



Bijlage 11
Model Dossier Afspraken
en & Procedures

Behorend bij

Openbare Europese Aanbesteding
Raamovereenkomst Diensten en Leveringen
Audiovisuele Middelen 2026

AV2026

Datum

1-4-2025

1 Inleiding

In deze bijlage treft u onderstaand een model van een eerste basisversie van het Dossier Afspraken en Procedures. Dit geeft een indruk van de te adresseren onderwerpen. Per Perceel kan dit tot aanzienlijke verschillen leiden bij de uitwerking. Dit model is gebaseerd op een geanonimiseerde oude DAP voor onderhoud en beheer.

2 Inhoudsopgave

1. WIJZIGINGSBEHEER, REFERENTIES EN DEFINITIES	4
1.1 Versiebeheer	4
1.2 Distributielijst	4
1.3 Document referenties en structuur	4
1.4 Ondertekening	5
2. INLEIDING	5
2.1 Partijen	5
2.2 Doel van het DAP	5
2.3 Onderwerp van het DAP	5
2.4 Geldigheidsduur van het DAP	6
2.5 Wijziging van het DAP	6
2.6 Distributie van het DAP	6
3. BEHEER DOOR <NAAM OPDRACHTNEMER> CONFORM ITIL PROCESMODEL	7
4. BEHEER EN ONDERHOUD	8
4.1 Inleiding	8
4.2 Servicedesk en contactgegevens	8
4.2.1 <Naam Organisatie> contactgegevens	8
4.2.2 Bereikbaarheid van <Naam Organisatie> binnen kantoortijd	10
4.2.3 Bereikbaarheid <Naam Organisatie> buiten kantoortijd	10
4.2.4 <Naam Opdrachtnemer> Servicedesk t.b.v. XXXX	10
4.2.5 Overige contactpersonen binnen <Naam Opdrachtnemer> mbt de dienstverlening	11
4.2.6 Adres van <Naam Opdrachtnemer>	11
4.2.7 Wijziging van (contact)gegevens	11
4.3 Incident management	12
4.3.1 Coördinatie incidentmeldingen	12
4.3.2 Reparatietijd	12
4.3.3 Classificatie incident	13
4.3.4 Schematisch overzicht interfacemomenten incidentmelding	13
4.3.5 Interfacemomenten reactieve incidentmelding	13
4.3.6 Verantwoordelijkheden van <Naam Opdrachtgever>	16
4.3.7 Verantwoordelijkheden van <Naam Opdrachtnemer>	16
4.3.8 Ten onrechte incidentmeldingen	16
4.4 Event management	17
4.4.1 Overzicht interfacemomenten events	17
4.4.2 Beschrijving Interfacemomenten events	17
4.5 Problem management	18
4.6 IT operation, backup and restore	19
4.6.1 Inleiding	19
4.6.2 Proces systeemback-up <Systeem XX>	19
4.6.3 Proces data backup	19
4.7 Change management	21
4.7.1 Trigger voor het proces	21
4.7.2 Change classificatie	21
4.7.3 Realisatietijd bij changes	22
4.7.4 Maintenance Window	22
4.8 Release management	23
4.8.1 Schematisch overzicht interfacemomenten standaard/minor changes	23
4.8.2 Interfacemomenten	23
4.8.3 Schematisch overzicht interfacemomenten major changes	25
4.8.4 Interfacemomenten	25
4.9 Configuration & Asset management	26

4.9.1	Configuratie Items	26
4.9.2	Informatie uitwisseling <Naam Opdrachtnemer> – <Naam Opdrachtgever>	26
4.10	Capacity management	26
4.11	Availability management	26
4.12	Continuity management	27
4.13	Security management	27
4.13.1	Toegankelijkheid systemen:	27
4.13.2	Fysieke toegang tot locaties van de Rvdr	28
4.13.3	Paswoorden en autorisaties:	28
4.14	Financial Management	29
5.	SERVICE LEVEL MANAGEMENT	30
5.1	Reporting	30
5.2	Vorm, frequentie en detailniveau van de rapportages	30
5.3	Inhoud van de rapportages	31
5.3.1	Algemeen	31
5.3.2	Specifiek Incident Management	31
5.3.3	Specifiek Problem Management	31
5.3.4	Specifiek Change Management	32
5.4	Service levels dienst telefonie	32
5.5	Klanttevredenheid	32
5.6	Leverancier management	33
5.7	Overlegstructuur	33
5.8	Dienstenniveau overleg	33
5.9	Contract-Commercieel overleg	34
5.10	Strategisch overleg	34
5.10.1	Strategische Afstemming	34
5.10.2	Strategische Overleg	34
5.11	Producten en Diensten Catalogus	35
6.	ESCALATIE	36
6.1	Escalatieprocedure voor incident management	36
6.2	Contactgegevens t.b.v. escalaties	36
7.	RACI TABEL MBT VERANTWOORDELIJKHEDEN DIENSTVERLENING	38

1. Wijzigingsbeheer, referenties en definities

1.1 Versiebeheer

[illegible]

1.2 Distributielijst

Naam	Functie

1.3 Document referenties en structuur

<Naam Opdrachtnemer> levert aan de Rechtspraak als vermeld in de Raamovereenkomst en/of Nadere Overeenkomst en de daartoe behorende bijlagen.

Hieronder in volgorde van belang:

- 1) Doc 1
- 2) Doc 2

Dit document ‘Document Afspraken en Procedures (DAP)’ beschrijft, op operationeel niveau de werkaafspraken die gemaakt zijn tussen de Raad voor de rechtspraak en <Naam Opdrachtnemer> ten behoeve van de serviceverlening zoals overeengekomen in de hierboven genoemde documenten. Het DAP is dus een vertaling van de overeenkomst en de SLA naar operationele werkaafspraken hierdoor staan bepaalde zaken zowel in de overeenkomst/SLA als ook in het DAP vermeld.

1.4 Ondertekening

Goedkeuring		
	Raad voor de rechtspraak	<Naam Opdrachtnemer>
Versie		
Naam		
Paragraaf		
Datum		

2. Inleiding

2.1 Partijen

- De Raad voor de rechtspraak, hierna te noemen 'de Rvdr' = opdrachtgever;
- <Naam Opdrachtgever>, de ICT-dienstverlener voor de Rechtspraak, hierna te noemen '<Naam Opdrachtgever>'; = uitvoerder Functioneel Beheer
- De Rechtspraak, alle werknemers werkzaam voor en namens de Rvdr = eindgebruikers
- <Naam Opdrachtnemer>, hierna te noemen '<Naam Opdrachtnemer>'

2.2 Doel van het DAP

Het DAP is onderdeel van de Dienstverlening die is overeengekomen tussen de Raad voor de Rechtspraak en <Naam Opdrachtnemer>. In onderstaande figuur is de relatie tussen de verschillende documenten schematisch weergegeven:

2.3 Onderwerp van het DAP

Het Document Afspraken en Procedures (DAP) beschrijft, op operationeel niveau, de werkafspraken die gemaakt zijn tussen de <Naam> en <Naam Opdrachtnemer> ten behoeve van de serviceverlening zoals overeengekomen in de overeenkomst genoemd in paragraaf 1.3 van dit document, hierna te noemen "de Overeenkomst" over:

- Overeengekomen dienstverlening
- Incident- en change-afhandeling
- Communicatie inclusief rapportage

Het DAP is een vertaling van de overeenkomst/SLA naar operationele werkafspraken. Hierdoor staan bepaalde zaken zowel in de overeenkomst/SLA als ook in het DAP vermeld.

De leveringen en diensten <Perceel X> wordt door <Naam Opdrachtnemer> geleverd aan de Raad voor de Rechtspraak.

2.4 Geldigheidsduur van het DAP

De geldigheidsduur van het DAP komt overeen met de geldigheidsduur van de Overeenkomst.

2.5 Wijziging van het DAP

Wijzigingen binnen het DAP zijn mogelijk voor zover dit niet in tegenspraak is met de overeenkomst. De wijzigingen dienen goedgekeurd te worden door de personen benoemd in paragraaf 1.4

Voorgestelde wijzigingen op het document zijn onderwerp van gesprek in het dienstenniveau overleg.

2.6 Distributie van het DAP

De Contract Manager van <Naam> is verantwoordelijk voor de distributie van het DAP bij initiële en gewijzigde uitgave binnen <Naam>, conform de distributielijst.

De Service Manager van <Naam Opdrachtnemer> is verantwoordelijk voor de distributie van het DAP bij initiële en gewijzigde uitgave binnen <Naam Opdrachtnemer>, conform de distributielijst.

Binnen <Naam Organisatie> zullen onderstaande rollen te maken gaan krijgen / gaan werken met dit DAP:

1. Lokale Medewerkers
2. Contractmanager
3. Regievoerder
4. Dienstverantwoordelijke

De Contractmanager van <Naam Organisatie> is zelf verantwoordelijk voor de distributie van het DAP naar deze betrokkenen of geeft duidelijk aan <Naam Opdrachtnemer> aan wie op de distributielijst moeten staan aangaande dit DAP.

3. Beheer door <Naam Opdrachtnemer> conform ITIL Procesmodel

Gedurende het implementatieproces van de nieuwe dienstverlening zal in gezamenlijk overleg gekozen hoe de beheerprocessen in te richten volgens het ITIL V3 procesmodel.

Concreet betekent dit dat het beheer wordt beschreven en uitgevoerd volgens onderstaand procesmodel:

Servicelevenscyclus	Processen
Beheer en Onderhoud	Service Desk
	Incident Management
	Event Management
	Problem Management
	IT operation, backup and restore
	Change Management
	Configuration & Asset management
	Capacity Management
	Availability Management
	Continuity Management
	Security Management
	Financial Management
Service Level Management	Reporting
	Service Levels Dienst Telefonie
	Klanttevredenheid
	Leverancier Management
	Overlegstructuur
	Producten en Diensten Catalogus

In de nu volgende hoofdstukken worden de diverse servicelevenscycli en de bijbehorende processen beschreven.

4. Beheer en Onderhoud

4.1 Inleiding

Bij beheer en onderhoud gaat het om de activiteiten die nodig zijn om de dienstverlening te kunnen leveren en ondersteunen. In de komende paragrafen worden de onderstaand processen en functies beschreven:

Functies:

- Servicedesk

Processen:

- Incident management
- Event management
- Problem management
- IT Operations, Back-up en Restore
- Changemanagement
- Configuration en Asset management
- Capacity management
- Availability management
- Continuity management
- Security management
- Financial management

4.2 Servicedesk en contactgegevens

In de nu volgende paragrafen is vastgelegd welke partijen elkaar kunnen/mogen aansturen en met elkaar in overleg kunnen/mogen treden.

4.2.1 <Naam Organisatie> contactgegevens

In geval van incidenten, changes en helpdeskvragen kan vanuit <Naam Organisatie> door een select aantal medewerkers contact opgenomen worden met <Naam Opdrachtnemer>.

Geautoriseerde medewerkers voor melding incidenten en standaard en Minor changes:

Naam	Functie	Tel./ Fax / GSM	E-mail

De wijze van terugkoppeling wordt tijdens elk nieuw contactmoment hernieuwd vastgelegd.

