

Dossier Afspraken en Procedures

Kenmerk: 538022

Versie: 1.0

Datum: 15-8-2025

Auteur:



Inhoudsopgave

1	Inleiding	3
	Doel van het DAP	3
	Geldigheidsduur.....	3
	Wijzigingsprocedure.....	3
2	Contactgegevens.....	4
	Contactgegevens Inschrijver	4
	Contactgegevens gemeente Huizen	4
3	Samenwerking	6
	Overlegvormen en frequentie	6
4	Governance	8
	Service Level Rapportage	8
	Privacy en Informatiebeveiliging	8
5	Processen en werkafspraken	10
	Servicedesk.....	10
	ITSM tooling.....	10
	Incidenten beheer	11
	Probleembeheer	11
	Wijzigingsbeheer	11
	Release management	11
	Informatiebeveiliging.....	11
6	Escalatieschema	12
	Bijlage A Overzicht van standaard wijzigingen	13
	Verklarende begrippenlijst.....	14

1 Inleiding

Doel van het DAP

Het voorliggende document 'Dossier van Afspraken & Procedures' (verder te noemen DAP) bevat een concrete beschrijving van de operationele werkafspraken die gelden voor de levering van Diensten door Inschrijver. Dit document is onlosmakelijk verbonden met de overeenkomst [overeenkomstreferentie] waarin de af te nemen Dienst(en) overeen zijn gekomen.

Verder beschrijft dit DAP de operationele en tactische afspraken evenals de procedures die noodzakelijk zijn om de diensten, die beschreven staan in de Service Level Agreement (SLA), succesvol te leveren aan gemeente Huizen.

Geldigheidsduur

Dit DAP kent een looptijd vanaf de startdatum van de overeenkomst tot en met de beëindiging van de overeenkomst.

Wijzigingsprocedure

De inhoud van het DAP is de gezamenlijke verantwoordelijkheid van Inschrijver en de gemeente Huizen. Voorstellen tot wijzigingen op dit document worden tussen Inschrijver en de Contract manager van gemeente Huizen vastgesteld. Wijzigingen op het DAP dienen te passen binnen de kaders die gedefinieerd zijn in de geldende Overeenkomst en Service Level Agreement (SLA) tussen gemeente Huizen en Inschrijver.

- Inschrijver voert de afgesproken wijzigingen in het DAP door;
- Het gewijzigde DAP wordt verspreid onder Opdrachtgever en Inschrijver.

2 Contactgegevens

Dit hoofdstuk beschrijft alle betrokken partijen en bijbehorende contactpersonen.

Contactgegevens Inschrijver

Algemene gegevens

Soort	Adres
Bezoekadres	
Postadres	

Contactpersonen

Rol	Eerste contact	Plaatsvervanger
<rol>	<naam> ☎ (088) 123 45 67 ✉ <e-mail>	<naam> ☎ (088) 123 45 67 ✉ <e-mail>
<rol>	<naam> ☎ (088) 123 45 67 ✉ <e-mail>	<naam> ☎ (088) 123 45 67 ✉ <e-mail>

Contactgegevens gemeente Huizen

Algemene gegevens

Soort	Adres
Bezoekadres	Graaf Wichman 10, 1276 KB Huizen Nederland
Postadres	Postbus 5 1270 AA Huizen Nederland

Contactpersonen

Rol	Eerste contact	Plaatsvervanger
Portfolio Manager ICT	<naam> ☎ (035) 123 45 67 ✉ <e-mail>	<naam> ☎ (035) 123 45 67 ✉ <e-mail>
Contract manager	<naam> ☎ (035) 123 45 67 ✉ <e-mail>	<naam> ☎ (035) 123 45 67 ✉ <e-mail>
Functioneel beheerder(s)	<naam> ☎ (035) 123 45 67 ✉ <e-mail>	<naam> ☎ (035) 123 45 67 ✉ <e-mail>
Servicepunt	<naam> ☎ (035) 123 45 67 ✉ <e-mail>	<naam> ☎ (035) 123 45 67 ✉ <e-mail>
Informatiemanager	<naam> ☎ (035) 123 45 67	<naam> ☎ (035) 123 45 67

