Service Level Agreement (SLA)

CIBG - *leverancier*

Service: Onderhoud en beheer van een Customer Care platform

Datum	: 13 maart 2026
Status	: Definitief
Versie	: 1.0

Revisiehistorie

versie	datum	opmerking
0.7	03-11-2025	1e concept t.b.v. aanbesteding
0.8	04-12-2025	Review OO en projectmanager verwerkt.
0.9	04-12-2025	Verwerkingen m.b.t. informatiebeveiliging
1.0	04-12-2025	Definitief

1. Algemeen

1.1. Onderwerp van Overeenkomst

Dit Service Level Agreement (verder als SLA) is het normenkader waarin de functionaliteit en de kwaliteit van de IT dienstverlening ten behoeve van het klantcontactcentrum is vastgelegd en door beide partijen, zoals benoemd in paragraaf 1.2, is overeengekomen.

1.2. Partijen, verklaring en ondertekening

De ondergetekenden (hierna opdrachtgever en opdrachtnemer) verklaren voor akkoord:

Opdrachtgever		**Opdrachtnemer**	
Datum:		Datum:	
Bedrijfsnaam:	CIBG	Bedrijfsnaam:	
Naam:		Naam:	
Functie:	Service Level Manager	Functie:	
Handtekening:		Handtekening:	

Overwegen dat:

- Partijen in dit SLA hun rechten en plichten wensen vast te leggen;
- Partijen zich verbinden om de toegewezen taken en verantwoordelijkheden, zoals die in dit SLA beschreven worden, te zullen vervullen conform de beschreven eisen.
- De nadruk ligt hierbij op de resultaatverplichting, hetgeen inhoudt dat de opdrachtnemer zich verplicht om het afgesproken resultaat te leveren, zoals nader omschreven in dit document.

1.3. Aanvang en looptijd

Dit SLA is onlosmakelijk verbonden aan de Overeenkomst met kenmerk *xxxxx* d.d. *dd-maand-jaar* en heeft een doorlooptijd die gelijk is aan deze Overeenkomst.

1.4. Doel van het SLA

Het doel van het SLA is het definiëren van de verplichtingen en verantwoordelijkheden van opdrachtgever en opdrachtnemer met betrekking tot de onderhavige diensten en servicelevels. Uitgangspunt hierbij is dat optimaal invulling wordt gegeven aan de inzet, de continuïteit en de toekomstige invulling van de behoeften van de opdrachtgever, binnen afgesproken kosten- en kwaliteitskaders. De inhoud van het SLA is de gezamenlijke verantwoordelijkheid van opdrachtnemer en opdrachtgever.

1.5. Beschrijving service

Opdrachtnemer verzorgt:

1) De levering van een geïntegreerde oplossing voor een multimediale Customer Care platform met multimediale klantingangen.
2) Ondersteuning, beheer, onderhoud en de doorontwikkeling van een oplossing, waarbij alle componenten goed op elkaar is afgestemd.

Onderdeel van de standaard dienstverlening door opdrachtnemer zijn alle activiteiten m.b.t. kwaliteitsborging (zoals structurele en incidentele overleggen en advisering).

1.6. Achtergrond van de service

Het klantcontactcentrum (KCC) is het centrale klantenloket van de opdrachtgever. Hier worden de klanten (burgers, professionals en organisaties) geïnformeerd. De klantvragen komen via diverse kanalen binnen en worden ook via diverse kanalen beantwoord (zoals telefoon, mail, balie, webcare, brief). Alle klantvragen en klachten over CIBG-producten worden hier aangenomen, vastgelegd en afgehandeld.

1.7. Controle en beheersing

Opdrachtnemer beheert de overeengekomen serviceverlening proactief. Dit wil zeggen dat de kwaliteit van de serviceverlening door opdrachtnemer continue wordt vergeleken met de aspecten zoals benoemd in dit SLA. Afwijkingen t.a.v. de gespecificeerde serviceverlening worden gesignaleerd en gerapporteerd. Opdrachtnemer zal bij normoverschrijding en verwachte normoverschrijding een voorstel doen om de serviceverlening zo spoedig mogelijk (weer) in overeenstemming te brengen met de specificaties zoals vastgelegd.

1.8. Service-, ondersteunings- en onderhoudswindow

servicewindow
Servicewindow 24x7

Het servicewindow is de tijdspanne waarbinnen de overeengekomen service wordt verleend.

ondersteuningsvenster
Servicedesk van 08.00 – 18.00 uur op werkdagen

Het ondersteuningsvenster is het tijdsslot waarin de Servicedesk van de opdrachtnemer bereikbaar is voor de klant om de serviceprocessen Incident management en Change management en service verzoeken te melden. Dit is het tijdsslot waarbinnen de servicenormen van toepassing zijn.
De Servicedesk is Nederlandstalig en is minimaal telefonisch en per e-mail bereikbaar voor het bieden van ondersteuning aan opdrachtgever ten behoeve van de dienstverlening.

onderhoudswindow
Onderhoud wordt gepleegd buiten het ondersteuningsvenster om.

Het onderhoudswindow is de tijdspanne waarbinnen een service niet of deels beschikbaar is, overeenkomstig de gemaakte afspraken.

Opdrachtnemer verplicht zich om minimaal 10 werkdagen voor aanvang van het gepland onderhoud de opdrachtgever te informeren.

1.9. Werkafspraken en procedures

De operationele uitwerking van dit SLA worden in een Dossier Afspraken en Procedures (DAP) vastgelegd. Voorgestelde wijzigingen in de versies van het DAP zullen worden vastgesteld in het Service overleg tussen opdrachtgever en opdrachtnemer.

In onderling overleg tussen partijen kan, in incidentele gevallen, worden afgeweken van het gestelde in dit SLA. De afwijkende afspraak wordt in het verslag van het Service of Tactisch overleg vastgelegd.

1.10. Documentbeheer

Dit document is eigendom van en wordt beheerd door opdrachtgever. Na het ondertekenen van deze Service Level Agreement kan deze met uitzondering van de bijlagen alleen nog maar worden

aangepast door middel van een Request for Change die door beide partijen schriftelijk moet worden goedgekeurd. Aanpassingen aan de procedures uit de bijlagen kunnen met wederzijdse afstemming worden doorgevoerd zonder dat het SLA opnieuw ondertekend hoeft te worden.

