanneer onderling overleg plaatsvindt en wat de procedure is bij het optreden van onderlinge conflicten of geschillen qua afhandeling en het betrekken van derde partijen. De geschillenprocedure is te vinden in het DAP en geeft onder andere aan welke personen betrokken zijn bij geschillen (bijvoorbeeld een onafhankelijke derde instantie of persoon) en het feit of een uitspraak van een onafhankelijke geschillencommissie bindend is of niet.

4.5 Tevredenheidsonderzoeken

Hier wordt de procedure beschreven voor het meten van de tevredenheid van de gemeente. Deze meting dient op regelmatige basis plaats te vinden. De procedure voor het meten van de tevredenheid is te vinden in het DAP.

4.6 Servicebeoordelingen

Hier wordt de procedure beschreven voor de herziening van de dienst met de gemeente. Deze meting dient op regelmatige basis plaats te vinden. De procedure voor de herziening van de dienst is te vinden in het DAP.

4.7 Geheimhouding, verantwoordelijkheid en concurrentiebeding

Afspraken met betrekking tot het niet openbaar maken of aan derden beschikbaar stellen van vernomen informatie tijdens het opstellen van de SLA of het functioneren van de dienst(verlening). Denk hierbij ook aan geheimhoudingsplicht met betrekking tot informatie en in het bijzonder geheime of vertrouwelijke informatie. Ook kunnen bepalingen worden opgenomen voor bescherming tegen het overnemen van personeel (concurrentiebeding) of het rechtstreeks onderhandelen van de gemeente (buiten de dienstleverancier om) met derden over de levering van (delen van) diensten.

5 Dienstenniveau eisen / doelen

In dit hoofdstuk worden de kwalitatieve en kwantitatieve dienstenniveaus vastgelegd voor de beschikbaarheids- en betrouwbaarheidsdoelen. Op basis van deze dienstenniveaus vindt monitoring plaats van het geleverde dienstenniveau in relatie met het afgesproken niveau.

5.1 Beschikbaarheidsdoelstellingen

Niet beschikbaarheidsvoorwaarden

Hier worden de voorwaarden beschreven wanneer de dienst als niet beschikbaar wordt beschouwd. Houdt hierbij rekening met de omstandigheid dat de dienst op meerdere locaties wordt aangeboden en het niet beschikbaar zijn van de dienst een gevolg kan zijn van beveiligingsincidenten (bijvoorbeeld DDoS).

- Beschikbaarheidsdoelen

De mate waarin aan de vraag naar een product wordt voldaan (servicegraad). Exacte definitie van hoe de overeengekomen beschikbaarheidsniveaus wordt berekend, op basis van de afgesproken servicetijd en downtime. Dit wordt meestal uitgedrukt in een percentage en kan gemeten worden op verschillende plaatsen in de keten.

Opslagbeheer

Aan de opslag en verwerking van de gebruikersgegevens kunnen door de gemeente aanvullende eisen gesteld worden, bijvoorbeeld ten aanzien van de wijze van bewaren, de bewaartermijn en de wijze van vernietiging. Eventueel kunnen voor bijzonder vertrouwelijke of privacygevoelige gegevens aanvullende afspraken worden gemaakt.

Uitval van infrastructurele voorzieningen

(niet relevant voor de SLA in deze aanbesteding, aangezien de gemeentelijke infrastructuur wordt ingezet).

Onvoldoende scheiding tussen ontwikkel-, test- en productieomgeving

Het aanbrengen van scheiding tussen ontwikkel-, test- en productieomgeving is primair bedoeld om in ieder geval de productieomgeving zo veel mogelijk te isoleren van versturende externe invloeden. Door middel van wijzigingsbeheer en autorisatiebeheer kan deze scheiding verder in stand worden gehouden.