	✉ <e-mail>	✉ <e-mail>
Informatiebeveiliging	<naam>	<naam>
	☎ (035) 123 45 67	☎ (035) 123 45 67
	✉ <e-mail>	✉ <e-mail>

Deze contactpersonen zijn gerechtigd om contact op te nemen met de Servicedesk van Inschrijver voor het plaatsen van een melding. Alleen de Contract manager is gerechtigd om wijzigingen aan te brengen in deze lijst van contactpersonen.

3 Samenwerking

Overlevormen en frequentie

Inschrijver voert, ten behoeve van het bewaken van de kwaliteit van de geleverde producten en dienstverlening, overleg met de gemeente Huizen. De gemeente Huizen en Inschrijver voeren de volgende overleggen met bijbehorende frequentie:

Operationeel overleg	
Doel	In dit overleg bespreken we lopende incidenten, wijzigingsaanvragen en wijzigingen. Het toetsen van de voortgang en prioritering.
Frequentie	1x per maand
Aanwezigen	<i>Gemeente Huizen:</i> Functioneel beheerder(s) <i>Inschrijver:</i> <deelnemers>
Resultaat	Acties op operationeel niveau, gericht op het realiseren van de gemaakte (SLA) afspraken.
Input	Service Level rapportage (maand)

Product overleg	
Doel	In dit overleg bespreken we de voortgang op de roadmap van Inschrijver, welke functionaliteiten zijn gereleased conform de gestelde roadmap en wat er de komende 6 - 9 maanden op de roadmap staat.
Frequentie	1x per kwartaal
Aanwezigen	<i>Gemeente Huizen:</i> Informatiemanager Functioneel beheerder <i>Inschrijver:</i> <deelnemers>
Resultaat	Acties op operationeel niveau, gericht op het realiseren van de gemaakte (SLA) afspraken.
Input	Roadmap & releasekalender Inschrijver

Service Level overleg	
Doel	In dit overleg bespreken we de kwaliteit van de dienstverlening, aan de hand van de Service level rapportages, en voorstellen tot verbetering van de kwaliteit van de dienstverlening.
Frequentie	1x per kwartaal
Aanwezigen	<i>Gemeente Huizen:</i> Contract manager Functioneel beheerder <i>Inschrijver:</i> <deelnemers>

Resultaat	Acties op operationeel niveau, gericht op het realiseren van de gemaakte (SLA) afspraken.
Input	Service Level rapportage (kwartaal)

Strategisch overleg

Doel	Doel van dit overleg is het bespreken van de dienstverlening in de afgelopen periode, het bespreken van nieuwe marktontwikkelingen en het bepalen van eventuele aanpassingen in de dienstverlening. Van Inschrijver wordt verwacht dat deze ook gevraagd en ongevraagd advies geeft over optimalisatie en kwaliteitsverbetering.
Frequentie	1x per kwartaal
Aanwezigen	<i>Gemeente Huizen:</i> Contract manager Teamleider Strategisch Inkoper <i>Inschrijver:</i> <deelnemers>
Input	Service Level rapportage (jaar)

Informatiebeveiliging overleg

Doel	Doel van dit overleg is het toetsen van de effectiviteit van de huidige informatiebeveiliging en privacy maatregelen en waar nodig bij te stellen, zodat zowel Opdrachtgever inzicht heeft in actuele risico's en incidenten, en concrete vervolg-acties en verantwoordelijkheden voor het komende jaar zijn vastgesteld.
Frequentie	1x jaar in december
Aanwezigen	<i>Gemeente Huizen:</i> CISO en/of ISO Privacy-officer <i>Inschrijver:</i> <deelnemers>
Input	Informatiebeveiliging Rapportage; Kwetsbaarhedenanalyses