Geautoriseerde medewerkers voor melding van 'Major Changes':

Naam	Functie	Tel./ Fax / GSM	E-mail

Vanuit <Naam Organisatie> worden tevens twee contactpersonen aangewezen. <Naam Opdrachtnemer> neemt contact op met één van deze beide personen indien de oplossing van het incident of implementatie

van een change gepaard gaat met:

- Werkzaamheden/incidenten/changes welke impact hebben op de gehele dienstverlening of een gedeelte hiervan, met mogelijke downtijd tot gevolg
- Impact in de functionaliteit van meerdere gebruikers
- Vervolgwerkzaamheden op locatie
- Indien kosten gemoeid zijn met de oplossing van het incident
- Dreigende escalaties
- Changes die niet onder de standaard changes vallen.
- Algemene ontwikkeling/uitbreiding dienstverlening
- Financiële discussies
- Communicatie naar alle gebruikers

Deze contactpersonen zijn voor de Servicedesk van <Naam Opdrachtnemer> als volgt bereikbaar:

Primaire contactpersonen	
Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	
Naam	
Afdeling	
Telefoon	
GSM	
Fax	
E-mail	
Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	

Secundaire contactpersoon	
Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	

Binnen <Naam Organisatie> is onderstaande contractmanager verantwoordelijk voor de Overeenkomst waarop dit DAP is gebaseerd:

Contractmanager bij de Rvdr

Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	

4.2.2 Bereikbaarheid van <Naam Organisatie> binnen kantoortijd

- De functioneel beheerders/AV-team zijn voor <Naam Opdrachtnemer> bereikbaar op werkdagen van XX:00 tot XX:00 uur, met uitzondering van binnen Nederland erkende feestdagen, voor het melden van storingen en het maken van afspraken over toegangsverlening tot de locaties.
- De Controlroom van <Naam Organisatie> is voor <Naam Opdrachtnemer> bereikbaar op werkdagen van 07:00 tot 21:00 uur, met uitzondering van binnen Nederland erkende feestdagen, voor het melden van storingen. Het maken van afspraken over toegangsverlening tot de locaties verloopt via Controlroom of AV-team.

Voor onderhanden incidenten worden, indien noodzakelijk, (per incident) door de lokale beheerder of de functioneel beheerder/AV-team maatregelen genomen om buiten de kantooruren door te kunnen werken.

4.2.3 Bereikbaarheid <Naam Organisatie> buiten kantoortijd

Naast de openingstijden zijn nog een aantal tijdstippen van belang.

Bereikbaarheid	op werkdagen 7:30 - 17:30, met uitzondering van binnen Nederland erkende feestdagen, gebruik met garantie (servicevenster);
Beschikbaarheid	werkdagen van 7:00 - 7:30 en 17:30 - 21:00, met uitzondering van binnen Nederland erkende feestdagen, gebruik zonder ondersteuning (systeemvenster); weekend- en feestdagen van 7:00 - 21:00 gebruik zonder ondersteuning(systeemvenster).
Calamiteit	ondersteuning bij calamiteiten; werkdagen van 7:00 - 7.30 en van 17:30 - 23:00 uur; feestdagen en in het weekend van 9:00 - 18:00 uur. De bereikbaarheidsdienst kan in geval van een calamiteit op een primair proces systeem benaderd worden via de boodschappendienst op (020) 1234567. U wordt dan binnen 30 minuten teruggebeld.

4.2.4 <Naam Opdrachtnemer> Servicedesk t.b.v. XXXX

Ten behoeve van de Rechtspraak wordt operationele ondersteuning geleverd door een Servicedesk van <Naam Opdrachtnemer>.

Servicedesk <Naam Opdrachtnemer> Incidenten, changes en helpdeskvragen aan de apparatuur:

- **Primaire ingang:** <Naam Opdrachtnemer> Support Desk;
- **Tel:**
- **Email:**

Incidenten welke door <Naam Organisatie> geclassificeerd zijn als type Major dienen altijd telefonisch te worden aangemeld. Incidenten welke door de <Naam Opdrachtgever> geclassificeerd zijn al Minor kunnen zowel telefonisch of per email worden gemeld.

Informatieverzoeken en klachten mailen. Op werkdagen tussen xx.00 en xx:00 uur worden mailberichten in behandeling genomen.

Bij spoedeisende aangelegenheden altijd telefonisch contact opnemen.

4.2.5 Overige contactpersonen binnen <Naam Opdrachtnemer> m.b.t. de dienstverlening

Naam	Functie	E-Mail	Telefoonnr.

4.2.6 Adres van <Naam Opdrachtnemer>

Kantooradres			
		website	www.<Naam Opdrachtnemer>.com
Postadres			

4.2.7 Wijziging van (contact)gegevens

Dit DAP is bedoeld om <Naam Organisatie> en <Naam Opdrachtnemer> optimaal te ondersteunen in het dagelijkse proces (o.a. incident afhandeling) m.b.t. de in paragraaf 1.3 benoemde Overeenkomst. Het is daarom van groot belang om alle gegevens vastgelegd in dit DAP zo actueel mogelijk te houden. Zowel <Naam Opdrachtgever> als <Naam Opdrachtnemer> wisselen daarom wijzigingen in o.a. contactgegevens zo snel als mogelijk met elkaar uit, doch minimaal 2 weken voor de daadwerkelijk ingang van de wijziging.

De Contractmanager van <Naam Organisatie> verwerkt de wijzigingen zo snel als mogelijk, uiterlijk binnen twee weken na het bekend worden van de wijziging en levert een nieuwe versie van de DAP op of een aangepaste versie van een der bijlagen behorende bij het DAP. Wijziging van één of meerdere bijlagen leidt niet tot een nieuwe versie van het DAP.

4.3 Incident management

Alle Incidentmeldingen op de door <Naam Opdrachtnemer> geleverde hardware en software worden centraal vanuit <Naam Opdrachtgever> gemeld. Bij een incident dient <Naam Opdrachtgever> de juiste en volledige informatie aan <Naam Opdrachtnemer> beschikbaar te stellen. <Naam Opdrachtnemer> is vanuit de dienst verantwoordelijk voor het herstel nadat <Naam Opdrachtnemer> de storing aan de hardware en/of software opgelost heeft.

4.3.1 Coördinatie incidentmeldingen

Incident management wordt primair uitgevoerd door <Naam Opdrachtgever>, secundair door <Naam Opdrachtnemer>.

Dit betekent dat <Naam Opdrachtnemer> niet voorziet in een eindgebruiker helpdesk.

Vanuit <Naam Opdrachtgever> zijn functioneel beheerders aangewezen welke incidenten kunnen melden bij <Naam Opdrachtnemer>. De gegevens van deze medewerkers worden vastgelegd in dit DAP.

De door <Naam Opdrachtgever> aangewezen functioneel beheerders stellen zover mogelijk vast waar en op welk component het incident betrekking heeft. Vervolgens wordt het geconstateerde incident door één van de medewerkers van <Naam Opdrachtgever> gemeld bij de van <Naam Opdrachtnemer>, conform de meldingsprocedure.

4.3.2 Reparatietijd

<Naam Opdrachtnemer> draagt er zorg voor dat binnen de hersteltijd en binnen het servicewindow het incident wordt opgelost. De ondersteuning die <Naam Opdrachtgever> ontvangt kan zowel telefonisch, remote als on-site zijn. Dit is afhankelijk van het type en de complexiteit van het incident.

Daarnaast bewaakt <Naam Opdrachtnemer> de dienst ten einde storingen snel te detecteren en op te lossen, waardoor de impact van de verstoring op de dienstverlening van de Rechtspraak beperkt blijft. De beschikbaarheid van de AV-omgeving van Rechtspraak staat altijd centraal.

4.3.3 Classificatie incident

Aan iedere incidentmelding wordt een classificatie toegekend door de Servicedesk van <Naam Organisatie>. De vaststelling van deze classificatie geschiedt na overleg met <Naam Opdrachtnemer> waarbij <Naam Organisatie> uiteindelijk de classificatie bepaalt, zijn hierin dus leidend.

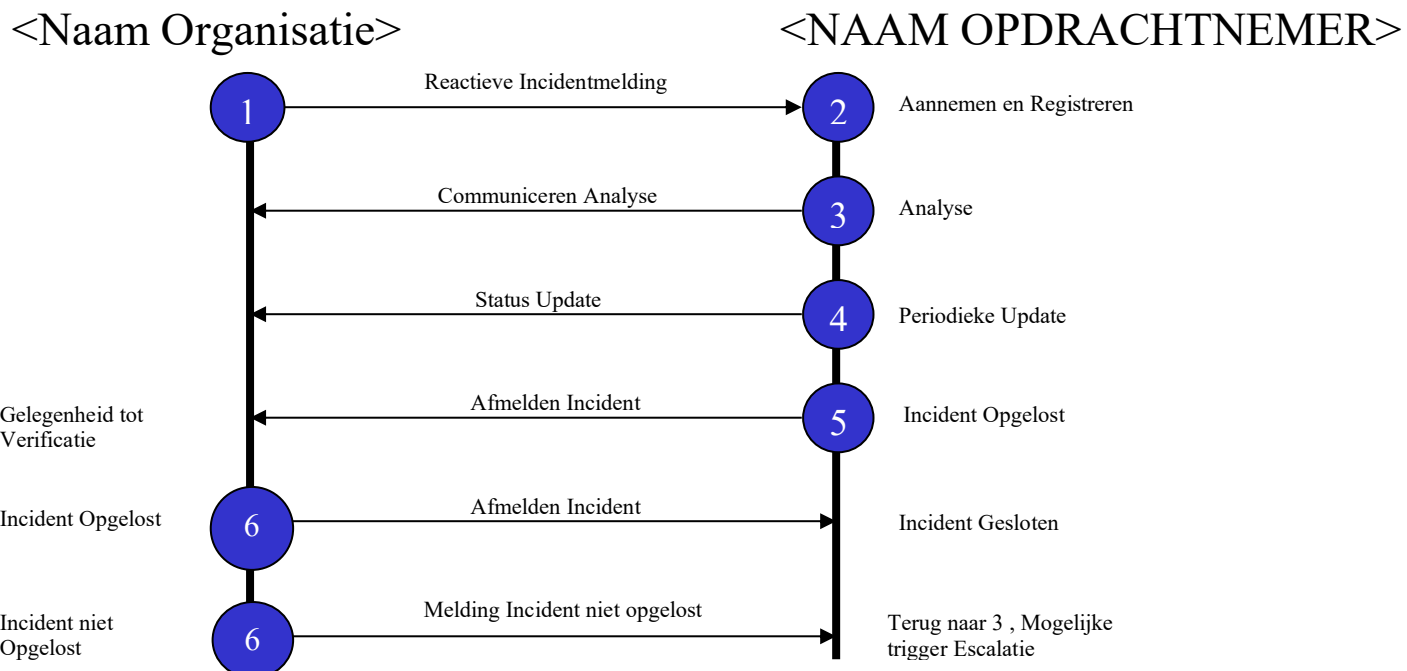
Aan de hand van deze classificatie voert <Naam Opdrachtnemer> de daarbij behorende activiteiten uit.

De classificatie biedt <Naam Opdrachtgever> de mogelijkheid om de oplossing van een incident op een ander tijdstip plaats te laten vinden, omdat het direct verhelpen van de storing een impact kan hebben op de dienstverlening aan de Rechtspraak.

<<Naam Organisatie> hanteert de hieronder genoemde incident classificatie:

Incident classificatie	Omschrijving
Major incident	Een incident dat leidt tot aanzienlijke (meer dan 25 gebruikers of een gehele locatie) uitval van de VOIP-omgeving van de Rvdr en/of belangrijke functionaliteiten hiervan.
Minor incident	Een incident die niet als Major Incident geclassificeerd kan worden.

4.3.4 Schematisch overzicht interfacemomenten incidentmelding



4.3.5 Interfacemomenten reactieve incidentmelding

1 <Naam Opdrachtgever> meldt een incident bij <Naam Opdrachtnemer>

Het primaire aanspreekpunt is de Servicedesk van <Naam Opdrachtnemer>. Aanvullende informatie

wordt, in overleg, uitgewisseld per telefoon, rechtstreeks in de gebruikte applicatie of e-mail. De melding kan 7x XX plaatsvinden. De Reactietijd gaat in zodra het incident telefonisch aangemeld is of het via e-mail gemelde incident door <Naam Opdrachtnemer> in het incidentmanagementsysteem is gelogd en <Naam Opdrachtnemer> het incidentnummer gemeld heeft aan <Naam Opdrachtgever>.