2. Normen en service credits

In deze paragraaf zijn de SLA-parameters en normen opgenomen, waaraan de dienstverlening van opdrachtnemer dient te voldoen. Een norm is de waarde waarbinnen de dienstverlening geleverd dient te worden.
De SLA-parameters en normen zijn per onderwerp opgenomen in aparte tabellen.

Indien de normen 2x achtereenvolgens worden overgeschreden, dan stelt opdrachtnemer binnen 10 werkdagen een Service Improvement Plan (SIP) op teneinde betreffende overschrijdingen in het vervolg te voorkomen.

Bij het achterwege blijven van de resultaten uit het SIP dient het tier 1 management van opdrachtnemer zich te komen verantwoorden bij de Afdelingshoofd Applicatie- en Servicemanagement van opdrachtgever.

Elke SLA-parametertabel kent de volgende indeling:

- Norm op maandbasis (de waarden waarbinnen de dienstverlening geleverd dient te worden);
- Service Credits (in deze kolom staat, waar van toepassing, de service credit aangegeven, die aan opdrachtnemer kan worden opgelegd, indien de norm in de betreffende regel wordt overschreden).

Het toepassen service credits
Vooropgesteld wordt dat de opdrachtgever streeft naar een partnership met opdrachtnemer en in beginsel niet voornemens is om service credits toe te passen.

De toepassing van opgelegde service credits komt niet in plaats van een schadevergoedingsvordering (op basis van 6:92 lid 2 Burgerlijk Wetboek).

Indien meerdere normen tegelijk worden overschreden, zijn er meerdere service credits tegelijkertijd van toepassing. De toepassing van de service credits geschiedt maandelijks in overleg met opdrachtnemer. Het totaal aan service credits is echter gemaximeerd en zal nooit meer dan 5% van de jaarlijkse kosten voor deze dienstverlening aan opdrachtgever overschrijden.

Iedere kwartaal vindt er een tactisch service overleg plaats waarin de eventuele overschrijding van de norm(en) en de daarmee gemoeide service credits worden vastgesteld.

Halfjaarlijks worden de normen, en specifiek degene niet behaald in de afgelopen 6 maanden, in het tactisch overleg besproken en eventueel bekrachtigd.
Afhankelijk van:

- de uitkomst van het tactisch service overleg;
- de aard (ad hoc versus structureel);
- impact op opdrachtgever;
- Service Improvement Plans inclusief hersteltermijnen en effort van opdrachtnemer,

worden de bij elkaar opgetelde service credits van de afgelopen 6 maanden daadwerkelijk opgelegd (geheel of gedeeltelijk) en moeten deze in mindering gebracht worden op de eerstvolgende factu(u)r(en). Hierover zal opdrachtnemer binnen 2 weken na het tactisch service overleg schriftelijk worden geïnformeerd.

Opdrachtnemer dient zelf in de Service Level rapportages over de afgelopen 6 maanden de overschrijding van de norm(en) en daarmee gemoeide service credits in een apart hoofdstuk op te nemen.
Mocht er binnen een redelijke termijn geen verbetering in de dienstverlening te zien zijn, dan wordt verder geëscaleerd. Met de hoogste escalatie dient het hoogst verantwoordelijk management van opdrachtnemer zich te komen verantwoorden bij het afdelingshoofd van de afdeling Applicatie- en servicemanagement van opdrachtgever.

Service credits	
Code	**Omschrijving service credits**
SC-1	Een cumulatieve korting van 0,5% op de maandelijkse totaal factuur voor iedere werkdag waarin de norm is overschreden.
SC-2	Een kortingspercentage "X" op de maandelijkse totaal factuur over de kalendermaand waarin de norm is overschreden. Het kortingspercentage "X" is in de betreffende tabellen aangegeven.

2.1. Beschikbaarheid

Opdrachtnemer monitort actief de beschikbaarheid van de systemen en garandeert een minimale beschikbaarheid van 99,8% gedurende kantoortijden. De beschikbaarheid van de dienstverlening wordt maandelijks gemeten t.o.v. de totale tijd in het servicewindow.

Beschikbaarheidspercentages				
Categorie	**Norm**	**Service credit bij overschrijden van de norm**		
		SC-2: 2%	**SC-2: 4%**	**SC-2: 6%**
Productie omgeving	99,8%	99,7% - 99,3%	99,2% - 98,8%	≤98,7%
Acceptatietest omgeving	98%	n.v.t	n.v.t	n.v.t
Test omgeving	98%	n.v.t	n.v.t	n.v.t

2.2. Calamiteit en hersteltijd

Calamiteit	Duur (norm)	Credits
Informeren opdrachtgever over calamiteit	Maximaal 1 uur	SC-1

Recovery (hersteltijd)	Duur (norm)	Credits
Restore Point Objective (RPO)	4 uur	SC-1
Restore Time Objective (RTO)	2 uur	SC-1

Retentie	Duur (norm)	Credits
Dagelijkse backup	8 dagen	N.V.T.
Wekelijkse backup	1 maand	N.V.T.

2.3. Incidentafhandeling

Prioriteit	Reactie tijd (norm)	Oplostijd 100% (norm)	Terugkoppeltijd (norm)	Credits
1 Hoog	<15 minuten	4 uur	Elke 1 uur	SC-1
2 Middel	< 2 uur	24 kantooruren	Op verzoek van opdrachtgever	SC-1
3 Laag	<4 kantooruren	In overleg	Op verzoek van opdrachtgever	SC-1

Urgentie
Urgentie is de gedefinieerde snelheid waarmee een probleem moet worden opgelost om de impact te beperken.

Urgentie	Beschrijving
Hoog	Geen uitstel mogelijk, directe actie nodig
Gemiddeld	Direct actie vereist volgens standaard procedure
Laag	Geen directe noodzaak tot handelen

Impact
Impact heeft betrekking op de potentiële nadelige gevolgen die een niet-opgeloste verstoring heeft op de mogelijkheid van het bedrijf om activiteiten effectief te kunnen voortzetten of om service te kunnen blijven leveren.