Aantasting van systemen en operationele processen

De beveiliging tegen de aantasting van systemen en operationele processen is erop gericht om de voortgang van de verwerkingsprocessen bij de dienstleverancier te waarborgen. De deskundigheid en kwaliteit van de operationele werkzaamheden zijn van directe invloed op de reputatie van de dienstleverancier. Daarnaast kan door een onafhankelijk deskundige periodiek een oordeel gegeven worden over de algemene kwaliteit van de operationele processen. Hoewel hier sprake is van processen bij de dienstleverancier dienen er in de SLA wel degelijk uitdrukkelijke eisen gesteld te worden aan de minimale beschikbaarheid, de verwerkingssnelheid, de capaciteit en de controleerbaarheid daarvan. Ook is het van groot belang in de SLA aandacht te besteden aan de procedure die gevolgd wordt bij het uitvallen van de productie. De gemeente moet eisen stellen aan de snelheid waarmee de productieomgeving wordt hersteld of tot uitwijk wordt overgegaan. De mate waarin recovery mogelijk is, is deels afhankelijk van de door de gemeente gekozen back-upmethode.

- Betrouwbaarheidsdoelen

Hier worden de betrouwbaarheidsdoelen van de dienst beschreven die door de gemeente worden vereist, meestal gedefinieerd als MTBF (Mean Time Between Failures) of MTBSI (Mean Time Between Service Incidenten)

- Onderhoudbaarheidsdoelen

Hier worden de onderhoudbaarheidsdoelen met betrekking tot de dienst beschreven.

- Niet beschikbaar in verband met onderhoud

Hier worden afspraken beschreven die te maken hebben met onderhoud van het ICT-systeem of-dienst. Denk hierbij aan het aantal toegestane periodes van het niet beschikbaar zijn (downtime) en welke periode vereist is om het niet beschikbaar zijn door te geven aan de gemeente.

- Onderhoudsbeperkingen

Hier worden afspraken beschreven met betrekking tot onderhoudsbeperkingen. Bijvoorbeeld toegestane onderhoudsvensters, wanneer mag er geen onderhoud plaatsvinden en procedures om de geplande onderbrekingen in de dienstverlening aan te kondigen. De procedures om de geplande onderbrekingen in de dienstverlening aan te kondigen zijn te vinden in het DAP.

- **Beschikbaarheidsrapportage**
Hier worden de eisen ten aanzien van de beschikbaarheidsrapportage beschreven. Verwijs naar een bijlage waar een voorbeeld van de rapportage is opgenomen.
- **Definities**
Hier worden de definities gegeven van bijvoorbeeld grote incidenten en spoedwijzigingen.

5.2 Capaciteit / prestatiedoelstellingen en garanties

Capaciteitsbeheer is zodanig geregeld dat de gevraagde dienstenniveaus gehaald en onderhouden kunnen worden tegen aanvaardbare kosten. Houdt hierbij rekening met het feit dat op mogelijke groei van de capaciteitsvraag wordt geanticipeerd en dat de specifieke capaciteitsbehoefte per systeem is vastgelegd.

- **Benodigde capaciteit**
Hier worden de benodigde capaciteitseisen, op basis van de onder- en bovengrens, beschreven voor de betreffende dienst. Denk hierbij aan de eisen met betrekking tot transacties en gebruikers.
De capaciteit geeft de maximale hoeveelheid weer van een bepaalde eigenschap (kenmerk/karakteristiek) van de dienst. Het is vaak een belangrijke waarde voor gemeenten om te weten wanneer ze gebruik gaan maken van een dienst. Relevante eigenschappen kunnen variëren, afhankelijk van de mogelijkheden die door de dienst worden ondersteund (geboden). Het is ook vaak het geval dat meerdere eigenschappen relevant zijn voor een bepaalde dienst met de bijbehorende capaciteit per eigenschap. Afspraken met betrekking tot de capaciteit dienen duidelijk in de SLA te worden beschreven voor een dienst. Merk op dat de capaciteit dienstniveaudoelstellingen verwijzen naar de capaciteiten zoals deze worden gezien door een individuele gemeente en dat reflecteert niet het totaal aan capaciteiten, die door de dienstleverancier wordt ondersteund. Vaak kan de gemeente capaciteitsgrenzen voor hun dienst(en) aanpassen door het aanvragen van een wijziging in hun abonnement.
Er zijn een aantal dienstniveaudoelstellingen, die betrekking hebben op de capaciteit van een dienst. Het gaat hierbij ondermeer om de hoeveelheid opgeslagen data, aantal gebruikers, aantal profielen, aantal transacties, aantal servicedesk calls, aantal (gelijktijdige) hits op de website, verwachte groei van deze dienstniveaudoelstellingen et cetera.
- **Responstijden**
Hier worden de eisen met betrekking tot responstijden van het ICT-systeem en –dienst beschreven. Zoals, op piektijden binnen drie seconden een antwoordbericht, verversen van een webpagina en respons geven binnen vijf seconden.
Responstijd is het tijdsinterval tussen de door de gemeente geïnitieerde gebeurtenis (stimulus) met betrekking tot de dienst en de door de dienstleverancier geïnitieerde gebeurtenis in reactie op die stimulus.