<Naam Opdrachtgever> verstrekt de volgende informatie bij het aanmelden van een incident:

1. Incident referentienummer <Naam Opdrachtgever>
2. Naam contactpersoon <Naam Opdrachtgever>
3. Telefoonnummer contactpersoon <Naam Opdrachtgever>
4. Naam contactpersoon <Naam Opdrachtgever> of het gerecht op locatie (eventueel)
5. Locatiegegevens contactpersoon <Naam Opdrachtgever> of het gerecht op locatie (gebouw, ruimte)
6. Telefoonnummer contactpersoon <Naam Opdrachtgever> of het gerecht op locatie (eventueel)
7. <Naam Opdrachtgever> geeft aan, op basis van de impact die het incident heeft op de klant, welke prioriteit het incident krijgt.
8. Type apparaat.
9. Omschrijving probleem.
10. Bijzondere omstandigheden? Werkzaamheden, spanningsproblemen?

2 Aannemen en registreren

De <Naam Opdrachtnemer> Servicedesk ontvangt de melding, registreert het incident en meldt het incidentnummer terug aan de <Naam Opdrachtgever>.

Behandeling Incident

Incidentafhandeling bestaat uit het repareren van apparatuur, software of gerelateerde componenten. Het functionele herstel van de apparatuur en programmatuur wordt gerealiseerd met het laden van de juiste configuratie op de apparatuur. Dit is een verantwoordelijkheid van <Naam Opdrachtnemer>.

3 Communiceren analyse

Binnen de reactietijd na melding van een incident wordt door de Servicedesk van <Naam Opdrachtnemer> een eerste analyse gecommuniceerd aan de melder van het incident. Daarin worden acties aangegeven welke uitstaan en wat de verwachte oplostijd is.

4 Statusupdate

De Servicedesk van <Naam Opdrachtnemer> informeert <Naam Opdrachtgever> periodiek over de voortgang en de status van het incident. <Naam Opdrachtnemer> gaat uit van een aantal momenten, te weten:

- Het moment van incidentmelding; (status nieuw)
- Technicus van <Naam Opdrachtnemer> neemt contact op met melder/functionaris van de <Naam Opdrachtgever> (status in behandeling).
- Aanvang herstelwerkzaamheden (op locatie) door <Naam Opdrachtnemer> technicus;

5 Incident opgelost

De <Naam Opdrachtnemer> Servicedesk meldt het incident af nadat de verstoring hersteld is. <Naam Opdrachtgever> kan de gereed melding direct accepteren waarop het incident wordt gesloten of kan overgaan tot verificatie van de oplossing. Het incident wordt pas gesloten, nadat <Naam Opdrachtgever> akkoord is met gereed melding.

6a Verificatie Incident opgelost

Indien er een verificatie gewenst is, wordt dit gedaan tijdens de afmelding door <Naam Opdrachtnemer>. <Naam Opdrachtgever> verifieert of het incident opgelost is, waarna <Naam Opdrachtnemer> over kan gaan tot sluiting van het incident. De Servicedesk van <Naam Opdrachtnemer> meldt elk incident telefonisch gereed aan de melder c.q. functionaris van <Naam Opdrachtgever>. De afmelding van het incident aan <Naam Opdrachtgever>, gebeurt direct na melding door de <Naam Opdrachtnemer> technicus aan de <Naam Opdrachtnemer> Servicedesk.

6b Melding Incident niet opgelost

Wanneer bij verificatie van de oplossing door <Naam Opdrachtgever> blijkt dat de apparatuur niet naar

behoren werkt, dan meldt <Naam Opdrachtgever> dit bij de Servicedesk van <Naam Opdrachtnemer>. Het incident wordt weer in behandeling genomen en het proces van oplossen wordt vervolgd. Tevens zal de <Naam Opdrachtnemer> Servicedesk nagaan of een escalatie noodzakelijk is. Een escalatie wordt in werking gesteld conform beschreven in hoofdstuk 6. Escalatie kan 7x XX-uur plaatsvinden.

4.3.6 Verantwoordelijkheden van <Naam Opdrachtgever>

- Is verantwoordelijk voor de juiste omgevingscondities van de apparatuur indien de apparatuur op locatie bij <Naam Opdrachtgever> geïnstalleerd is;
- Draagt zorg voor een juiste incidentanalyse;
- Meldt incident bij <Naam Opdrachtnemer>;
- Geeft informatie volgens de meldingsprocedure conform bijlage;
- Draagt zorg voor toegangsverlening op locatie indien deze werkzaamheden plaatsvinden op een locatie van de Rechtspraak;
- Geeft, indien van toepassing, schriftelijk akkoord op door <Naam Opdrachtnemer> aangeleverde fax/mail kosten.
- Geeft, bij werkzaamheden op een Rechtspraak-locatie schriftelijk akkoord middels servicebon op locatie, na gereed melding door <Naam Opdrachtnemer>;
- Signaleert een mogelijke escalatie en stuurt conform de escalatieprocedure zoals beschreven in hoofdstuk 6;
- Geeft ontvangen statusinformatie door aan de achterliggende organisatie;
- Stuurt eigen operationele organisatie aan.

4.3.7 Verantwoordelijkheden van <Naam Opdrachtnemer>

- Neemt incidentmelding aan;
- Registreert de incidentmelding in de incidentmanagementapplicatie;
- Vraagt de melder uit conform de meldingsprocedure conform bijlage;
- Analyseert de incidentmelding;
- Stuurt de eigen 1e en/of 2elijns organisatie aan;
- Bij de initiële melding wordt het incidentnummer van <Naam Opdrachtnemer> aan de <Naam Opdrachtgever> gemeld;
- Bewaakt de incidentmelding op contractuele verplichtingen;
- Signaleert een mogelijke escalatie en stuurt conform de escalatieprocedure zoals beschreven in hoofdstuk 6;
- Meldt de incidentmelding gereed;
- Laat de service bon accorderen door een door <Naam Opdrachtgever> aangewezen verantwoordelijke op locatie. In geval van apparatuur in het rekencentrum wordt de service bon per fax aangeboden aan de <Naam Opdrachtnemer> Servicedesk
- Sluit de incidentmelding af na akkoord melder/functionaris;
- Verwerkt gegevens ten behoeve van schriftelijke rapportage.
- Verzorgt aanmelding incidenten naar derden (bijv. NEC)
- Informeert <Naam Opdrachtgever> proactief bij gesignaleerd incident.

4.3.8 Ten onrechte incidentmeldingen

Ten onrechte incident meldingen zijn meldingen waarbij <Naam Opdrachtnemer> onterecht ingeschakeld wordt. Indien bijvoorbeeld blijkt dat het incident niet veroorzaakt wordt door hardware of software die door <Naam Opdrachtnemer> ondersteund wordt, behoudt <Naam Opdrachtnemer> zich het recht voor de gemaakte kosten aan <Naam Opdrachtgever> in rekening te brengen. Deze kosten worden door de <Naam Opdrachtnemer> technicus middels de servicebon inzichtelijk gemaakt.

Voordat <Naam Opdrachtnemer> in actie komt bij deze meldingen wordt er tevoren teruggekoppeld aan de functioneel beheerders. In overleg wordt bepaald waar het incident verder wordt behandeld.

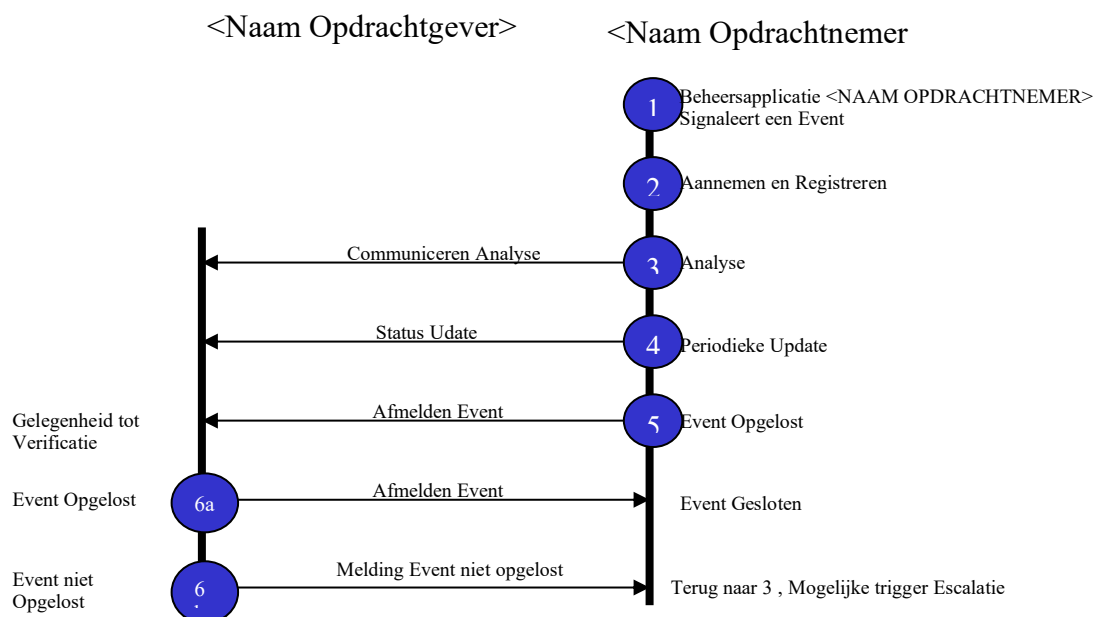
Bij remote assistentie dient het incidentnummer als leidraad voor het inzichtelijk maken van de kosten. Vanuit <Naam Opdrachtnemer> worden de ten onrechte meldingen gerapporteerd en besproken tijdens het dienstenniveau overleg

4.4 Event management

<Naam Opdrachtnemer> monitort XX x7 alle (indien technisch mogelijk) componenten van de AV voor Rvdr. Deze monitoring gebeurt op basis van SNMP-traps. Deze worden via de beheerverbinding doorgegeven aan de monitoring tools van <Naam Opdrachtnemer>.

Om event management volledig te kunnen uitnuttten moet beheerverkeer over het netwerk van <Naam Opdrachtgever> worden toegelaten. Hierover zullen binnen het project afspraken worden gemaakt.

4.4.1 Overzicht interfacemomenten events



4.4.2 Beschrijving Interfacemomenten events

1 Beheersapplicatie <Naam Opdrachtnemer> signaleert een Event

De te monitoren componenten zijn gekoppeld aan de beheersapplicaties van de Servicedesk <Naam Opdrachtnemer>. Indien zich in één van de componenten een Event voordoet, wordt dit Event automatisch aangeboden aan de op de <Naam Opdrachtnemer> Servicedesk aanwezige beheersapplicatie. De melding kan 7x24 plaatsvinden.

2 Aannemen en registreren

De Beheersapplicatie registreert het Event.

3 Analyse en Behandeling

Na registratie van een automatische melding van een major Event wordt een incident geregistreerd die door de Servicedesk van <Naam Opdrachtnemer> waarna de primaire contactpersoon van <Naam Opdrachtgever> wordt ingelicht en een eerste analyse wordt gecommuniceerd.

Daarin worden acties aangegeven welke uitstaan en wat de verwachte oplostijd is. De reactietijd gaat in zodra het event als incident geregistreerd is en de <Naam Opdrachtnemer> Servicedesk het incidentnummer gemeld heeft aan <Naam Opdrachtgever>.

Minor Events zonder impact of mogelijke impact op de bedrijfsvoering van de Rechtspraak worden niet gemeld aan <Naam Opdrachtgever>, tenzij de Servicedesk <Naam Opdrachtnemer> veelvuldig repeterende meldingen ziet. De Servicedesk <Naam Opdrachtnemer> informeert <Naam Opdrachtgever> dan wel en de Events opschalen naar incidenten. Alle incidenten worden gerapporteerd.