Impact	Beschrijving
Hoog	Uitval van dienstverlening/kosten/imagoschade
Gemiddeld	Gedeeltelijk onderbroken/verminderde prestatie
Laag	Beperkte gevolgen van de klant

Aanduiding van prioriteiten zoals gedefinieerd binnen dit SLA
De prioriteit wordt bepaald door opdrachtgever op basis van urgentie en impact en door opdrachtnemer vastgelegd in het registratiesysteem.

Urgentie	Impact		
	Hoog	**Gemiddeld**	**Laag**
Hoog	1	1	2
Gemiddeld	1	2	3
Laag	2	3	3

2.4. Root cause analysis

Bij een prioriteit 1 Hoog incident levert de opdrachtnemer standaard en op eigen initiatief uiterlijk 5 werkdagen na de oplosdatum van het incident een Root Cause Analysis (RCA) op.
RCA's voor incidenten met een lagere prioriteit dan P1 Hoog, worden op verzoek van opdrachtgever opgesteld.

De RCA beschrijft minimaal onderstaande onderdelen:

- Omschrijving van het incident;
- Chronologisch overzicht van gebeurtenissen;
- Oorzaken die tot het incident hebben geleid;
- Toegepaste voorlopige of structurele oplossing;
- Noodzakelijke wijzigingen om te komen tot een structurele oplossing;
- Aanvullende maatregelen om het incident in de toekomst te voorkomen;
- Conclusie en aanbevelingen.

prioriteit	Opleveren RCA (norm)
1 Hoog	Maximaal 8 werkdagen na de oplosdatum incident en voldoet aan kwaliteitseisen
2 Middel of lager	Maximaal 8 werkdagen na aanvraagdatum RCA en voldoet aan kwaliteitseisen

2.5. Change- en opdrachtafhandeling

1) Bij een verzoek tot wijziging zal waar nodig, een overleg tussen opdrachtnemer en opdrachtgever worden gepland. In dit overleg wordt bepaald wat de aanpassing is, en wat de acties zijn die beide partijen op zich nemen om de verandering door te voeren.
2) Indien er wijzigingen in de software worden doorgevoerd, hetzij om bugs op te lossen, hetzij voor verbeterde of nieuwe functionaliteit, zal opdrachtnemer hiervan de release notes opleveren en beschikbaar zijn voor inhoudelijke vragen.
3) Opdrachtnemer zal opdrachtgever voorzien van alle noodzakelijke bijgewerkte documentatie. Bijvoorbeeld:
   - Eindgebruikers-documentatie;
   - Installatie- en configuratie documentatie;
   - Waar nodig kunnen wijzigingen door opdrachtnemer leiden tot veranderingen in de architectuur of systemen in beheer bij opdrachtgever. Opdrachtnemer biedt dan ondersteuning bij dergelijke wijzigingen alsook bij het aanpassen van beheerdocumenten.
4) Opdrachtnemer zal in het kader van het beheer en onderhoud van afhankelijke beheercomponenten beschikbaar zijn voor ondersteuning.

Start opdrachtafhandeling		
Soort	**Aanvangmoment (norm)**	**Credits**
Requests for information en standaard opdrachten	Maximaal 2 werkdagen tenzij in samenspraak een ander aanvangsmoment is overeengekomen	SC-1
Niet standaard opdrachten	Maximaal 10 werkdagen na goedkeuring offerte tenzij in samenspraak een ander aanvangsmoment is overeengekomen	SC-1
Urgente opdrachten	Maximaal 2 werkdagen tenzij in samenspraak een ander aanvangsmoment is overeengekomen	SC-1

Oplevering		
Soort opdracht	**Oplevermoment (norm)**	**Credits**
Offerte	100% binnen 10 werkdagen, tenzij in samenspraak een ander moment is overeengekomen	SC-1
Service requests en requests for information	100% binnen met opdrachtgever afgestemde datum en/of tijd	SC-1
Standaard changes	100% binnen met opdrachtgever afgestemde datum en/of tijd	SC-1
Niet standaard changes	100% binnen met opdrachtgever afgestemde datum en/of tijd	SC-1
Urgente changes	100% binnen met opdrachtgever afgestemde datum en/of tijd	SC-1

2.6. Problemafhandeling

problemafhandeling				
categorie	**prioriteit**	**max. reactie-tijd (norm)**	**start werken aan oplossing**	**oplostijd (norm)**
Problem dat de productie of acceptatie in ernstige mate verstoort	Hoog	4 uren	Direct	1 maand
Problem verstoort de productie of acceptatie, maar hoeft	Middel	8 uren	In overleg	3 maanden

problemafhandeling				
categorie	**prioriteit**	**max. reactie-tijd (norm)**	**start werken aan oplossing**	**oplostijd (norm)**
niet direct te worden opgelost				
Problem verstoort niet de productie of acceptatie	Laag	8 uren	In overleg	6 maanden

2.7. Klanttevredenheid

Ieder kwartaal zal er intern een tevredenheidsonderzoek plaatsvinden onder de directe afnemers (minimaal 5) van de geleverde dienst. Het tevredenheidsonderzoek richt zich op de onderstaande kwalitatieve tevredenheidscriteria (voldoende/onvoldoende):

- algehele kwaliteit van de geleverde producten en diensten;
- samenwerking tussen opdrachtgever en opdrachtnemer;
- klantgerichtheid;
- op tijd leveren;
- responsiviteit;
- nakomen van afspraken (SLA, DAP, etc.) met uitzondering van de normen in de SLA.

De uitkomsten van het onderzoek zullen gedeeld worden met de opdrachtnemer. Opdrachtnemer zal in de gelegenheid worden gesteld om met een verbeterplan (SIP) te komen en deze uit te voeren, zodat het tevredenheidsniveau op het gewenste niveau wordt gebracht.

Indien in het eerste jaar na afsluiten van de eerste Overeenkomst, ondanks de verbeterplannen en gesprekken, het gewenste tevredenheidsniveau toch uitblijft zal de opdrachtgever ook naar aanleiding van de resultaten van het klanttevredenheidsonderzoek kunnen besluiten om service credits in het jaar daarop toe te gaan passen.