De responstijd dienstniveaudoelstelling kan variëren afhankelijk van het moment waarop de stimulus van de gemeente gemeten wordt. Bijvoorbeeld: de meting kan worden gestart op het moment dat de gemeente de stimulus initieert op hun (mobiele) apparaat, of de meting kan starten op het moment dat het verzoek van de gemeente op het eindpunt van de dienstleverancier arriveert. Het verschil zit hem in de transporttijd over het netwerk (meestal het internet), waarop de dienstleverancier vaak geen invloed kan uitoefenen (niet zijn verantwoordelijkheid). Evenzo kan het punt waarop de reactie van de dienstleverancier gemeten wordt verschillen.

Responstijd is een belangrijk aspect met betrekking tot de gebruikerservaring van een dienst. Afhankelijk van de dienstverlening kan het zijn dat als responstijden groter zijn dan een afgesproken drempelwaarde, deze worden beschouwd als onaanvaardbaar en dat de dienst effectief gezien onbruikbaar is. Een belangrijk aspect hierbij is dat responstijden kunnen variëren afhankelijk van de aard van het verzoek aan de betreffende dienst die wordt afgenomen.

Een factor die moet worden meegenomen is dat veel diensten verschillende bewerkingen ondersteunen en dat waarschijnlijk de responstijd voor deze verschillende bewerkingen verschillen. Het is daarom noodzakelijk om voor de dienstniveaudoelstellingen met betrekking tot de responstijd duidelijk aan te geven om welke bewerkingen het gaat.

- **Schaalbaarheid**
Hier worden de eisen met betrekking tot de schaalbaarheid van het ICT-systeem en –dienst beschreven. Verwachte stijging van het gebruik van de dienst op middellange en lange termijn.
- **Capaciteit- en prestatierapportage**
Hier worden de eisen met betrekking tot de inhoud (capaciteit en prestatie) en frequentie (interval) van de rapportage beschreven die door de dienstleverancier worden opgeleverd. Als gemeente dient u zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de afgenomen dienstverlening.

5.3 Continuïteitseisen

Hier worden de continuïteitseisen (beschikbaarheid) met betrekking tot de dienst beschreven. Bijvoorbeeld in het geval van een calamiteit/ramp.

- **Hersteltermijn minimale dienstverlening**
Hier wordt de termijn beschreven waarbinnen een verstoorde dienst op een (minimaal) vastgesteld dienstverleningsniveau hersteld dient te zijn. Om dit vast te stellen kan het noodzakelijk zijn dat de gemeente een baselinetoets BIO uitvoert.
- **Hersteltermijn normale dienstverlening**
Hier wordt de termijn beschreven waarbinnen een verstoorde dienst op het normale dienstverleningsniveau hersteld dient te zijn. Ook regels opnemen over escalatie (zie ook hoofdstuk 4 Communicatie tussen gemeente en dienstverlener).

5.4 Beveiligingseisen

Het specificeren van meetbare beveiligingsdoelstellingen in SLA's is nuttig om zowel de zekerheid (assurance) als transparantie te verbeteren. Op hetzelfde moment, zorgt het voor een gemeenschappelijke semantiek om de beveiliging van de dienst vanuit twee invalshoeken te beheren, namelijk (i) het beveiligingsniveau dat wordt aangeboden door een dienstleverancier en, (ii) het door een gemeente gevraagd beveiligingsniveau.

De aanpak die hierbij kan worden gebruikt is het analyseren van de beveiligingsmaatregelen van bekende frameworks (Bijvoorbeeld ISO 27001 of de BIO) in een of meer dienstniveaudoelstellingen. Deze dienstniveaudoelstellingen kunnen zowel kwantitatief als kwalitatief zijn. Deze paragraaf behandelt de dienstniveaudoelstellingen die betrekking hebben op de beveiliging van de dienst. Het aantal beschreven dienstniveaudoelstellingen is zeker niet uitputtend, en hou ook rekening met het feit dat wellicht niet alle doelstellingen van toepassing zijn op alle diensten.