4 Periodieke Update

De Servicedesk van <Naam Opdrachtnemer> informeert <Naam Opdrachtgever> periodiek over de voortgang en de status van het Incident. <Naam Opdrachtnemer> gaat uit van een aantal momenten, te weten:

- Het moment van Incidentmelding; (status nieuw)
- Technicus van <Naam Opdrachtnemer> neemt contact op met functionaris van <Naam Opdrachtgever> (status in behandeling).
- Aanvang herstelwerkzaamheden (op locatie) door <Naam Opdrachtnemer> technicus;

5 Event opgelost

De <Naam Opdrachtnemer> Servicedesk meldt het Event af nadat de verstoring is hersteld. <Naam Opdrachtgever> kan de gereed melding direct accepteren waarop het Incident wordt gesloten of kan overgaan tot verificatie van de oplossing. Het Incident wordt pas gesloten, nadat <Naam Opdrachtgever> akkoord is met gereed melding.

6a Verificatie Event opgelost

Indien er een verificatie gewenst is, wordt dit gedaan tijdens de afmelding door <Naam Opdrachtnemer>. <Naam Opdrachtgever> verifieert of het Incident opgelost is, waarna <Naam Opdrachtnemer> over kan gaan tot sluiting van het Incident. De Servicedesk van <Naam Opdrachtnemer> meldt elk Incident telefonisch gereed aan de melder c.q. functionaris van <Naam Opdrachtgever>. De afmelding van het Incident, aan <Naam Opdrachtgever>, gebeurt direct na melding door de <Naam Opdrachtnemer> technicus aan de <Naam Opdrachtnemer> Servicedesk.

6b Melding Event niet opgelost

Wanneer bij verificatie van de oplossing door <Naam Opdrachtgever> blijkt dat de apparatuur of software niet naar behoren werkt, dan meldt <Naam Opdrachtgever> dit bij de Servicedesk van <Naam Opdrachtnemer>. Het Incident wordt weer in behandeling genomen en het proces van oplossen wordt vervolgd. Tevens gaat de <Naam Opdrachtnemer> Servicedesk na of een escalatie noodzakelijk is. Een escalatie wordt in werking gesteld conform beschreven in hoofdstuk 6. Escalatie kan 7x24 uur plaatsvinden.

4.5 Problem management

Om het beheer en onderhoud tegen de gewenste service levels te kunnen garanderen heeft <Naam Opdrachtnemer> o.a. een volgens de ITIL-methodiek ingericht Problem management proces.

Waar nodig inhoudelijke expertise leveren ten aanzien van het analyseren van problemen.

Problem management heeft als doel het actief voorkomen van incidenten cq het voorkomen van herhaal incidenten en daarmee het voorkomen van onderbrekingen in de dienstverlening.

4.6 IT operation, back-up and restore

4.6.1 Inleiding

Het doel van een back-up is om gegevens te kunnen herstellen in geval van verlies of vernieling van de originele media/data.

Back-ups worden gemaakt op de alle centrale componenten van de <systeem naam> zoals geleverd volgens de Overeenkomst.

Er wordt onderscheid gemaakt in 2 soorten back-ups. De configuratie back-up en de systeem back-up.

- Data back-up: Een reservekopie van alle configuratiedata van de diverse instellingen op de apparatuur
- Systeem back-up: Een reservekopie (image) van de installed base van de diverse servers welke gebruikt worden voor de dienstverlening. Onder installed base wordt onder andere het operating systeem en aanwezige applicaties verstaan, specifiek voor de hardware waar deze installed base op geïnstalleerd is.

Voor het opslaan/maken van de back-ups wordt gebruik gemaakt van een back-up server. Deze server is geplaatst op het DC in Groningen, fysiek gescheiden van de productieserver(s).

Binnen de door <Naam Opdrachtnemer> gerealiseerde technische oplossing dient van de volgende componenten een back-up gemaakt te worden:

- A
- B
- C
- D

4.6.2 Proces systeemback-up <Systeem XX>

Bij oplevering van de omgeving, is van de servers een initiële systeem back-up gemaakt. Dit wordt ook wel image genoemd. Een systeem back-up wordt door een Engineer van <Naam Opdrachtnemer> gemaakt.

De systeem back-ups worden op dezelfde wijze bewaard als configuratie back-ups en zijn opgeslagen op de back-up server.

Triggers systeem back-up:

- Vanuit change management
Op het moment dat er een change uitgevoerd wordt met betrekking tot de hardware en/of software van de servers wordt er indien noodzakelijk een nieuwe systeem back-up gemaakt. Onder software update wordt o.a. verstaan:
 - Nieuwe servicepack voor het Operating System.
 - Kritische updates voor het Operating System.
 - Nieuwe release voor de applicaties
 - Kritische updates voor de applicaties
- Vanuit releasemanagement
Indien een nieuwe release geïnstalleerd wordt, wordt ook een nieuwe systeem back-up gemaakt.

4.6.3 Proces data back-up

Om verlies van data te voorkomen moeten er dagelijks en wekelijks data back-ups gemaakt worden van de configuratie van de diverse servers.

<Naam Opdrachtnemer> zorgt ervoor dat deze geautomatiseerd worden weggeschreven op een specifiek daarvoor bestemde server in het afgesproken service window.

Voor het back-up proces komen de volgende applicaties in aanmerking:

- A
- B
- C
- D
- E

De onder punt 2 t/m punt 4 genoemde applicaties draaien op virtuele machines. De onder punt 1 en 5 genoemde applicatie zijn fysiek aparte servers.

Ten behoeve van de data back-up is er een automatisch back-up proces ingeregeld wat iedere week een back-up maakt van iedere machine en dagelijks een incremental back-up.

De back-ups worden weggeschreven op de back-up server.

4.7 Change management

Indien wijzigingen binnen de afgenomen dienstverlening gewenst zijn, kan <Naam Opdrachtgever> hiervoor een schriftelijk verzoek indienen bij de <Naam Opdrachtnemer> Servicedesk. Tevens beschikt <Naam Opdrachtgever> over de mogelijkheid om met behulp van de selfcare oplossing, een groot aantal configuratie wijzigingen uit te voeren waarvoor uiteraard geen changeverzoek behoeft te worden ingediend bij <Naam Opdrachtnemer>.

Het daarvoor benodigde formulier en te volgen procedures worden hieronder beschreven:

4.7.1 Trigger voor het proces

Voor de inleg van changes wordt gebruik gemaakt van het Change Formulier. Het formulier is als bijlage 1 toegevoegd aan dit document.

Het change proces kan gestart worden door inleg van een Change Formulier bij de <Naam Opdrachtnemer> Servicedesk via de mailbox support@<Naam Opdrachtnemer>.com . Hier vindt de controle op volledigheid en uitvoerbaarheid plaats. Daarbij wordt o.a. gekeken naar de levertijd van desbetreffende change. Hierna wordt de <Naam Opdrachtgever> geïnformeerd over het change-nummer waaronder het verzoek is geregistreerd en de uitvoerbaarheid van de order, wijziging of opzegging.

4.7.2 Change classificatie

Bij iedere change aanvraag wordt een classificatie toegekend door de <Naam Opdrachtnemer> Servicedesk. De vaststelling van deze classificatie geschiedt (eventueel) na overleg. Aan de hand van deze classificatie voert <Naam Opdrachtnemer> de daarbij behorende activiteiten uit. <Naam Opdrachtnemer> kent hierbij de classificatie standaard, minor en major change. Changes met een technisch karakter worden door <Naam Opdrachtnemer> uitgevoerd.

Change	Omschrijving
Standaard change	Change welke door de <Naam Opdrachtgever> zelf kan worden uitgevoerd met de daarvoor beschikbaar gestelde tooling. Dit betreft voornamelijk changes welke uitgevoerd moeten worden i.v.m. het wijzigen van eindgebruikers faciliteiten op toestelniveau.
Minor change (softwarematig)	Een op afstand door te voeren softwarematige aanpassing waarbij de impact beperkt blijft tot een gebruiker of een groep van gebruikers
Minor change (uitbreiding aantal werkplekken)	Uitbreiding van het aantal werkplekken (maximaal 10 per keer).
Major change	Alle overige changes. Hiervoor geldt een projectmatige aanpak waarbij u een aparte offerte krijgt met betrekking tot de kosten, de impact en het voorgestelde plan van aanpak.

Een Major Change kan na de impact analyse verder als Minor Change worden afgehandeld, maar ook als project geclassificeerd worden, hiertoe wordt dan een offerte uitgebracht. Per project wordt er een separate offerte aangevraagd en opgesteld.

4.7.3 Realisatietijd bij changes

De volgende realisatietijden zijn van toepassing op change aanvragen:

Soort	Realisatietijd
Standaard change	Op basis van beschikbaarheid capaciteit
Minor change (softwarematig)	Op basis van beschikbaarheid capaciteit
Minor change (uitbreiding aantal werkplekken max.10)	Op basis van beschikbaarheid capaciteit
Spoed change	Incidenteel op basis van beschikbaarheid capaciteit
Major change	Projectmatig op basis van offerte.

Indien er een conflict is tussen de wensdatum en de uitvoerbaarheid van de order, wijziging of opzegging zal dit aan de <Naam Opdrachtgever> gemeld worden.

Standaard en Minor Changes binnen de telefonie omgeving worden tijdens kantooruren en in overleg met de <Naam Opdrachtgever> uitgevoerd, mits de beschikbaarheid niet wordt geraakt Changes kunnen op verzoek van de <Naam Opdrachtgever> buiten kantoor tijden worden uitgevoerd tegen meerkosten. De kosten voor deze changes zijn in de PDC opgenomen.

4.7.4 Maintenance Window

Bij gepland onderhoud (Maintenance Window) worden de werkzaamheden volgens de overeengekomen afspraken vooraf door de <Naam Opdrachtnemer> Servicedesk aan <Naam Opdrachtgever> gemeld en gepland.

Het Maintenance Window en afspraken zijn als volgt:

Omschrijving	Afspraak
Periode waarin gepland onderhoud zal worden gepleegd (Minor/Major)	<i>Buiten</i> de normale kantoor tijden; - dinsdag tussen 18:00 - 20:00 uur; - andere momenten: alleen na onderlinge afstemming.
Kennis geven van urgent onderhoud i.v.m. werkzaamheden <Naam Opdrachtnemer>	Minimaal 24 uur van tevoren meldt <Naam Opdrachtnemer> aan <Naam Opdrachtgever> of gebruik gemaakt wordt van een onderhoudsvenster. Als er geen gebruik van het onderhoudsvenster wordt gemaakt hoeft er geen melding plaats te vinden.
Kennis geven gepland onderhoud i.v.m. werkzaamheden <Naam Opdrachtnemer>	Minimaal 5 werkdagen van tevoren meldt <Naam Opdrachtnemer> aan <Naam Opdrachtgever> of gebruik gemaakt wordt van een onderhoudsvenster. Als er geen gebruik van het maintenance window wordt gemaakt hoeft er geen melding plaats te vinden.
Kennis geven van urgent onderhoud i.v.m. werkzaamheden <Naam Opdrachtgever>	Minimaal 24 uur van tevoren meldt <Naam Opdrachtgever> aan <Naam Opdrachtnemer> of gebruik gemaakt wordt van een onderhoud venster. Als er geen gebruik van het onderhoud venster wordt gemaakt hoeft er geen melding plaats te vinden.
Kennis geven gepland onderhoud i.v.m. werkzaamheden <Naam Opdrachtgever>	Minimaal 5 werkdagen van tevoren meldt <Naam Opdrachtgever> aan <Naam Opdrachtnemer> of gebruik gemaakt zal worden van een onderhoudsvenster. Als er geen gebruik van het onderhoudsvenster wordt gemaakt hoeft er geen melding plaats te vinden.