4 Governance

Service Level Rapportage

5 werkdagen voorafgaande aan het Operationeel overleg en Service Level overleg stuurt Inschrijver in digitale vorm een Service Level Rapportage naar de gemeente Huizen. De rapportage heeft betrekking op de voorliggende periode (kalendermaand, kwartaal of jaar). De ontvangers van deze rapportage zijn, ten minste, de functioneel beheerder(s), informatiemanager en contract manager van Opdrachtgever. De rapportage bevat ten minste de volgende onderdelen:

Incident management rapportage

- Incidenten in de afgelopen periode en trends m.b.t. behalen SLA;
- Status en voortgang openstaande incidenten

Probleem beheer rapportage

- Problemen in de afgelopen periode en trends m.b.t. behalen SLA;
- Status en voortgang openstaande problemen

Wijzigingsbeheer rapportage

- Wijzigingen in de afgelopen periode en trends m.b.t. behalen SLA;
- Status en voortgang openstaande wijzigingsverzoeken en wijzigingen.

Privacy en Informatiebeveiliging

Informatiebeveiliging Rapportage

5 werkdagen voorafgaande aan het Informatiebeveiliging overleg stuurt Inschrijver in digitale vorm een Informatiebeveiliging Rapportage naar Opdrachtgever. De ontvangers van deze rapportage zijn, ten minste, de functioneel beheerder(s), informatiemanager en CISO van Opdrachtgever. De rapportage bevat ten minste de volgende onderdelen:

- alle security gerelateerde incidenten en kwetsbaarheden in de afgelopen periode
- alle geconstateerde datalekken in de afgelopen periode

Kwetsbaarhedenanalyse

Inschrijver voert minimaal ieder kwartaal een kwetsbaarhedenanalyse uit. Inschrijver stuurt na iedere kwetsbaarhedenanalyse een Rapportage van bevindingen naar Opdrachtgever. De ontvangers van deze rapportage zijn, ten minste, de CISO en ISO. De rapportage bevat ten minste de volgende onderdelen:

- Beoordeling van het risico per kwetsbaarheid.
- Bewijs van opvolging (patches, mitigatie, etc.).
- Aangegeven wat er is opgelost of nog open staat.

Inschrijver rekent geen extra kosten voor het uitvoeren van kwetsbaarheidsanalyses.

Pentest

Inschrijver laat door een onafhankelijke partij een pentest uitvoeren. Inschrijver stuurt na de pentest een Rapportage van bevindingen naar Opdrachtgever. De ontvangers van deze rapportage zijn, ten minste, de CISO en ISO van Opdrachtgever. De rapportage bevat ten minste de volgende onderdelen:

- volledig rapport van de pentest inclusief aanpak, scope, bevindingen, risicoanalyse.
- Aangegeven welke kwetsbaarheden daadwerkelijk exploiteerbaar waren.
- Actieplan voor mitigatie of herstel.

Een aanvullende penetratietest kan vereist zijn bij:

- Ingrijpende wijzigingen aan de applicatie (zoals herbouw, migratie of ingrijpende technische updates).
- Implementatie van nieuwe functionaliteit die impact heeft op authenticatie, autorisatie of gegevensuitwisseling.
- Ernstige beveiligingsincidenten of datalekken waarbij twijfels ontstaan over de weerbaarheid van het systeem.
- De noodzaak tot een extra pentest wordt beoordeeld door een security professional op basis van een risico-inschatting in overleg met de opdrachtgever (gemeente).

Inschrijver rekent geen extra kosten voor het uitvoeren van pentesten.

DigiD-aansluiting

Inschrijver laat een externe audit uitvoeren op ten minste de normen die door ENSIA zijn voorgeschreven. Deze audit dient te voldoen aan de eisen van ENSIA, waarbij gecontroleerd wordt op compliance over een aaneengesloten periode van minimaal zes maanden. Het bijbehorende RDO-rapport (Rapport Doelmatigheid Operationeel) (eerder gehete TPM-verklaring) dient zo spoedig mogelijk na ontvangst met Opdrachtgever te worden gedeeld. Inschrijver rekent geen extra kosten voor het uitvoeren van de audits.