Deze afweging zal aan de hand van twee criteria worden gemaakt;

- de resultaten van de 4 intern gedane tevredenheidsonderzoeken en
- het SLA-scoreverloop van het afgelopen jaar.

Hierover zal opdrachtnemer per e-mail beargumenteerd worden geïnformeerd waarna deze binnen een overeengekomen termijn de mogelijkheid krijgt om te reageren.

Aan het einde van ieder kalenderjaar zal een dergelijk onderzoek en SLA- beoordeling plaatsvinden om te bezien of service credits het kalenderjaar daarop van toepassing zullen zijn.

Klanttevredenheid	Credits
Rapportcijfer 7	N.v.t.

2.8. Maandelijkse Service Level Rapportage (SLR)

Opdrachtnemer zal op drie maandelijkse basis rapporteren over de in dit hoofdstuk weergegeven prestatie-indicatoren.
Opdrachtnemer zal op verzoek van opdrachtgever de rapportages binnen 10 werkdagen van het nieuwe kwartaal toelichten, advies uitbrengen, als klankbord dienen voor opdrachtgever en verbetervoorstellen doen.

Minimaal wordt gerapporteerd over de volgende onderdelen en de voortgang ervan, begeleid met een Management samenvatting:

- Beschikbaarheid;

- Overzicht lopende en afgesloten opdrachten;
- Behaalde resultaten buiten of binnen de afgesproken tijd;
- Incident management;
- Problem management;
- RCA's;
- Change management;
- Klachten en escalaties;
- Service credits;
- Aantal licenties en overzichten gebruikersaccounts (indien van toepassing);
- Backup status (overzicht succesvol/niet succesvol) en verbeteracties;
- Security rapportage met onder andere:
    - Voortgang pentest bevindingen;
    - Voortgang overige security incidenten en aanbevelingen en hotfixes.
- Overzicht en voortgang van uitgevoerde en openstaande beheeractiviteiten, welke minimaal bestaat uit: de status van lopende werkzaamheden, de bestede uren, de nog verwachtte bestede uren en doorlooptijd. Opdrachtgever kan ook tussentijdse voortgangsrapportages opvragen naar gelang de behoefte.
- Ontwikkelingen en nieuwe wensen.

Soort	Indienen uiterlijk op (norm)	Credits
Service Level rapportage (inclusief security rapportage)	10e werkdag van elke kwartaal na het verstrijken van de verslagperiode	SC-1

Rapportages worden opgestuurd naar de e-mail adressen zoals aangegeven in het DAP.
Indien de norm van 10 werkdagen 2x achtereenvolgens is overgeschreden stelt opdrachtnemer binnen een week een Service Improvement Plan (SIP) op teneinde dit soort vertragingen In het vervolg te voorkomen.

3. Klachten en escalaties

Klachten worden aangemeld bij de Service Desk van opdrachtnemer en worden volgens een door de opdrachtnemer opgestelde standaard klachtenprocedure geregistreerd en afgehandeld. De klacht is afgehandeld indien de aanmelder vanuit opdrachtgever een formeel en bevredigend antwoord heeft gekregen op de klacht.

In bepaalde situaties is het wellicht noodzakelijk om langs de hiërarchische lijn in te grijpen teneinde de dienstverlening vlot te trekken dan wel te bespoedigen. De escalatielijnen hiervoor zullen worden opgenomen in een DAP.

4. Leveranciersmanagement

soort	toelichting
Management van onderaannemers	Opdrachtnemer voert het leveranciersmanagement uit over onderaannemers die Opdrachtnemer zelf inschakelt om delen van de geleverde service te realiseren (zoals ten behoeve van het leveren van support op server hardware). Dit heeft impact op de in dit SLA gestelde normen.
Management van derde leveranciers	Opdrachtnemer voert op verzoek van opdrachtgever operationele regievoering uit over derde partijen die door opdrachtgever zijn aangesteld als leverancier van service en waar opdrachtnemer geen contract mee heeft. Dit heeft geen impact op de in dit SLA gestelde normen.

5. Serviceafspraken

Ticket registratie
Opdrachtgever voert haar ticket administratie in Topdesk, van waaruit e-mail berichten m.b.t. incidenten, changes en serviceverzoeken worden verstuurd naar opdrachtnemer.
Opdrachtnemer zorgt voor registratie van deze klantvragen en incidenten in diens eigen service management systeem en geeft opvolging aan de vragen.
Voor de eenduidigheid worden elkaars registratie kenmerk uitgewisseld en vastgelegd.
Medewerkers van opdrachtgever kunnen eveneens via het service portaal inzicht krijgen in de voorgang van tickets.

6. Informatiebeveiliging

Dit hoofdstuk beschrijft de informatiebeveiligingsafspraken en de daaraan gerelateerde criteria tussen opdrachtgever en opdrachtnemer in relatie tot de door opdrachtgever afgenomen diensten.

Het uitgangspunt van opdrachtgever is dat informatiebeveiliging een onderwerp is alleen realiseerbaar is wanneer dit in de hele keten is belegd. Vandaar dat opdrachtgever stuurt op een samenwerking met alle partijen om de gewenste situatie tot stand te brengen. Meer inhoudelijke afspraken omtrent informatiebeveiliging zal eventueel in een DAP worden vastgelegd.

6.1 Gezamenlijke verantwoordelijkheid

Informatiebeveiliging is voor opdrachtgever een van de pijlers voor het leveren van betrouwbare diensten en producten. Er is daarbij sprake van een gezamenlijke verantwoordelijkheid voor opdrachtgever en haar opdrachtnemers. De definitie van wat veilig is en hoe de gewenste veiligheid op werkbare en kostenefficiënte wijze tot stand moet komen zal door betrokken partijen in onderlinge afstemming moeten worden bepaald. Informatieveiligheid kan alleen verwezenlijkt worden wanneer een ieder zijn eigen verantwoordelijkheden kent. Daarnaast zet opdrachtgever bij samenwerking in op wederzijdse ondersteuning bij het invullen van de respectievelijke eigen verantwoordelijkheden. Opdrachtgever verwacht van haar opdrachtnemers daarom dat zij niet alleen acteren wanneer hen iets gevraagd wordt, maar ook dat zij de rol van goed huisvaderschap vervullen en adequaat acteren bij dreigende beveiligingsincidenten, falende beveiligingsmaatregelen en proactief inspelen op ontwikkelingen in het dreigingsveld.