4.8

Release management

Voor noodzakelijke/gewenste release upgrades geldt dat <Naam Opdrachtnemer> op verzoek van de Rechtspraak separaat offertes zal uitbrengen. <Naam Opdrachtnemer> zal de Rvdr actief adviseren aangaande de noodzaak/wenselijkheid van nieuwe software releases gebaseerd op het advies van NEC.

<Naam Opdrachtnemer> stelt op verzoek van de Rvdr tweemaal per jaar haar apparatuur in het testlab ter beschikking aan de Rvdr. <Naam Opdrachtnemer> zal ervoor zorg dragen dat deze apparatuur zover als mogelijk voorzien is van een gelijkwaardige configuratie als die van de Rvdr.

<Naam Opdrachtnemer> biedt daar waar gewenst ondersteuning tijdens het testen of zal op verzoek van de Rvdr het testen uitvoeren tegen een passende vergoeding, vooraf te offren.

Regulier zullen deze patches en Maintenance Releases 2x per jaar getest en beschikbaar worden gesteld. Urgente Releases worden direct getest en ter beschikking gesteld.

<Naam Opdrachtnemer> zorgt voor technische testen en acceptatie, <Naam Opdrachtgever> is verantwoordelijk voor functionele en gebruikers testen en acceptatie.

Nieuwe software releases vanuit de leverancier worden na ontvangst bij <Naam Opdrachtnemer> eerst getest in de Lab omgeving van <Naam Opdrachtnemer>. Na het succesvol doorlopen van deze testen kan de software beschikbaar gesteld worden voor de Rvdr. Als in onderling overleg wordt besloten dat de Rvdr de nieuwe software releases zal gaan krijgen, zal <Naam Opdrachtnemer> gezamenlijk met de Rvdr de software testen zoals in testprocedure hierboven is beschreven.

De changes worden vooraf bij <Naam Opdrachtgever> ingediend en geaccordeerd conform het Changeplan Template zoals in Bijlage 1 Documenten is opgenomen.

4.8.1 Schematisch overzicht interfacemomenten standaard/minor changes

4.8.2 Interfacemomenten

1 Aanvraag standaard/minor change

Aanvraag <Naam Opdrachtgever>: Een geautoriseerde contactpersoon stuurt middels het Change Formulier een aanvraag voor een Minor Change naar de <Naam Opdrachtnemer> Servicedesk. Het formulier dient volledig ingevuld te zijn. De aanvraag wordt per mail ingediend bij de Servicedesk van <Naam Opdrachtnemer>. De doorlooptijd gaat in na registratie van de aanvraag. De <Naam Opdrachtnemer> Servicedesk controleert of alle gegevens om een order aan te nemen en later te factureren compleet zijn en registreert de Change aanvraag.

De <Naam Opdrachtnemer> Servicedesk maakt een impact analyse om te bepalen of een Change major of minor is.

<Naam Opdrachtnemer>: Een geautoriseerde contactpersoon stuurt middels het Change Plan document een aanvraag voor een Minor Change per mail naar het AV-team en een CC aan de Controlroom van <Naam Opdrachtgever>. Het control AV-team controleert of alle gegevens om de Change aan te nemen compleet zijn en registreert de Change aanvraag.

2 Orderbevestiging

Aanvraag <Naam Opdrachtgever>: De <Naam Opdrachtnemer> Servicedesk zal dezelfde dag terugkoppelen welke classificatie een Change meekrijgt. Als <Naam Opdrachtgever> niet genoeg of niet de juiste gegevens heeft aangeleverd, dan neemt <Naam Opdrachtnemer> contact op met de aanvrager van <Naam Opdrachtgever> om de juiste gegevens na te vragen. Dit gebeurt telefonisch en zal per e-mail bevestigd worden.

Minor changes worden tegen standaard tarief uitgevoerd zoals in de PDC opgenomen.

Aanvraag <Naam Opdrachtnemer>: Het AV-team van <Naam Opdrachtgever> geeft terugkoppeling als de Change aanvraag akkoord is. Als er onvoldoende of onjuiste gegevens zijn neemt <Naam Opdrachtgever> hierover contact op met de aanmelder van de Change.

3 Uitvoeren en testen

De Minor Change wordt in behandeling genomen en geanalyseerd door de <Naam Opdrachtnemer> Servicedesk. Hierna wordt er contact opgenomen met de contactpersoon binnen <Naam Opdrachtgever>. Deze wordt gevraagd of men met de kosten akkoord gaat en de gevraagde wijziging wordt doorgesproken. Als dit akkoord is maakt de <Naam Opdrachtnemer> Servicedesk middels de verbinding contact met het te muteren component en start met de uitvoering.

4 Gereed melden

Na uitvoering wordt er weer contact opgenomen met de contactpersoon binnen <Naam Opdrachtgever> en wordt de wijziging gezamenlijk uitgetest.

5a Afmelden

Indien de Minor Change akkoord is, wordt de Change aanvraag afgesloten en wordt het facturatie proces getriggert.

5b Melding Change niet akkoord

Indien dit niet akkoord is wordt het benodigde aangepast en opnieuw getest (terug naar stap 3).

4.8.3 Schematisch overzicht interfacemomenten major changes

4.8.4 Interfacemomenten

1 Aanvraag Major Change (Project)

Aanvraag <Naam Opdrachtgever>: De aangewezen contactpersoon stuurt middels het Change Formulier Managed IPT een aanvraag voor een Major Change (verder te noemen: Project) naar de <Naam Opdrachtnemer> Servicedesk. Het formulier dient volledig ingevuld te zijn. De aanvraag wordt per mail ingediend bij de Servicedesk van <Naam Opdrachtnemer>. Doorlooptijd gaat in na registratie van de aanvraag. De <Naam Opdrachtnemer> Servicedesk controleert of alle gegevens om de Change Request te kunnen behandelen en later te factureren compleet zijn en registreert de Change aanvraag.

Aanvraag <Naam Opdrachtnemer>: De aangewezen contactpersoon stuurt middels het Change Plan document een aanvraag voor een Major Change (verder te noemen: Project) naar het AV-team en een CC aan de Controlroom van <Naam Opdrachtgever>. <Naam Opdrachtgever> controleert of alle gegevens van de Change compleet zijn en verzoekt <Naam Opdrachtnemer> om een offerte uit te brengen.

2 Uitbrengen offerte

<Naam Opdrachtnemer> brengt naar aanleiding van de ingeleide Change Request een offerte uit aan de Rvdr. De offerte wordt door de servicemanager doorgesproken met <Naam Opdrachtgever>.

3 Acceptatie Offerte

Indien <Naam Opdrachtgever> akkoord gaat met de uitgebrachte offerte wordt de offerte ook door <Naam Opdrachtgever> ondertekend, en aan de servicemanager overhandigd.

4 Orderbevestiging

De order wordt door <Naam Opdrachtnemer> in behandeling genomen. De servicemanager stelt een orderbevestiging op. Het ordernummer wordt per mail teruggekoppeld aan de genomineerde contactpersoon van <Naam Opdrachtgever> en wordt gedurende het leverproces gebruikt als referentie voor het betreffende project.

Tevens koppelt de servicemanager de naam van de ordercoördinator of projectmanager terug die het project zal begeleiden. Deze projectleider of ordercoördinator is tot en met het moment van ondertekening van het Protocol van Oplevering voor het project het primaire aanspreekpunt voor <Naam Opdrachtgever>. Detailafspraken over de wijze van implementatie van het project worden vastgelegd in het door de projectmanager op te stellen Plan van Aanpak

5 Projectafstemming

Gedurende implementatie van het project vindt overleg en afstemming plaats tussen de projectmanager en <Naam Opdrachtgever>

6 Aanbieden Protocol van Oplevering

Na afronding van de werkzaamheden en succesvolle uitvoering van het test en acceptatieplan biedt de projectmanager het protocol van oplevering ter ondertekening door de Servicemanager en de genomineerde contactpersoon van <Naam Opdrachtgever> aan.

7 Ondertekening Protocol van Oplevering

Indien het resultaat van het project akkoord is, wordt het Protocol van Oplevering door de servicemanager, de projectmanager en de genomineerde contactpersoon van <Naam Opdrachtgever> ondertekend. De Change Request wordt afgesloten en het factuurproces wordt getriggerd.

4.9 Configuration & Asset management

Om het onderhoud tegen de gewenste service levels te garanderen, dienen de CMDB gegevens up-to-date te zijn.

<Naam Opdrachtnemer> houdt haar eigen CMDB bij en deelt deze met <Naam Opdrachtgever>. <Naam Opdrachtnemer> zal de CMDB indien gewenst beschikbaar stellen in Excel formaat via Email.

In dit hoofdstuk worden de rollen en verantwoordelijkheden van zowel <Naam Opdrachtnemer> als <Naam Opdrachtgever> beschreven zodat het onderhoud geborgd kan worden.

4.9.1 Configuratie Items

Alle Configuratie Items die deel uitmaken van de dienst, zoals benoemd in Bijlage 4 worden vastgelegd in een configuratie management database (CMDB). Dit geldt voor alle Configuratie Items die bij de initiële installatie geleverd zijn door <Naam Opdrachtnemer> uitgezonderd de toestellen.

Wijzigingen op de Configuratie Items dienen door beide partijen uitgewisseld te worden. De minimaal geregistreerde gegevens van de Configuratie Items zijn:

- Adresgegevens apparatuur
- Type IT component
- Fabrikant
- Serienummer
- Productomschrijving

4.9.2 Informatie uitwisseling <Naam Opdrachtnemer> – <Naam Opdrachtgever>

Tijdens het dienstenniveau overleg tussen de servicemanager en <Naam Opdrachtgever> kan op verzoek van <Naam Opdrachtgever> een overdracht plaats vinden van de bij <Naam Opdrachtnemer> geregistreerde CI gegevens.

4.10 Capacity management

Het capacity management binnen de dienst beperkt zich tot binnen de dienst opgenomen componenten.

- CPU Capaciteit
- Poort Capaciteit
- Disk Opslag Capaciteit
- Aantallen Licenties

De tijdens het dagelijkse beheer opgeslagen gegevens worden geanalyseerd. Analyse van de huidige telefonie omgeving kan leiden tot het nemen van efficiency maatregelen of bestelling van aanvullende componenten of licenties. Tevens zal tijdens het kwartaaloverleg inzicht worden verkregen in toekomstige uitbreidingen die van invloed zijn op de capaciteit van de beheerde componenten.

<Naam Opdrachtnemer> zal <Naam Opdrachtgever> ondersteunen bij het opstellen van een capaciteitsplan <Naam Opdrachtgever> is verantwoordelijk voor het opstellen van het plan.

4.11 Availability management

Met de <Naam Opdrachtnemer> dienst Actieve Monitoring zal <Naam Opdrachtnemer> alle IPT devices binnen de communicatieoplossing van de Rvdr bewaken. Dit gebeurt het automatisch ontvangen en analyseren van SNMP-berichten, deze monitoring wordt uitgevoerd onder het ITIL proces Event management.

- Door Actieve Monitoring zal in veel gevallen al vooraf gesignaleerd kunnen worden als de beschikbaarheid van de dienstverlening onder de norm dreigt te raken, waardoor vroegtijdig passende maatregelen getroffen kunnen worden. Zo kunnen (dreigende) incidenten worden gesignaleerd en opgelost, vaak al voordat daar binnen <Naam Opdrachtgever> daadwerkelijk hinder door wordt ondervonden.
- Op basis van de beschikbaarheidsrapportages en analyses zullen door <Naam Opdrachtnemer> voorstellen worden opgesteld voor verdere waarborging en verbetering van de beschikbaarheid van de dienstverlening. Deze voorstellen zullen door de Service Level Manager met <Naam Opdrachtgever> worden besproken.
- Om de kans op verstoring van de beschikbaarheid, veroorzaakt door onderhoud, zo klein mogelijk te houden, zal regulier onderhoud in overleg met <Naam Opdrachtgever> worden ingepland tijdens het maintenance window (buiten kantoor tijd).
- <Naam Opdrachtnemer> zal door regulier onderhoud en het tijdig installeren van software patches en updates, de in de dienstverlening gebruikte software release actueel houden. Door de software actueel te houden wordt de beschikbaarheid en een snel herstel van eventuele onbeschikbaarheid van de dienstverlening vergroot. Bij security patches volgt <Naam Opdrachtnemer> de richtlijnen van de leverancier.