ISO 27001

Inschrijver deelt gedurende de contractperiode jaarlijks een samenvatting van de meest recente surveillance-audit. Deze audit wordt uitgevoerd door een certificerende instantie in het kader van de jaarlijkse controle tijdens de looptijd van het certificaat. Deze samenvatting dient de scope, de auditdatum, geconstateerde afwijkingen (indien van toepassing), en de status van opvolging te bevatten. Inschrijver deelt ook een Actuele Verklaring van Toepassing waarin duidelijk is aangegeven welke beheersmaatregelen van ISO 27001 van toepassing zijn en waarom, en waarom bepaalde maatregelen eventueel niet van toepassing zijn.

De ontvangers van deze samenvatting en verklaring zijn, ten minste, de CISO en ISO van Opdrachtgever. Inschrijver rekent geen kosten door aan Opdrachtgever voor het uitvoeren van de audits.

5 Processen en werkafspraken

In de volgende paragrafen zijn de beheerprocessen op de koppelvlakken tussen Opdrachtgever en Inschrijver in detail beschreven. Het beheer behelst de dagelijkse werkzaamheden voor het in bedrijf houden van de dienstverlening voor Opdrachtgever. Het grootste deel van deze activiteiten is belegd bij Inschrijver.

Het beheer omvat de volgende processen:

1. Incidenten beheer
2. Probleem beheer
3. Wijzigingsbeheer
4. Release management
5. Informatiebeveiliging

Service desk

De volgende soorten meldingen kunnen door Opdrachtgever bij de Service desk van Inschrijver worden ingediend:

Soort	Toelichting
Vraag	Verzoek om informatie of advies
Verzoek	Een verzoek van de gebruiker om ondersteuning, autorisatie, levering of documentatie etc. (<i>Service request</i>)
Verstoring	Een verstoring van de bestaande dienstverlening (<i>Incident</i>)

Alleen het Servicepunt van Opdrachtgever en de functioneel beheerders bij Opdrachtgever zijn gerechtigd om meldingen bij de Service desk van Inschrijver in te dienen. Inschrijver ziet hierop toe.

ITSM tooling

Ter ondersteuning aan de beheersprocessen gebruikt Opdrachtgever de service management tool TOPdesk. TOPdesk geldt binnen de gemeente als centraal systeem voor het vastleggen, volgen en beheren van verzoeken, incidenten, wijzigingen en overige aan beheer gerelateerde taken.

Opdrachtgever werkt in haar eigen TOPdesk omgeving en gaat er vanuit dat Inschrijver in haar eigen ITSM tooling zal werken. Inschrijver accepteert en organiseert één van onderstaande manieren, om samen te kunnen werken met Opdrachtgever:

1. **Communicatie middels e-mail;** Inschrijver accepteert het ontvangen van verzoeken via e-mail en communiceert per e-mail terug naar het generieke e-mailadres van de gemeente Huizen. In de onderwerpregel van e-mailberichten gebruikt Inschrijver, indien van toepassing, het referentienummer van de bijbehorende melding in de TOPdesk omgeving van Opdrachtgever.
2. **Integratie middels de REST API** van TOPdesk; Inschrijver is verantwoordelijk voor het opzetten en onderhouden van de integratie.

Incidenten beheer

Geen nadere afspraken.

Probleembeheer

Inschrijver voert Probleembeheer uit op haar dienstverlening. Inschrijver communiceert openstaande bekende fouten met Opdrachtgever en bijbehorende work-arounds.

Wijzigingsbeheer

Standaard en niet-standaard wijzigingen mogen alleen worden aangevraagd door gemandateerde gebruikers van Opdrachtgever.

Release management

De ICT prestatie wordt gedurende de looptijd van de overeenkomst periodiek voorzien van (security)patches en upgrades (nieuwe releases). De releasenotes moeten per wijziging een duidelijke omschrijving bevatten van wat er gewijzigd is.