De uitbesteding van ICT-processen mag niet leiden tot een aantasting van het bestaande beveiligingsniveau. Uitgaand van het feit dat voorafgaand aan de uitbesteding reeds een passend beveiligingsniveau bestond (BIO), dient dit niveau ook na de uitbesteding te worden voortgezet. Uiteraard is het geen enkel probleem als de uitbesteding tot een andere of een efficiëntere uitvoering van de beveiliging leidt. Beveiliging van systemen, diensten en data zijn hierbij belangrijke aspecten. Deze onderdelen dienen dan ook beschermd te worden tegen zowel interne als externe aanvallen. Zaken waar afspraken over gemaakt dienen te worden zijn:

- Specifieke beveiligingsmaatregelen om de normen en afspraken uit deze SLA te halen. Denk hierbij aan back-up/restore en encryptie/sleutelbeheer.
- Procedure van beveiliging van systemen, diensten en data.
- Maatregelen bij het schenden van beveiligingsprocedures.
- Aanspreekpunt bij beveiligingsincidenten.

- **Betrouwbaarheid van de dienst**

Betrouwbaarheid van de dienst is de eigenschap van een dienst om zijn functies correct en zonder fouten uit te voeren, meestal over een bepaalde tijdsperiode. Deze categorie is meestal gerelateerd aan de beveiligingsmaatregelen: implementeren bedrijfscontinuïteitsbeheer en disaster recovery in standaarden zoals ISO 27002. Voor deze dienstniveaudoelstelling dient rekening gehouden te worden met de toegestane downtime, die onder andere bestaat uit gepland onderhoud.

Opmerking: Betrouwbaarheid omvat ook de mogelijkheid van de dienst om op een adequate manier om te gaan met storingen en het voorkomen van onbeschikbaarheid van de dienst of het verlies van gegevens in het geval van dergelijke storingen.

De doelstelling met betrekking tot betrouwbaarheid moet worden vermeld, zodat de gemeente kan beoordelen of de specifieke dienst voldoet aan hun zakelijke behoeften. Sommige databeheer dienstniveaudoelstellingen kunnen relevant zijn voor betrouwbaarheid (zie ook paragraaf 5.5).

- **Authenticatie & Autorisatie**

(niet relevant voor SLA behorend bij deze aanbesteding)

- **Cryptografie**

(niet relevant voor SLA behorend bij deze aanbesteding)

- **Incidentbeheer en rapportage**

Een (informatiebeveiligings)incident is een enkele of een reeks van ongewenste of onverwachte gebeurtenissen die een aanzienlijke kans hebben om de bedrijfsvoering te compromitteren of verstoren en een bedreiging vormen voor de informatiebeveiliging. Incidentbeheer bestaat uit de processen voor het detecteren, rapporteren, beoordelen, reageren op, omgaan met, en leren van (informatiebeveiligings)incidenten. Hoe informatiebeveiligingsincidenten worden behandeld door een dienstleverancier is van groot belang voor de gemeente, omdat een informatiebeveiligingsincident met betrekking tot de dienst ook een informatiebeveiligingsincident is voor de gemeente.

- **Logging en monitoring**

Logging is het vastleggen van gegevens met betrekking tot de werking en het gebruik van een dienst. Monitoring is het vaststellen van de status van één of meer parameters van een dienst. Logging en monitoring zijn de verantwoordelijkheid van de dienstleverancier.

Registraties (records) in logbestanden zijn belangrijk voor de gemeente bij het analyseren van incidenten, zoals inbreuken op de beveiliging en fouten van de dienst, alsook bij het monitoren van het dagelijkse gebruik van de dienst. Hiervoor is het noodzakelijk om dienstniveaudoelstellingen met betrekking tot logging en monitoring van de dienst en de bijbehorende mogelijkheden volledig te beschrijven.