4.12 Continuity management

<Naam Opdrachtnemer> zal <Naam Opdrachtgever> ondersteunen bij het opstellen en realiseren van een continuïteit plan en het daarvoor beschikbaar stellen van de benodigde middelen. <Naam Opdrachtgever> is verantwoordelijk voor het opstellen van het plan.

4.13 Security management

Security management maakt deel uit van de door <Naam Opdrachtnemer> aangeboden dienstverlening en bestaat uit:

4.13.1 Toegankelijkheid systemen:

- <Naam Opdrachtgever> zal erop toezien dat ongeautoriseerde personen geen toegang hebben tot de centrale hardware welke gebruikt wordt voor de dienstverlening.
- Geautoriseerde remote toegang tot de systemen van <Naam Opdrachtgever> middels een registratie logging.
- De logging van activiteiten op de systemen ten behoeve van Rvdr. Overzicht van wie en wanneer, is op verzoek van Rvdr beschikbaar
- Toegankelijkheid voor derden, <Naam Opdrachtnemer> is verantwoordelijk voor:
 - Indien noodzakelijk voor de continuïteit van de dienstverlening behoudt <Naam Opdrachtnemer> het recht om de 3^e lijns (leverancier) tijdelijke toegang te geven op de systemen van <Naam Opdrachtgever> hetgeen uiteraard gebeurt in overleg met <Naam Opdrachtgever>. Toegang zal pas worden verleend na de uitdrukkelijke toestemming van <Naam Opdrachtgever>.
 - <Naam Opdrachtnemer> zal aan geen enkele derde partij informatie beschikbaar stellen welke afkomstig is van het netwerk van <Naam Opdrachtgever> zonder de nadrukkelijke toestemming van <Naam Opdrachtgever>.

- <Naam Opdrachtnemer> zal er voor zorg dragen dat alleen medewerkers met de juiste product certificering toegang krijgen tot de systemen van <Naam Opdrachtgever>.

4.13.2 Fysieke toegang tot locaties van de Rvdr

- De Rvdr is verantwoordelijk voor de fysieke toegangscontrole van de locaties met de hardware welke gebruikt wordt voor de dienstverlening.
- Alle medewerkers van <Naam Opdrachtnemer>, inclusief derden die werkzaamheden uitvoeren voor <Naam Opdrachtnemer>, die on-site activiteiten uitvoeren zijn in het bezit van een VOG verklaring en zullen deze op verzoek tonen.
- De procedure om een engineer van <Naam Opdrachtnemer> toegang te verlenen tot een locatie van de Rechtspraak-locatie is als volgt:
 - De <Naam Opdrachtnemer> maakt met de Rechtspraak (beheerder op locatie) de afspraak dat een engineer van <Naam Opdrachtnemer> een bezoek gaat brengen aan een Rechtspraak-locatie. De naam van de engineer; de geplande aankomsttijd en de verwachte doorlooptijd moeten daarbij bekend zijn.
 - Indien nodig brengt de functioneel beheerder/AV-team de lokale beheerder op de hoogte van het geplande bezoek.
 - De lokale beheerder geeft altijd een telefoonnummer door aan <Naam Opdrachtnemer>, waar vervolgens bilateraal mee afgestemd kan worden omtrent aankomsttijd, parkeren e.d.
 - De lokale beheerder meldt de bezoeker aan bij de receptie van de betreffende locatie
 - Bij aankomst op de locatie meldt de engineer zich (met geldig legitimatiebewijs), waarna de receptie hem/haar een tijdelijke toegangspas verstrekt
 - De lokale beheerder begeleidt de engineer naar de betreffende apparatuur
 - Na voltooiing van de reparatie meldt de lokale beheerder indien nodig de resultaten c.q. voortgang aan de functioneel beheerder, die de oplossing controleert.
 - De lokale beheerder ondertekent de <Naam Opdrachtnemer>-werkbbon, ontvangt een kopie/doorslag hiervan en begeleidt de engineer naar de receptie, waar de tijdelijke pas wordt ingeleverd
 - De lokale beheerder actualiseert de incidentadministratie met een logcomment (conform incidentproces).

4.13.3 Paswoorden en autorisaties:

- Password management. <Naam Opdrachtnemer> zal ervoor zorg dragen dat 1x per 2 maanden de passwoorden van de toegang tot de systemen van Rvdr worden gewijzigd. Een overzicht van deze wijzigingen kan Rvdr indien gewenst beschikbaar gesteld worden.
- <Naam Opdrachtnemer> legt de autorisatieniveaus van de diverse betrokken rollen vast in Identity and Acces Management (IAM)
- De Rvdr en <Naam Opdrachtgever> kunnen ten alle tijden het door <Naam Opdrachtnemer> uitgevoerde proces 'laten' controleren d.m.v. een audit procedure.

Virus en Malware:

- <Naam Opdrachtnemer> is verantwoordelijk voor het updaten van de McAfee virus en Malware protection suite. Rapportage hierover staat in de maandelijkse Service Rapportage.

4.14 Financial Management

De periodiek verschuldigde vergoedingen voor de dienst wordt conform Overeenkomst maandelijks vooraf in rekening gebracht. Indien aangevraagde changes invloed hebben op de periodiek verschuldigde vergoeding dan zal het bedrag van de periodiek verschuldigde vergoeding worden aangepast na de uitvoering van de change en worden gefactureerd bij de eerst volgende periodieke facturatie. De periodieke kosten worden vooraf gefactureerd.

Niet periodieke, dit zijn de changes die op verzoek van <Naam Opdrachtgever> zijn uitgevoerd worden achteraf gefactureerd, goedkeuring inclusief de daarbij behorende kosten vindt tijdens het Dienstniveau overleg plaats.

Facturatie van uitgevoerde changes vindt op een aparte factuur plaats.

De maandelijksse factuur zal verstuurd worden naar:

Factuurgegevens de Rvdr	
Naam	
Afdeling	<Naam Opdrachtgever>
Postadres	
Kenmerk klant	Ordernummer <Naam Opdrachtgever>
Contactpersoon	
Telefoon	

De maandelijksse factuur zal door de servicemanager worden opgesteld en indien gewenst besproken worden in het operationele overleg. Tijdens het operationele kan de servicemanager de factuur desgewenst specificeren.

5. Service Level Management

Bij service level management gaat het om die activiteiten die nodig zijn om nieuwe of te wijzigen IT-diensten te kunnen ontwerpen zodat de Rvdr krijgt wat zij nodig heeft voor hun nieuwe of gewijzigde bedrijfsproces of dienst.

Binnen service Level Management vallen de volgende processen:

- Reporting
- Service Levels Dienst Telefonie
- Klanttevredenheid
- Leverancier management
- Overlegstructuur
- Producten en Diensten Catalogus

Na oplevering vanuit het implementatie project zal in eerste instantie op maandelijkse basis een dienstenniveau overleg gehouden worden. Nadat alle processen in place zijn, de documentatie gereed is en de dienstverlening stabiel is zal dit in gezamenlijk overleg over gaan in een kwartaaloverleg. In het dienstenniveau overleg zullen de navolgende zaken worden besproken:

- Resultaten van de afgelopen maanden aan de hand van de rapportages;
- Resultaat van verbeteracties en/of verbeteringen, indien van toepassing;
- Eventuele gewenste aanpassingen DAP en SLA.
- Facturering
- Configuration Management, als onderdeel van het dienstenniveau overleg wordt de inhoud van de CMDB besproken met <Naam Opdrachtgever>

5.1 Reporting

Uitgangspunten van de rapportage:

- Rapportage heeft tot doel aan <Naam Opdrachtgever> aan te tonen met welk resultaat de Dienstverlening door <Naam Opdrachtnemer> is uitgevoerd.
- <Naam Opdrachtnemer> beschikt over meetmethodes waarmee voor elk service level, zoals vastgelegd in deze SLA, wordt aangetoond of de vereiste waarde over de betreffende rapportageperiode gehaald is.
- <Naam Opdrachtnemer> rapporteert over alle service levels in de SLA.
- Aan de basis van de rapportages liggen door <Naam Opdrachtnemer> verzamelde meetdata.
- <Naam Opdrachtnemer> bewaart de meet- en registratiedata gedurende een periode van ten minste 12 maanden na de totstandkoming ervan en zal deze, op verzoek van de Rvdr, voor een externe audit ter beschikking stellen.
- <Naam Opdrachtnemer> stelt de Rvdr in staat een externe audit uit te laten voeren op de meetresultaten.
- Rapportage over Calamiteiten zal afhankelijk van de aard en omvang separaat aan de Rvdr geschieden.
- Aspecten op het niveau van beveiliging (bv update antivirus)

De meetmethodes op basis waarvan de rapportages worden opgesteld voldoen minimaal aan de volgende criteria:

- Alle in de SLA opgenomen service levels worden gemeten.
- Indien noodzakelijk vinden metingen, in overleg met <Naam Opdrachtgever>, plaats op basis van een representatieve steekproef.
- Metingen worden zodanig uitgevoerd, dat de Dienstverlening (service levels) niet nadelig beïnvloed wordt.
- Metingen worden, voor zover mogelijk, zodanig uitgevoerd, dat ze reproduceerbaar zijn ten behoeve van eventuele audits.

5.2 Vorm, frequentie en detailniveau van de rapportages

<Naam Opdrachtnemer> levert maandelijks de Service Level Rapportage aan in PDF formaat aan de SDM

van <Naam Opdrachtgever>.

<Naam Opdrachtnemer> rapporteert over de in de SLA vastgestelde KPI's en analyseert de KPI's die onder de afgesproken norm is.

5.3 Inhoud van de rapportages

5.3.1 Algemeen

De rapportage bevat in ieder geval de volgende onderdelen :

- **Service level rapportage:** overzicht van de gerealiseerde Beschikbaarheid en kwaliteit in de afgelopen maand, voor wat betreft alle onderdelen van de Dienstverlening;
- **Incident management:** overzicht van openstaande en afgesloten Incidenten in de afgelopen maand , verdeeld naar prioriteit en inclusief oplostijdsduur;
- **Problem management:** overzicht van openstaande en afgesloten problemen en, overzicht van het aantal problemen zonder known errors, aantal wijzigingsverzoeken dat vanuit problem management is geïnitieerd;
- **Change management:** overzicht van openstaande en afgesloten changes in de afgelopen maand , inclusief doorlooptijd en status in relatie tot de service levels. Dit overzicht bevat tevens een orderrapportage van uitgevoerde orders, lopende orders en de status ervan.
- **Configuratiemanagement:** overzicht van alle configuratie items (inclusief documentatie) die in beheer zijn bij <Naam Opdrachtnemer>. Dit overzicht hoeft niet maandelijks te worden opgeleverd, maar eenmaal per jaar. Dit overzicht dient ook te worden opgeleverd op verzoek van <Naam Opdrachtgever>.
- **Capaciteits management:** overzicht van trends in het gebruik van capaciteit van componenten in de infrastructuur, mogelijke knelpunten in de capaciteit. <Naam Opdrachtnemer> stelt eens per half jaar een capaciteitsprognose samen op basis waarvan de capaciteit van de bij <Naam Opdrachtnemer> in beheer zijnde voorzieningen kan worden bijgesteld. De <Naam Opdrachtnemer> ontwikkelt waar nodig prestatie modellen om de correlatie van werklast, prestatieparameters en capaciteit te kunnen verklaren.
- **Availability management:** overzicht van de beschikbaarheid van de centrale omgeving en de SV8100 op de locaties.