Bij updates, upgrades, patches en fixes zorgt Inschrijver ervoor dat configuraties (denk aan bestaande werkstromen en instellingen) intact blijven en hun werking behouden. Het moet duidelijk zijn welke invloed de wijzigingen hebben op de configuraties (zoals werkstromen). Daarnaast zorgt Inschrijver voorafgaand aan de update, upgrades, patch of fix voor de bijbehorende releasenotes.

Inschrijver levert minimaal jaarlijks een releasekalender op dat inzicht verschaft in de, over minimaal de opvolgende 12 maanden, geplande softwareversies van de ICT oplossing.

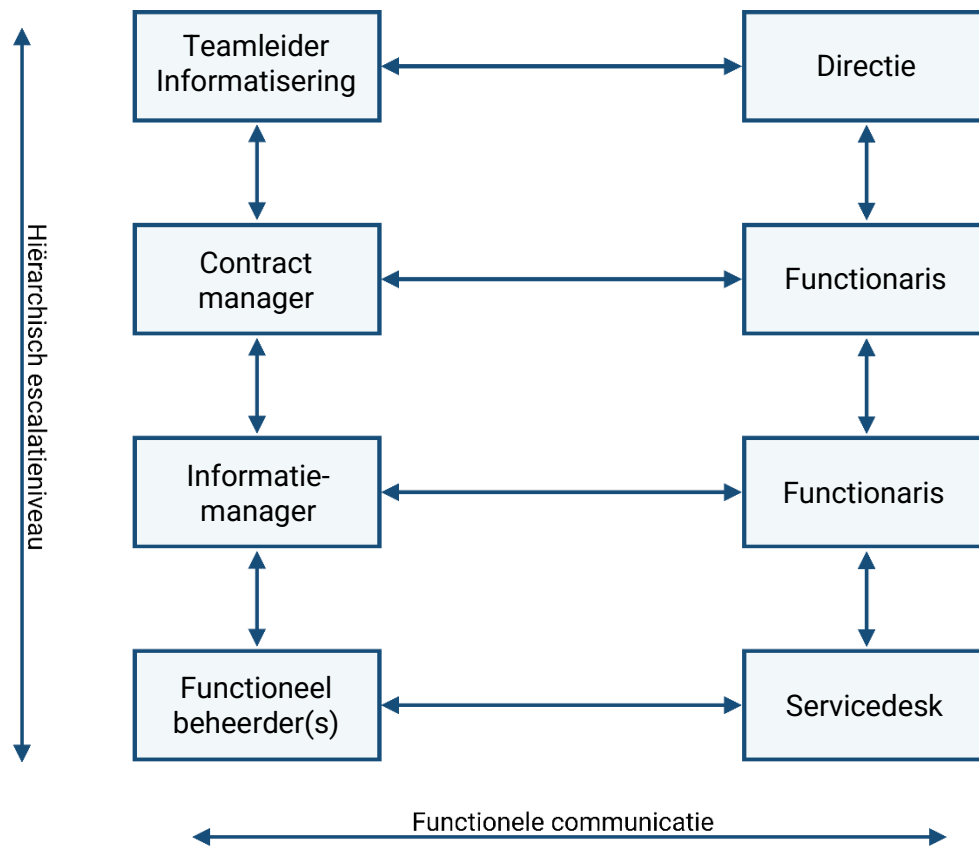
Informatiebeveiliging

Inschrijver meldt een beveiligingsincident op het moment van onderkennen altijd aan Opdrachtgever en uiterlijk binnen 72 uur, zodat de melding bij de Autoriteit Persoonsgegevens (AP) ook binnen de geldende termijn plaatsvindt. Opdrachtgever beslist of een beveiligingsincident kan worden gekwalificeerd als datalek en zorgt in dat geval voor de melding aan de AP en het in kennis stellen van de betrokkenen. Niet door Inschrijver gemelde beveiligingsincidenten, die leiden tot een boete van de AP en/of aan een betrokkene toe te kennen schade als gevolg van schending van diens privacy, zal Opdrachtgever verhalen op Inschrijver.