6.2 Gebruik van standaarden en normenkaders

Als onderdeel van de Rijksoverheid past opdrachtgever de Rijksbrede kaders toe en maakt daarbij zoveel mogelijk gebruik van algemeen geaccepteerde standaarden en best practices op het vlak van informatiebeveiliging. Het verplichte gebruik van deze standaarden geldt niet alleen voor opdrachtgever, maar ook voor haar opdrachtnemers. Deze voor de Rijksoverheid voorgeschreven aanpak draagt bij aan een eenduidige, uniforme benadering van informatiebeveiliging.
Daar waar specifieke afspraken of beleid vanuit de opdrachtgever rondom informatiebeveiligingsonderwerpen ontbreken, worden de algemeen erkende beveiligingsstandaarden en best practices als kaderstellend beschouwd, zowel voor opdrachtgever als haar dienstenleveranciers.

6.3 Audits en penetratietesten

1) Opdrachtnemer laat minimaal jaarlijks een penetratietest uitvoeren door een onafhankelijke derde partij en in ieder geval voor de live gang met de productie omgeving. Opdrachtgever wordt op de hoogte gesteld van de resultaten en eventuele bevindingen die van invloed zijn op de oplossing, de werking en veiligheid.

2) Opdrachtgever kan in overleg met opdrachtnemer een additionele penetratietest of audit willen laten uitvoeren. Opdrachtnemer verleent medewerking aan de uitvoering van penetratietest en andere audits daar waar van toepassing en door een partij naar de keuze van opdrachtgever. Opdrachtgever bepaalt de scope en methode.
De bevindingen van de penetratietesten zullen aan de opdrachtnemer beschikbaar worden gesteld.
In een dergelijk geval zal opdrachtgever voor de uitvoering van de penetratietest opdrachtnemer vooraf informeren over:
    a. De periode waarin de penetratietest zal plaatsvinden, waarbij de penetratietest gestart zal worden na instemming van Opdrachtnemer. Buiten de aangekondigde periode zullen geen onderzoeken plaatsvinden;
    b. De IP-nummers die gebruikt zullen worden voor het uitvoeren van de penetratietest;
    c. Een contactpersoon waarmee Opdrachtnemer altijd en onmiddellijk contact kan opnemen, ingeval van calamiteiten met betrekking tot de penetratietest en gedurende de periode waarbinnen de penetratietest uitgevoerd wordt.

3) Opdrachtgever behoudt zich het recht om minimaal jaarlijks een audit op de applicatie, systemen en infrastructuur te doen of te laten uitvoeren.

4) Opdrachtgever dient in staat te worden gesteld om gedurende of na informatiebeveiligingsincidenten controles uit te oefenen.

5) Opdrachtnemer zal alle medewerking verlenen, indien toezichthouders van opdrachtgever onderzoek zouden willen doen naar het handelen van opdrachtnemer en/of het functioneren van de oplossing.

6) Bevindingen vanuit audits dienen onmiddellijk of binnen een met opdrachtgever afgestemde termijn te worden verholpen. Critical vulnerabilities dienen binnen 5 werkdagen opgelost te worden. De prioriteit wordt bepaald op basis van de prioriteiten matrix uit paragraaf 2.3 Incidentafhandeling. De hiermee samenhangende kosten zijn voor rekening van Opdrachtnemer.

7) Opdrachtnemer dient ten aanzien van de oplossing en de diensten die worden geleverd periodiek minimaal jaarlijks een Third Party Memorandum (TPM) auditverklaring te overleggen, opgesteld door een, door opdrachtgever goed te keuren, onafhankelijke auditor, bij voorkeur een ISO 27001 certificaat met een Verklaring van Toepasselijkheid c.q. Statement of Applicability (SOA) als bijlage.

6.4 Eisen

De informatiebeveiligingseisen staan vermeld in het programma van eisen en wensen (PvE) en dienen als zodanig te worden ingericht en uitgevoerd. De invulling van de eisen worden door Opdrachtnemer nader uitgewerkt en in het DAP vastgelegd.

1) Opdrachtnemer moet minimaal de beveiligingsmaatregelen implementeren en onderhouden die voldoen aan de vigerende Baseline Informatiebeveiliging Overheid (BIO).

2) Beveiligingsnormen en maatregelen mogen in de visie van opdrachtgever geen reden zijn om gevraagde functionaliteit zonder meer af te wijzen. Opdrachtgever verwacht van haar leveranciers dat zij in een dergelijke situatie met een (technisch) oplossingsvoorstel komt. Opdrachtnemer zal aanvullende beveiligingsmaatregelen treffen op verzoek van opdrachtgever of op eigen initiatief. Dit gebeurt:
    a. in verband met wijzigingen in wet- en regelgeving;

b. wanneer het NCSC een (dwingend) beveiligingsadvies afgeeft. In dit geval treden de partijen in overleg over het overnemen van het advies en het al dan niet doorvoeren van benodigde wijzigen c.q. maatregelen. De hiermee samenhangende kosten komen voor rekening van opdrachtnemer;
c. met het oog op het beveiligen van persoonsgegevens.

3) Opdrachtnemer voldoet aan het 'pas toe of leg uit'-beleid van de aanbevolen en verplichte standaarden van het forum standaardisatie: https://www.forumstandaardisatie.nl/open-standaarden.

4) Het 'security by design' principe dient toegepast te worden, waarbij minimaal de volgende standaarden/best practices dienen te worden toegepast:
   a. CIP-overheid Grip op Secure Software Development (SSD)
   b. NCSC eisen voor webapplicaties.
      De principes 'privacy by design' en 'privacy by default' dienen zoveel mogelijk in de oplossing te zijn verankerd op basis van de context en het doel van de verwerking, en de waarschijnlijkheid en ernst van de risico'.