5.3.2 Specifiek Incident Management

Ten behoeve van de rapportage en eventuele nadere analyses over Incident Management registreert de <Naam Opdrachtnemer> minimaal de volgende gegevens:

- De unieke codering
- Status van het Incident
- De gegevens van de melder van het Incident
- Specificaties van de betrokken CI's
- Impact van het Incident
- Prioriteit van het Incident
- Datum en tijd van optreden van het Incident
- Datum en tijd van het in behandeling nemen van het Incident
- Datum en tijd van het opheffen/oplossen van het Incident
- Datum en tijd van akkoord op het afsluiten van het Incident
- Beschrijven van de genomen maatregelen voor het opheffen/oplossen van het Incident
- De oorzaak van het Incident
- Verwijzing naar een onderliggend probleem (zie problem management) indien bekend
- De relatie naar een wijziging, indien het Incident door een wijziging is veroorzaakt.

5.3.3 Specifiek Problem Management

Ten behoeve van de rapportage en eventuele nadere analyses over Problem Management registreert de <Naam Opdrachtnemer> minimaal de volgende gegevens:

- De unieke codering
- Status van het probleem
- De gegevens van de melder van het probleem
- Specificaties van de betrokken CI's
- Specificatie van gerelateerde Incidenten (inclusief de relatie naar continuïteitincidenten en beveiligingincidenten)

- Beschrijving van het probleem
- Impact van het probleem
- Prioriteit van het probleem
- Datum en tijd van het in behandeling nemen van het probleem
- Datum waarop verwacht wordt dat het probleem is opgelost
- Datum en tijd van akkoord op het oplossen van het probleem
- Beschrijven van de genomen maatregelen voor het opheffen/oplossen van het probleem
- Verwijzing naar het Wijzingverzoek voor de oplossing van het probleem (zie change management)

5.3.4 Specifiek Change Management

Ten behoeve van de rapportage en eventuele nadere analyses over Change Management registreert de <Naam Opdrachtnemer> minimaal de volgende gegevens:

- De unieke codering
- De aanvrager van de wijziging
- Specificaties van de CI's die worden gewijzigd, toegevoegd of verwijderd
- Reden waarom de wijziging wordt doorgevoerd
- Status van het probleem
- De gegevens van de melder van de wijziging
- Impact van de wijziging
- Prioriteit van de wijziging
- Gegevens van degene die de wijziging heeft goedgekeurd
- Gewenste realisatiedatum van de wijziging
- Overeengekomen realisatiedatum
- De werkelijke realisatiedatum
- De identificatie van gerelateerde wijzigingen

Resultaat van de uitgevoerde wijziging (bijvoorbeeld een succesvol opgelost/opgeheven probleem of Incident

5.4 Service levels dienst telefonie

De dienst telefonie wordt geleverd met de servicevorm Managed Service Comfort Continu plus. In onderstaande tabel zijn de SLA's van deze servicevorm samengevat.

Dienst	Service Level Element	Service Level
Response	Meldingsperiode	7x24
	Service window	7x24
Responsetijden	Tijdens kantooruren	30 minuten
Hersteltijden	Bij Minor incident	Next Business Day (NBD)
	Bij Major incident	Binnen 4 klokuren
Mutaties/changes	Minor change	Op basis van beschikbaarheid capaciteit
	Major change	O.b.v. offerte
	Projecten	O.b.v. offerte

5.5 Klanttevredenheid

Buiten optimalisatie op het gebied van techniek zullen <Naam Opdrachtgever> en <Naam Opdrachtnemer> gezamenlijk effort steken in de verbetering van de klanttevredenheid. Dit gebeurt o.a. door de dienstverlening optimaal aan te passen aan de wensen van de eindgebruiker.

Vragen, wensen en klanttevredenheid zullen op verschillende manieren worden gemeten/geïnterviewd o.a. door een jaarlijkse klant tevredenheidsmeting uitgevoerd door <Naam Opdrachtgever>. <Naam Opdrachtgever> rapporteert de resultaten aan de Rvdr en aan <Naam Opdrachtnemer>. <Naam Opdrachtnemer> zal gezamenlijk met <Naam Opdrachtgever> kijken hoe de dienstverlening verbeterd kan worden.

<Naam Opdrachtgever> zal op regelmatige basis de eindgebruikers vragen over hun tevredenheid over de door <Naam Opdrachtnemer> geleverde dienst. Deze vragen zullen dusdanig van aard zijn dat ook de kwaliteit van de dienstverlening van <Naam Opdrachtnemer> kan worden beoordeeld. <Naam Opdrachtnemer> zal aan dit onderzoek haar medewerking verlenen door, indien gewenst, het opleveren van specifieke vragen welke richting de eindgebruiker kunnen worden gebruikt voor het bepalen van de tevredenheid.

5.6 Leverancier management

<Naam Opdrachtnemer> levert zijn dienstverlening aan de Rvdr, leveranciersmanagement zal dus in zijn geheel door de Rvdr worden ingevuld. <Naam Opdrachtnemer> zal daar waar nodig ondersteuning bieden bij het inzichtelijk maken van zijn performance of kosten.

<Naam Opdrachtnemer> maakt bij de levering van deze dienst ook gebruik van de diensten van een derde partij. Het 4^e-lijns support deel voor o.a. incident- en change management wordt ingevuld door ondermeer NEC. <Naam Opdrachtnemer> zal het stuk leverancier management voor deze partij uiteraard voor zijn rekening nemen.

<Naam Opdrachtnemer> is verantwoordelijk voor de te volgen “Roadmap” met betrekking tot hardware en software en de daarmee samenhangende gevolgen voor de telefonie omgeving bij Rvdr. Hierbij wordt ondermeer bedoeld veranderingen in de te supporten versie van software, wijzigingen in hardware en applicaties.

5.7 Overlegstructuur

De overlegstructuur staat in detail beschreven in het overeengekomen Governance model.

- Dienstenniveau overleg
- Contract-Commercieel overleg
- Strategische Afstemming
- Strategische overleg

5.8 Dienstenniveau overleg

Het dienstenniveau overleg vindt in eerste instantie maandelijks plaats, daarna 1x per kwartaal en heeft als doel om alle operationele zaken te bespreken die lopen of gelopen hebben. Onderwerpen zijn ondermeer: Service Levels - Incidenten, Changes, Problems, Capacity, Availability)
Financiële afstemming - Aanrekening contract, disputen, buiten contract incidenten/changes.
Security incidenten. Deelnemers aan dit overleg zijn:

Tabel 1: Dienstenniveau overleg

Participanten	Functie	Verantwoordelijkheid
		Voorzitter & Notulist

5.9 Contract-Commercieel overleg

Dit overleg vindt iedere kwartaal plaats. Onderwerpen zijn onder meer contractuele issues, mutaties en uitbreidingen. Verslaglegging van dit overleg vindt plaats op roulatiebasis. Escalaties vanuit het dienstenniveau overleg gaan naar het contract-commercieel overleg.

Tabel 2: Contract-Commercieel overleg

Participanten	Functie	Verantwoordelijkheid
		Voorzitter

5.10 Strategisch overleg

5.10.1 Strategische Afstemming

Strategisch Afstemming richt zich op de ontwikkeling van de <Naam Opdrachtnemer> dienstverlening op middellange termijn en vindt ieder half jaar plaats.

Onderwerpen voor het overleg zijn ondermeer ICT ontwikkeling Rvdr, Commerciële escalaties, Innovatie, vernieuwingen en innovatie van diensten en algemene ontwikkelingen in het <Naam Opdrachtnemer> portfolio.

Escalatie vanuit het contract-commercieel overleg gaat naar de contactpersoon van Rvdr en de betrokken Manager van <Naam Opdrachtnemer>

Participanten	Functie	Verantwoordelijkheid

5.10.2 Strategische Overleg

Het strategisch overleg richt zich op de ontwikkeling van de <Naam Opdrachtnemer> dienstverlening op lange termijn en wordt in onderling overleg vastgesteld.

Mogelijke onderwerpen voor het overleg zijn ondermeer ICT ontwikkeling Rvdr, Procuratie, Businesscase, Capex.

Dit is het hoogste escalatie niveau. Escalatie vanuit de strategische afstemming gaat naar de contactpersoon van Rvdr en de betrokken Manager van <Naam Opdrachtnemer>

Participanten	Functie	Verantwoordelijkheid

5.11 Producten en Diensten Catalogus

De Producten en Diensten Catalogus (PDC) staat in detail beschreven in het overeengekomen PDC document.

6. Escalatie

6.1 Escalatieprocedure voor incident management

Definitie

Er is sprake van een escalatie wanneer <Naam Opdrachtnemer> niet in staat is een onder hun verantwoording vallend incident binnen de SLA met de Rvdr op een voor <Naam Opdrachtgever> acceptabele wijze op te lossen, of indien een gemaakte klantafpraak niet nagekomen kan worden en een (andere) afspraak niet gemaakt kan worden. Escalaties worden door betrokkenen altijd via de "lijn" op geëscaleerd.

Zowel <Naam Opdrachtnemer> als <Naam Opdrachtgever> kan een escalatie in gang zetten. De Servicedesk van <Naam Opdrachtnemer> zal in overleg met <Naam Opdrachtgever> treden en een escalatie naar hoger niveau opstarten. In onderstaand schema staan de betrokken afdelingen genoemd. De managementescalatie zal primair vanuit de Servicedesk van <Naam Opdrachtnemer> geïnitieerd worden.

<Schematische voorstelling>

In geval van een eerste escalatie en bij het opschakelen naar een hoger escalatieniveau zal <Naam Opdrachtgever> dit bij <Naam Opdrachtnemer> expliciet aangeven. De contactpersoon van de zijde van <Naam Opdrachtnemer> zal dan verder zorg dragen voor het bewaken van de escalatie en (doen) uitvoeren van de vereiste acties. De contactpersonen van <Naam Opdrachtgever> en <Naam Opdrachtnemer> zullen zo spoedig mogelijk en bij voortduring geïnformeerd worden over de voortgang van de escalatie.

De escalatieprocedure treedt in werking indien één van de partijen (<Naam Opdrachtgever> of <Naam Opdrachtnemer>) van oordeel is dat de andere partij:

- een slechte prestatie levert;
- gemaakte afspraken in het kader van de incidentafhandeling niet nakomt;
- een incident niet volgens de overeengekomen afspraken kan oplossen.

Tevens kan de escalatieprocedure in werking treden indien er sprake is van een calamiteit waarbij het incident de bedrijfsvoering van <Naam Opdrachtgever> in gevaar brengt. De escalatie vindt plaats volgens bovenstaand schema.