6 Escalatieschema

Er is sprake van een Escalatie bij het overschrijden van de afgesproken Service Level Afspraken of een Incident met Prioriteit 1, of wanneer partijen geen overeenstemming bereiken over toekenning van een Prioriteit aan een Incident. Bij Prioriteit 2, 3 of 4 kan ook geëscaleerd worden indien Opdrachtgever dat nodig acht. Escalaties vragen een actieve management betrokkenheid, wanneer processen geen acceptabele oplossing bieden aan de klant of business in de afgesproken tijdsperiode.

Escalaties proberen we zoveel mogelijk te voorkomen. Inschrijver zorgt ervoor dat te allen tijde functionarissen van voldoende hiërarchisch niveau beschikbaar zijn om escalaties af te handelen. Een escalatie vindt plaats conform onderstaande schema.



Figuur 5.1 – Escalatieschema

Bijlage A Overzicht van standaard wijzigingen

Hieronder is het overzicht van de standaard changes van Inschrijver. Gedurende de looptijd van de afgenomen dienst(en) kunnen er andere standaard changes gedefinieerd worden.

<geen specifieke standaard wijzigingen>

Verklarende begrippenlijst

Begrip	Omschrijving
DAP (Dossier van Afspraken en Procedures)	Een document waarin alle operationele afspraken, procedures en werkinstructies zijn vastgelegd die gelden tussen Inschrijver Opdrachtgever.
Datalek	Toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.
Hersteltijd	De termijn waarbinnen de dienstverlening is hersteld na het constateren van een incident.
ICT prestatie	Alle door Inschrijver op grond van de Overeenkomst te leveren goederen, waaronder Producten, Gebruiksrechten en Diensten.
Incident	Een ongeplande verstoring in de dienstverlening waardoor de te verwachten kwaliteit dienstverlening in zijn geheel of gedeeltelijk is verdwenen of dreigt te verminderen.
Klacht	Een klacht over de dienstverlening van Inschrijver.
Onderhoudsvenster	Het onderhoudsvenster stelt partijen in staat op vooraf vastgestelde tijden regulier onderhoud uit te voeren. Ook bekend als maintenance window.
Overeenkomst	De tussen Partijen gesloten overeenkomst waarvan de SLA onderdeel uitmaakt.
Prestatie indicatoren	Minimum, standaard en meetbare prestatie-indicator waaraan gemeten wordt of Inschrijver aan de gemaakte afspraken voldoet.
Probleem	De onderliggende oorzaak van één of meerdere incidenten.
Reactietijd	De termijn waarbinnen een (eerste) inhoudelijke reactie op een verzoek plaatsvindt door Inschrijver.
Release	Een release is een verzameling van één of meer wijzigingen die samen worden getest, goedgekeurd en uitgerold naar de productieomgeving.
Releasenotes	Documentatie die de inhoud van een release beschrijft, inclusief nieuwe functionaliteiten, verbeteringen, opgeloste bugs en bekende beperkingen.
Service level	Een service level is een meetbare prestatie-eis waaraan een dienst moet voldoen. Het vormt de basis voor afspraken in een SLA.
Service request	Een service request is een formeel verzoek van een gebruiker voor een standaarddienst of -actie, die vaak vooraf is goedgekeurd. Het betreft géén storing of wijziging.
Servicevenster	Het servicevenster is de tijd waarbinnen een beroep gedaan kan worden op de dienstverlening van Inschrijver. Ook bekend als service window.
SLA (Service Level Afspraken)	Een formele overeenkomst tussen Inschrijver en klant waarin afspraken staan over service levels.
Wijziging	Een wijziging (ook wel Change genoemd) is elke aanpassing aan de bestaande IT-diensten, bedoeld om functionaliteit te verbeteren of problemen op te lossen of te voorkomen.

Wijzigingsaanvraag	Een wijzigingsaanvraag is een formeel verzoek om een wijziging door te voeren. Deze aanvraag wordt geëvalueerd op risico's, impact, urgentie en kosten voordat deze wordt goedgekeurd.
--------------------	--