5) Opdrachtnemer dient binnen de oplossing gebeurtenissen te registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

6) De oplossing is compliant met de relevante wet- en regelgeving op het gebied van privacy- en gegevensbescherming, waaronder, maar niet beperkt tot, de Algemene verordening gegevensbescherming en de Uitvoeringswet algemene verordening gegevensbescherming.

7) Opdrachtnemer werkt mee aan het opstellen van een DPIA (Data Protection Impact Assessment) en Risicoanalyse (van Informatiebeveiliging) en hiervoor de benodigde input aan te leveren. Indien nodig is opdrachtnemer bereid mee te werken aan het herzien van de DPIA.

8) Opdrachtgever heeft het eigenaarschap over bijbehorende data en heeft te allen tijde toegang tot de bron data en/of databases en datamodellen. Opdrachtgever behoudt de mogelijkheid om data te exporteren dan wel importeren via eigen ETL tools en zal niet worden gehinderd door autorisaties en/of encryptie van de data.

9) Opdrachtnemer levert controleerbaar bewijs, in de vorm van een formele audit-verklaring, m.b.t. de opzet, bestaan en werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van het geheel van de te leveren dienst(en).

6.5 Verantwoordelijkheden

Risicobeoordeling en risicobehandeling

risicobeoordeling en risico behandelingen – afspraken		
Rollen/Verantwoordelijkheden (P=Primair, O= Ondersteunend)	Opdrachtnemer	Opdrachtgever
Controleren van de opzet, bestaan en werking van de aan de dienstverlening gerelateerde beveiligingsmaatregelen.	P	

Beveiliging van Personeel

Risicobeoordeling en risico behandelingen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	Opdrachtnemer	Opdrachtgever
Alle werkzame medewerkers ten behoeve van de aan opdrachtgever te leveren diensten worden op de hoogte gehouden van het beveiligingsbeleid van opdrachtgever voor zover dit noodzakelijk is voor de werkzaamheden.	P	O
Alle werkzame medewerkers ten behoeve van de aan opdrachtgever te leveren diensten dienen te beschikken over de juiste informatiebeveiligingskennis en -kunde die noodzakelijk is voor de werkzaamheden.	P	
Bij ondersteuning van en instructies aan medewerkers van opdrachtgever wordt gewezen op de mogelijke risico's en hoe vanuit beveiligingsoptiek op passende wijze om wordt gegaan met diensten en middelen.	P	O
Van alle werkzame medewerkers ten behoeve van de aan opdrachtgever te leveren diensten met mogelijke toegang tot gegevens van opdrachtgever heeft opdrachtnemer een geheimhoudingsverklaring.	P	

Organisatie van informatiebeveiliging

organisatie van informatiebeveiliging - afspraken		
Rollen/Verantwoordelijkheden (P=Primair, O= Ondersteunend)	Opdrachtnemer	Opdrachtgever
Een deskundig *´single point of contact'* leveren voor Beveiligingsbeheer	P	P

organisatie van informatiebeveiliging - criteria	
Doorgeven wijzigingen contactpersonen	14 dagen voorafgaand wijziging

Beheer van informatiebeveiligingsincidenten

beheer van informatiebeveiligingsincidenten - afspraken		
Rollen/Verantwoordelijkheden (P=Primair, O= Ondersteunend)	Opdrachtnemer	Opdrachtgever
Er is een generiek draaiboek voor incidenten en calamiteiten binnen de dienstverlening.	P	
Er zijn draaiboeken beschikbaar voor een aantal specifieke incidenten binnen de dienstverlening.	P	
Gesignaleerde (dreigende) kritieke incidenten (major incidents) worden aan het informatiebeveiligingsaanspreekpunt van beide partijen gemeld.	P	P

beheer van informatiebeveiligingsincidenten - afspraken		
Na ieder prioriteit 1 incident wordt een analyse uitgevoerd van het incident en waar nodig een verbetervoorstel (actieplan) gedaan conform security incidenten proces.	P	
Bij incidenten waarbij mogelijk sprake is van aantasting van integriteit of vertrouwelijkheid van gegevens van opdrachtgever zal opdrachtnemer op aanvraag medewerking verlenen door gegevens uit de systemen van opdrachtgever ter beschikking te stellen, rekening houdend met wettelijke eisen.	O	P

beheer van informatiebeveiligingsincidenten - criteria	
Melding (dreigend) incident	Volgens P1 procedure (Incidentmanagement)
Verbetervoorstel n.a.v. (P1) Incident	Binnen 1 maand

Naleving

naleving - afspraken		
Rollen/Verantwoordelijkheden (P=Primair, O= Ondersteunend)	Opdrachtnemer	Opdrachtgever
Opdrachtnemer draagt er zorg voor dat de door haar aan opdrachtgever geleverde diensten aantoonbaar voldoen aan de met opdrachtgever gemaakte afspraken.	P	
Bij beëindiging of wijziging van de dienstverlening worden op verzoek van opdrachtgever alle gegevens waarvoor opdrachtgever verantwoordelijk is en/of waarvan opdrachtgever eigenaar is tijdig en in bruikbaar formaat overgedragen aan opdrachtgever.	P	
Er worden regulier pentesten op de geleverde diensten en onderliggende voorzieningen uitgevoerd om de technische beveiligingsmaatregelen te controleren.	P	O

naleving - criteria	
Overdracht gegevens bij beëindiging dienst	Conform verwerkersovereenkomst en exitplan dat door de opdrachtnemer is opgesteld.

6.6 Security Overleg

Op verzoek van opdrachtgever vindt er security overleg plaats tussen de verantwoordelijke beveiligingsfunctionarissen van opdrachtgever en opdrachtnemer en/of onderopdrachtnemer. Doel van dit overleg is om security gerelateerde onderwerpen te bespreken, zoals:

- Vraagstukken, knelpunten en ontwikkelingen die spelen ten aanzien van de dienstverlening in relatie tot de informatiebeveiliging.
- Afhandeling en analyse van beveiligingsincidenten
- Afstemming en bespreking wijzigingsverzoeken met hoge security impact
- Afstemming en bespreking uitkomsten pentesten en vulnerability scans
- Afstemming en bespreking advisories uitgebracht door het NCSC

7. Overlegstructuren

Tussen opdrachtgever en Opdrachtnemer worden structureel op diverse niveaus overleggen gevoerd aangaande de serviceverlening en samenwerking.