- **Auditing**

Auditing is een systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van informatie (bewijsmateriaal) over een dienst en een objectieve evaluatie hiervan om te bepalen in welke mate aan de audit criteria wordt voldaan. De noodzakelijke informatie (bewijs) en de audit criteria worden meestal bepaald door het audit- of certificeringschema die wordt gebruikt om de audit uit te voeren. Audits zijn een middel waarmee de dienstleverancier kan aantonen dat een dienst voldoet aan bepaalde criteria die van belang zijn voor de gemeente op basis van onafhankelijk verkregen bewijs. Audits zijn er op gericht om het vertrouwen in de dienst te verhogen.

- **Vulnerability management**

Een kwetsbaarheid is een zwakke plek in een informatiesysteem, beveiligingsprocedures van het systeem, interne controles, of de implementatie die kan worden misbruikt door een bedreiging. Het beheer van kwetsbaarheden betekent dat informatie over technische kwetsbaarheden van informatiesystemen die wordt gebruikt tijdig moet worden verkregen en de blootstelling aan dergelijke kwetsbaarheden dient te worden geëvalueerd en er dienen passende maatregelen genomen te worden om de bijbehorende risico's te beperken. De dienstleverancier is in veel gevallen de eigenaar van de informatiesystemen die zijn geassocieerd met een dienst met als gevolg dat de gemeente afhankelijk is van de dienstleverancier voor het juiste en tijdige beheer van de kwetsbaarheden voor deze informatiesystemen. De dienstniveaudoelstellingen met betrekking tot vulnerability management dienen hierin transparantie voor de gemeente te bieden.

5.5 Databeheer

(niet relevant, behoudens backup/restore)

5.6 Bescherming persoonsgegevens

(uit te werken conform Bijlage 4 Verwerkersovereenkomst)

5.7 Performanceniveau

In de vorige paragrafen zijn de prestatie-eisen welke aan de te leveren diensten gesteld worden beschreven. Om vast te stellen of beide partijen zich aan de overeengekomen afspraken houden, zal de dienstverlening gemeten moeten worden. Elke prestatie-eis dient vertaald te worden in één of meer kritieke/kritische prestatie-indicatoren (KPI). Vervolgens dient voor elke KPI een norm bepaald te worden, die niet overschreden mag worden. De KPI's moeten toetsbaar zijn, dat wil zeggen dat ze aan een aantal eisen moeten voldoen, zoals:

- Validiteit: De prestatie-indicator moet een maat zijn voor de prestatie(eis) waarin inzicht nodig is.
- Geldigheid: De prestatie-indicator moet toepasbaar zijn in de situatie waarin deze toegepast wordt.
- Eenduidigheid: De prestatie-indicator moet slechts op één manier geïnterpreteerd kunnen worden.
- Meetbaarheid: De meetwaarden van de prestatie-indicator moeten kwantitatief te bepalen zijn (er moet een meetschaal voor de indicator zijn).
- Vergelijkbaarheid: De meetwaarden van dezelfde prestatie-indicator in verschillende situaties moeten vergelijkbaar zijn. Uiteindelijk dient er voor iedere prestatie-indicator een norm bepaald te worden, oftewel een waarde die niet overschreden mag worden. Een norm kan een minimum zijn (bijvoorbeeld voor beschikbaarheid), of een maximum (bijvoorbeeld voor vertraging).

6 Taken en verantwoordelijkheden

(zie uitvoeringseisen in Bijlage 1)

7 Kosten

7.1 Kosten dienstverlening

(zie overeenkomst)

7.2 Sancties, bonussen

(zie overeenkomst)

8 Verklarende woordenlijst

Optioneel: In de verklarende woordenlijst wordt een uitleg gegeven van de belangrijkste begrippen die van toepassing zijn binnen de context van alle documenten behorende tot deze SLA.

8.1 Definities

8.2 Afkortingen

9 Bijlagen

Denk aan andere SLA's, rapportageformat, contracten, beveiligingseisen et cetera.

1. Rapportage templates
 - a. Contractmanagement (SLA wijzigingen)
 - b. Opdrachtmanagement (dienstenniveaus op maand basis)
 - c. Service-/helpdesk: openstaande en afgehandelde incidenten, status openstaande incidenten, overschrijdingen.
 - d. Template voor wijzigingsverzoeken
2. Document Afspraken en procedures (DAP)
3. Onderhoudsdocumentatie
4. Beveiligingseisen uit de BIO

5. Woordenlijst/begrippenlijst