6.2 Contactgegevens t.b.v. escalaties

In de nu volgende tabel zijn de contactgegevens van de diverse betrokkenen binnen <Naam Opdrachtgever> aangaande het escalatieproces vastgelegd:

Escalatieniveau 1:

- Functioneel beheerder

Naam	Afdeling/Functie	Tel. Nr. / GSM	E-mail

Escalatieniveau 2:

- Management

Naam	Afdeling/Functie	Tel. Nr. / GSM	E-mail

Escalationiveau 3:

- Contract manager

Naam	Afdeling/Functie	Tel. Nr. / GSM	E-mail

Escalationiveau 4:

- Dienst verantwoordelijke

Naam	Afdeling/Functie	Tel. Nr. / GSM	E-mail

7. Raci tabel m.b.t. verantwoordelijkheden dienstverlening

R = Responsible, verantwoordelijk
A = Accountable, eindverantwoordelijk
C = Consulted, consulteren
I = Informed, infomeren

	De Rvdr/ <Naam Opdrachtge ver>	<Naam Opdracht nemer>
Dienstverlening	A	R
Beschikbaarheid 7 x 24 hrs		
Operationeel & technisch advies	I	R
Infrastructuur monitoring & alarmering	I	R
Evaluatiebeschikbaarheid	I	R
Capaciteit is beschikbaar in het juiste volume		
Forecast benodigde capaciteit	R	I
Capaciteit beschikbaar stellen in lijn met de Rvdr forecasts	I	R
Capaciteit is beschikbaar op het juiste moment		
Utilisatie monitoring	I	R
Management proces	I/C	R
Trendanalyse op de telefonie utilisatie data	I	R
Een verstoring in de infrastructuur moet opgelost worden binnen de gestelde Service Levels		
Oplossing Hardware & software incidenten	I	R
Oplossing Hardware & software incidenten in de Rvdr Infrastructuur	R	I
Voorkom, terugkerende, incidenten door het elimineren van de "root cause"		
Trendanalyse (root cause analyse) van terugkerende incidenten	I	R
Probleemoplossende services en producten in scope	I	R
Probleemoplossende services en producten out of scope	R	I
Hardware-elementen		
Configureren en test nieuwe infrastructuur voor operationele inzet	I	R

Bijlage 1 Documenten

Bijlage 2 Overzicht functies en contactpersonen

De volgende personen en/of afdelingen zijn gemachtigd/gerechtigd servicemeldingen bij de servicedesk van <Naam Opdrachtnemer> op te geven:

Geautoriseerde medewerkers voor melding incidenten en standaard en Minor changes:

Naam	Functie	Tel./ Fax / GSM	E-mail

Geautoriseerde medewerkers voor melding van 'Major Changes':

Naam	Functie	Tel./ Fax / GSM	E-mail

Primaire contactpersonen

Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	
Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	
Naam	
Afdeling	
Telefoon	
GSM	
Fax	
E-mail	
Secundaire contactpersoon	
Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	
Contractmanager <Naam Opdrachtgever>	

Naam	
Afdeling	
Telefoon	
GSM	
FAX	
E-mail	

- <Naam Opdrachtnemer> Support Desk;
 - Tel:
 - @mail: abcd@<Naam Opdrachtnemer>.com

Naam	Functie	E-Mail	Telefoon nr.

Bijlage 3 Locaties de Rvdr

Gegevens over de locaties worden overgenomen uit het locatieoverzicht CMDB.
Na oplevering van het project wordt deze aan deze DAP toegevoegd.

Bijlage 4 Componentenlijst

Onderstaand overzicht geeft aan welke onderdelen deel uitmaken van de in dit DAP beschreven werkwijze:

Datacenter Groningen:

Componenten	Type	Aantal	Eigendom / Investerings	Onderhoud	Looptijd Contract

Locatie Uniceflaan Utrecht:

Componenten	Type	Aantal	Eigendom / Investerings	Onderhoud

Overige Locaties:

Componenten	Type	Aantal	Eigendom / Investerings	Onderhoud
		1	Rvdr	<Naam Opdrachtnemer >

Bijlage 5 Gehanteerde definities (voorbeeld)

Service window	Het servicevenster is de periode waarin een systeem beschikbaar is, met garantie op het dienstenniveau (24x7)
Meldingsperiode	Het tijdvak waarbinnen <Naam Opdrachtnemer> bereikbaar is voor het ontvangen van incidentmeldingen.
Maintenance Window / onderhoudsvenster	De periode waarbinnen <Naam Opdrachtnemer> gerechtigd is gepland onderhoud uit te voeren zonder dat dit impact heeft op de berekening van de gerealiseerde beschikbaarheid.
Service niveau	Het service level met betrekking tot herstel en response tijden
Major incident	Verstoring in de dienstverlening die leidt of kan leiden tot uitval van de functionaliteit van het geheel van apparatuur (hardware) en/of programmatuur (applicatiesoftware). Bij uitval van meer dan 20% van deze functionaliteiten is sprake van een Major incident.
Minor incident	Verstoring in de dienstverlening die niet leidt of kan leiden tot uitval van de functionaliteit van het geheel van apparatuur (hardware) en/of programmatuur (applicatiesoftware).
Calamiteit	Storing die het gevolg is van externe oorzaken (Overmacht) en die niet door <Naam Opdrachtnemer> direct beïnvloedbaar is en die kan leiden tot uitval van het geheel van apparatuur en/of programmatuur en/of belangrijke functionaliteiten daarvan, waardoor bedrijfskritische onderdelen van de Raad voor de Rechtspraak niet kunnen functioneren. Hoewel de aard, plaats en tijd van de calamiteit zich niet laten voorspellen, behoren de onderstaande gebeurtenissen tot de meest waarschijnlijke: • grootschalige verstoring van de stroomvoorziening • grootschalige ongecontroleerde technische verstoringen • grootschalige wateroverlast • grote ongelukken/rampen (bijv. brand, dodelijke gevallen en gewonden) • terrorisme, waaronder (bom)aanslagen en ontvoering • pandemie.
Standaard change	Change welke door <Naam Opdrachtgever> zelf kan worden uitgevoerd met de daarvoor beschikbaar gestelde tooling. Dit betreft voornamelijk changes welke uitgevoerd moeten worden i.v.m. het wijzigen van eindgebruikers faciliteiten op toestelniveau.
Minor Change	Change die door de serviceorganisatie op afstand uitgevoerd kan worden of door de Raad voor de Rechtspraak d.m.v. self-care portal. Deze changes kunnen worden uitgevoerd zonder geplande uitval van functionaliteit. Ook wel bekend onder standaard changes waarvoor een procedure in de DAP wordt opgenomen. Grotere aantallen minor changes of minor changes die impact kunnen hebben op de bedrijfsprocessen cq doorlooptijd, worden in overleg met de Raad voor de Rechtspraak uitgevoerd en kunnen eventueel als major change worden behandeld. Minor changes die niet functioneel zijn worden door <Naam Opdrachtnemer> uitgevoerd.
Major Change	Alle overige changes Technische changes worden in alle gevallen door <Naam Opdrachtnemer> uitgevoerd.
Overeenkomst	Overeenkomst met referentienummer xxxxxxxx tussen de Raad voor de Rechtspraak en <Naam Opdrachtnemer>.
Responstijd / reactietijd	De tijd in tussen het moment van ontvangst van een storingsmelding bij de daartoe aangewezen meldpunten van <Naam Opdrachtnemer>/en het moment waarop <Naam Opdrachtnemer> start met de storingsanalyse.
Hersteltijd	De tijd in uren tussen het moment van ontvangst van een storingsmelding bij de daartoe aangewezen meldpunten van de Dienstverlener en het moment waarop de Dienstverlener het incident/verstoring functioneel hersteld meldt. Bij verschil van inzicht bepaalt de Raad voor de Rechtspraak welke prioriteit de major/minor incident heeft.
Systeembekabeling	Deze bestaat uit de bekabeling waarmee de apparatuur welke onder het contract valt met elkaar verbonden is. Voorwaarde is dat de bekabeling oorspronkelijk geleverd is door <Naam Opdrachtnemer> en zich beperkt tot verbindingen in één der SER ruimtes

	of daartussen. Gebouwbekabeling is hierbij uitgesloten.
Kantoortijden <Naam Opdrachtnemer>	Alle uren tussen 08:00 en 18:00 op maandag tot en met vrijdag, met uitzondering van in Nederland erkende feestdagen
Kantoortijden de Raad voor de Rechtspraak	Alle uren tussen 08:00 en 17:30 op maandag tot en met vrijdag, met uitzondering van in Nederland erkende feestdagen
Storingen	Het niet conform de overeengekomen technische en functionele specificaties functioneren van Apparatuur en/of Programmatuur.
Randapparatuur	betreft alle apparatuur welke niet onder de overeenkomst valt maar wel aangesloten is op de omgeving.
Functioneel hersteltijd	De tijd tussen het moment van initieel vastleggen van een storingsmelding bij de daartoe aangewezen meldpunt(en) binnen <Naam Opdrachtnemer> en het moment waarop <Naam Opdrachtnemer> de dienst functioneel heeft hersteld. Een incident kan zowel door de Raad voor de Rechtspraak als <Naam Opdrachtnemer> zelf worden ingelegd, op beide situaties is definitie van toepassing,
Functioneel herstel	Het herstellen van de dienstverlening d.m.v. een passende work-around (waardoor de basisfunctionaliteit wordt hersteld) waarna eventueel definitief herstel volgt.
Correctief onderhoud	Storingen oplossen ten behoeve van de beschikbaarheid van de dienstverlening. - het verhelpen van storingen binnen de overeengekomen service levels; - het afhandelen van garantieclaims in het 1^e contractjaar - het verrichten van reparaties
Meldtijd	Onder meldtijd wordt verstaan: het tijdstip waarop de klant een storing aan de leverancier heeft gemeld
Communicatiesysteem	Producten waarvoor <Naam Opdrachtnemer> en de Raad voor de Rechtspraak een overeenkomst hebben gesloten.
Herstelgarantie	Functioneel herstel van het communicatiesysteem
Klokuren	Alle uren van het etmaal, 7 dagen per week
Next Business Day (NBD)	De werkdag volgend op de dag van de incidentmelding. Werkdagen zijn maandag tot en met vrijdag van 08.00 tot 18.00 uur exclusief de erkende feestdagen.
Overmacht	Tekortkoming die de schuldenaar niet kan worden toegerekend, indien zij niet is te wijten aan zijn schuld, noch krachtens wet, rechtshandeling of in het verkeer geldende opvattingen voor zijn rekening komt.
Beheer	Betreft het actief monitoren van de omgeving, remote oplossen van incidenten en het doorvoeren van wijzigingen (changes).
Onderhoud	Onderhoud (Service of Break&Fix) betreft het (on-site) verhelpen van hardwarematige en/of softwarematige verstoringen. Tevens het informeren over en het beschikbaar stellen van relevante patches, software updates, etc.
Herhaal incident	Een gelijksoortig incident op hetzelfde component en/of werkplekconfiguratie met dezelfde aantoonbare oorzaak waardoor de overeengekomen minimale beschikbaarheid van de dienst niet wordt gehaald. Een herhaalincident wordt pas aangenomen indien het initiële incident is gesloten.
Beschikbaarheid	Beschikbaarheid van de door <Naam Opdrachtnemer> geleverde dienstverlening voor de gebruikersorganisatie van de Raad voor de Rechtspraak met de daartoe regulier aanwezige functionele werking en prestatie.
Programmatuur	Het geheel van de geleverde programmatuur inclusief documentatie en materialen en welke deel uitmaken van de overeenkomst
Servicedesk <Naam Opdrachtnemer>	Voorziening van <Naam Opdrachtnemer> waar incidenten worden geregistreerd en waarmee de Raad voor de Rechtspraak operationele contacten onderhoud.
RACI	Bij iedere combinatie van een naam en resultaat/proces/taak staat een letter, de R, A, C, of I. Deze letter staan voor de volgende termen: R (Responsible, NL: Verantwoordelijkheid) Degene(n) die het werk doet/doen. Verantwoording wordt afgelegd aan de persoon die accountable is. A (Accountable, NL: Eindverantwoordelijk) Degene die (ein)verantwoordelijk, bevoegd is. Als het erom gaat, moet hij/zij het eindoordeel vellen, veto-recht hebben. C (Consulted, NL: Raadplegen) Iemand die vooraf geraadpleegd. Is twee-richting communicatie. Deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan de beslissingen of acties geraadpleegd. I (Informed, NL: Informatie) Iemand die achteraf geïnformeerd wordt over de genomen beslissingen, over de voortgang, bereikte resultaten enz. Dit is één-richtingscommunicatie