Overleg en deelnemers	Periodiciteit	Vastlegging
Operationeel overleg	Op verzoek van opdrachtgever	Opdrachtnemer
Tactisch overleg	1x per 3 maanden	Opdrachtnemer
Strategisch overleg	1x per 12 maanden	Opdrachtnemer
Security overleg	1x per 6 maanden	Opdrachtnemer

In het DAP zullen de overleggen nader worden uitgewerkt (inhoud, contactpersonen, locatie etc.). Van de periodiciteit en samenstelling (tactisch, strategisch) kan in overleg en met wederzijds akkoord afgeweken worden.

8. Retransitie

Tijdens de retransitieperiode dient een exit strategie te worden geformuleerd. De exit strategie heeft ten doel om risico's die zich kunnen manifesteren tijdens de retransitieperiode te mitigeren om zo verstoring van (bedrijfs-)processen te voorkomen.
De uit te voeren retransitie activiteiten maken eveneens deel uit van de resultaatverplichting die Opdrachtnemer aangaat.
Opdrachtnemer commiteert zich aan ten minste de volgende eisen:

1) Opdrachtnemer geeft zijn volledige medewerking aan de exit strategie bij de overgang naar een andere opdrachtnemer.
2) Binnen 10 werkdagen na kennisgeving van de beëindiging van de overeenkomst levert opdrachtnemer een gedetailleerd overdrachtsplan waarin de gestelde eisen zijn vertaald naar concrete activiteiten en tijdslijnen met daarbij de bijbehorende rolverantwoordelijkheden en doorlooptijden.
3) In dit Plan van aanpak (PvA) beschrijft opdrachtnemer tevens de aanpak en maatregelen in het kader van de Exit strategie.
4) Na beëindiging van de Overeenkomst dienen alle gegevens uit de systemen van opdrachtnemer verwijderd te worden. Hiervan dient de opdrachtnemer een verklaring af te geven.
5) Opdrachtgever is te allen tijde in regie met betrekking tot een retransitie van de oplossing. De uitvoering van de retransitie zal in samenwerking tussen de latende-, de nieuwe partij en opdrachtgever worden uitgevoerd.
6) In geval van beëindiging/Exit-regeling duurt de Verwerkers Overeenkomst voort totdat de exit-regeling helemaal is uitgevoerd en door opdrachtgever is geaccepteerd. (overgangsperiode).
7) In geval van beëindiging/Exit-regeling duurt de dienstverlening voort, totdat de exit-regeling helemaal is uitgevoerd en door opdrachtgever is geaccepteerd. (overgangsperiode). De exit verloopt zonder dataverlies of onderbreking van de dienstverlening.
8) De opdrachtnemer garandeert dat hij zijn personeel, en andere middelen, onverwijld beschikbaar stelt voor de overdracht van data en eventuele migratie ten behoeve van de Retransitie/Exit.
9) Data en configuratiegegevens (indien relevant) mogen niet verwijderd worden, totdat de Retransitie/Exit succesvol is uitgevoerd en geaccepteerd door opdrachtgever. Opdrachtnemer levert daarvoor een bewijs van vernietiging aan.
10) Na kennisgeving van de beëindiging van de overeenkomst draagt Opdrachtnemer alle documentatie over, indien nog niet aanwezig op de omgeving van opdrachtgever, inclusief technische documentie m.b.t. datamodellen, scripts, pipelines, beveiligingsinstellingen, changelogs en gebruikersdocumentatie.
11) De exitfase wordt afgesloten met een overgangsgesprek en een gezamenlijke evaluatie.

12) De Opdrachtnemer levert een exitverslag met geleerde lessen, risico’s en aanbevelingen voor toekomstig beheer.

9. Wederzijdse verplichtingen

9.1 Algemeen

Onderstaand zijn de algemene verplichtingen beschreven waar beide partijen zich aan conformeren ten aanzien van de serviceverlening die in dit SLA is beschreven.

9.2 Uitvoering

Opdrachtnemer is verantwoordelijk voor het beheer en onderhoud van de applicatie en de overeengekomen service aan opdrachtgever aan te bieden volgens het afgesproken niveau van serviceverlening.

Opdrachtgever is verantwoordelijk voor het functioneelbeheer, tactisch beheer en strategisch beleid, alsmede evaluaties en reviews van de dienstverlening. Opdrachtnemer speelt in de totstandkoming van het strategisch beleid en tactische planning een adviserende rol.

9.3 Informatie

Opdrachtgever informeert via het Tactisch/strategisch overleg opdrachtnemer tijdig over tactische en strategische planningen en beleidsbepalingen die van invloed kunnen zijn op de operationele uitvoering van de taken van de opdrachtnemer.

Het informeren van (personeel van) opdrachtgever omtrent organisatorische en procedurele wijzigingen in de serviceverlening wordt door opdrachtgever zelf geïnitieerd en uitgevoerd.

Opdrachtnemer informeert opdrachtgever over de kwaliteit van de service en trends daarin. Dit vindt plaats door middel van de in dit SLA gedefinieerde rapportages en het Tactisch/strategisch overleg.

9.4 Bezetting personeel

De levering van de service vindt plaats door de opdrachtnemer. Opdrachtnemer staat garant voor de inzet van voldoende personeel met adequate kennis voor het succesvol uitvoeren van taken alsmede voldoende capaciteit in het kader van de beschreven serviceverlening.

10. Condities en Voorwaarden

10.1 Beperkingen, afhankelijkheden en overmacht

Vermindering van de beschikbaarheid en/of performance van de gecontracteerde serviceverlening valt niet binnen de verantwoordelijkheid van de opdrachtnemer indien deze het gevolg is van:

- Storingen in omgevingsfactoren die binnen de verantwoordelijkheid van opdrachtgever. Bij dergelijke storingen vervallen de verplichtingen van de opdrachtnemer t.a.v. de gestelde eisen binnen dit SLA.
- Het in gebreke blijven van derde partijen waarmee opdrachtgever onafhankelijk van deze SLA contractuele verplichtingen is aangegaan.
- Werkzaamheden, uitgevoerd door derde partijen die onafhankelijk van dit SLA contractuele verplichtingen zijn aangegaan met opdrachtgever.
- Storingen in componenten die niet vallen onder de verantwoordelijkheid van opdrachtnemer. Dit geldt met name voor het netwerk in zoverre dit niet in onderhoud is bij de opdrachtnemer.

10.2 Geschillen

In gevallen waarin het SLA niet voorziet, zal naar goed inzicht en vakmanschap worden gehandeld en zal onderlinge afstemming plaatsvinden met de betreffende verantwoordelijken, teneinde de serviceverlening te waarborgen. Indien partijen niet tot overeenstemming kunnen komen, is de geschillenregeling, zoals vermeld in de Overeenkomst van toepassing.

Indien naar de mening van de opdrachtgever de opdrachtnemer verzaakt om voldoende invulling te geven aan de gemaakte afspraken m.b.t. de dienstverlening, of opdrachtnemer voldoet niet aan de serviceprestaties, dan is opdrachtgever gerechtigd om een externe partij te benaderen om tijdelijk invulling te geven aan de dienstverlening of delen daarvan. Voorgaand treedt pas in werking na het doorlopen van de escalatieprocedure en dit naar de mening van opdrachtgever, niet tot verbetering heeft geleidt (max 1 week).

10.3 Normen en standaards

De beschrijving van de serviceverlening en de inhoud van dit SLA is gebaseerd op de 'IT Infrastructure Library' (ITIL), de Referentie Architectuur van opdrachtgever en de organisatie Blauwdruk van opdrachtgever.

10.4 Geheimhouding

1) Opdrachtnemer en opdrachtgever gebruiken specifieke documentatie en informatie slechts in het kader van de in dit SLA en bijbehorende Overeenkomst vastgelegde relatie en stellen deze documentatie en informatie niet beschikbaar aan derden.
   Het gaat hier om zaken zoals:
   - Bedrijfsspecifieke informatie en interne documenten van opdrachtgever;
   - Het SLA en daarbij behorende documentatie;
   - De systeemspecificaties;
   - Eventuele andere documenten en informatie zoals beschreven in de bij de Overeenkomst behorende stukken.

2) Medewerkers die een arbeidsovereenkomst hebben met de opdrachtnemer en toegang hebben tot informatie betreffende deze overeenkomst, dienen een Non-Disclosure/Confidentiality agreement te hebben ondertekend. In incidentele gevallen kan opdrachtgever verzoeken om bewijsvoering.

2) Opdrachtnemer hanteert een privacyreglement, waarin de vertrouwelijke behandeling van gegevens van opdrachtgever wordt geregeld. Medewerkers van opdrachtnemer die toegang hebben tot deze gegevens zullen zich enkel toegang verschaffen op verzoek van opdrachtgever, of wanneer dat nodig zou zijn om storingen of onvolkomenheden te verhelpen. Medewerkers van Opdrachtnemer worden geacht in het bezit te zijn van een VOG. Het privacyreglement kan op aanvraag worden ingezien.

11 Bijlagen

11.1 Bijlage A Begrippenkader v1.0

begrip	afk.	definitie
Beschikbaarheid		Beschikbaarheid is als volgt gedefinieerd: ▪ Beschikbaarheidspercentages worden per kalendermaand gemeten over de beschreven services en serviceniveaus. ▪ Beschikbaarheidspercentages drukken beschikbaarheid uit, exclusief benodigde tijd voor onderhoudswerkzaamheden binnen het onderhoudsvenster. Een service is beschikbaar als: ▪ De voor deze service overeengekomen functionaliteit kan worden gebruikt; ▪ En de voor deze service overeengekomen performance wordt gehaald.
Calamiteit		Een onverwachte interruptie van (kritieke) bedrijfsprocessen en -systemen, waardoor de continuïteit van de opdrachtgever in gevaar komt of de veiligheid van de medewerkers in het geding is.
Change management		Change management is het proces dat gebruik maakt van gestandaardiseerde procedures. Deze procedures helpen om eenvoudiger wijzigingen door te voeren in de IT-infrastructuur, met zo min mogelijk onderbrekingen.
Incident management		Het proces van Incident management richt zich op het zo snel mogelijk terugbrengen van diensten naar hun normale staat. In het ideale scenario gebeurt dit met zo weinig mogelijk of zelfs geen impact op de core business.
Kantooruren		Ieder uur van een werkdag tussen 08.00 en 18.00 uur.
Oplostijd		De tijd tussen het melden van het incident en het weer beschikbaar zijn van de service door middel van het aanbieden van een oplossing of work-around.
Problem management		Een problem is een onbekende oorzaak van een of meer incidenten. Het proces Problem management gaat op een gestructureerde wijze om met bundelen van incidenten, en het proactief voorkomen van een problem.
Root Cause Analysis	RCA	Een systematische aanpak om de oorzaak van een incident of probleem te identificeren.
Service Improvement Plan	SIP	Het SIP is bedoeld om structurele afwijkingen van servicenormen te onderzoeken, maatregelen te definiëren en te effectueren.
Service Level Agreement	SLA	Een SLA is een Overeenkomst tussen een opdrachtnemer en een opdrachtgever van bepaalde diensten en/of producten. In een SLA staan, naast de beschrijving van de te leveren diensten, ook de rechten en de plichten van zowel de opdrachtnemer als de opdrachtgever ten aanzien van het overeengekomen kwaliteitsniveau (service level) van de te leveren diensten en/of producten (services).
Terugkoppeltijd		In geval van een storing die niet direct oplosbaar blijkt, is dit de tijd waarbinnen wordt aangegeven wat de vervolgstappen, de verwachte doorlooptijd en volgende terugkoppelmomenten zijn.
Urgente change		In uitzonderlijke gevallen kan een spoedchange worden aangevraagd; daarvoor bestaat een door de opdrachtnemer opgestelde speciale procedure.

begrip	afk.	definitie
Werkdag		Iedere dag van de week met uitzondering van zaterdag en zondag en erkende nationale feestdagen.