Gemeente Amsterdam

Dossier Afspraken en Procedures

Tussen <Leverancier> en Gemeente Amsterdam

Behorende bij de overeenkomst Geo-registraties informatievoorziening

Alle rechten voorbehouden. Niets van deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van de auteursrechthebbende.

Document controle

File Name:

Document geschiedenis

Auteur	Versie	Datum	Status	Commentaar
	0.1	xx/xx/20xx	Concept	

Document eigenaar	Leverancier

Referentie documentatie

Document Naam	Bestand identificatie

Review

Naam	Versie	Datum	Status	Commentaar
Leverancier				
Gemeente				

Verspreidingslijst

Naam	Functie	Actie
Leverancier		
Gemeente		

INHOUDSOPGAVE

1 Inleiding 4

2 Algemeen 4

2.1 Doel 4

2.2 Looptijd 4

3 Communicatie –overlegstructuur 4

3.1 Communicatie 4

3.2 Overleg 5

4 Proces afspraken en procedures Beheer 6

4.1 Afspraken algemeen 6

4.2 Klachten 6

4.3 Escalatie 6

4.3.1 Afspraak 7

4.3.2 Procedure 7

4.3.3 Rapportage 8

4.4 Service Desk 8

4.4.1 Afspraken 9

4.4.2 Procedure 10

4.5 Incident Management 10

4.5.1 Prioriteiten Incidenten 10

4.5.2 Procedure 11

4.6 Change Management 13

4.6.1 Algemeen 13

4.6.2 Prioriteit, Impact en Urgentie 13

4.6.3 Niet –standaard changes 13

4.6.4 Afspraken Niet –standaard changes 13

4.6.5 Procedure Niet –standaard changes 13

4.6.6 Standaard changes 14

4.6.7 Afspraken Standaard changes 14

4.6.8 Procedure 14

4.6.9 Urgente changes 15

4.6.10 Afspraken 15

4.6.11 Procedure 15

4.6.12 Escalatie Change afhandeling 16

4.7 Release Management 16

4.7.1 Afspraken 16

4.7.2 Procedure 16

4.8 Beveiliging/Security Management 16

4.8.1 Afspraken 16

4.8.2 Procedure 17

5 Akkoordverklaring 18

Bijlage 1: Rollen en functies 19

Bijlage 2: Communicatie en escalatie 20

Bijlage 3: Afkortingen en begrippenlijsten 21

Bijlage 4: Voorbeeld Service Management rapportage 24

Bijlage 5: Voorbeeld Major Incident Rapportage 24

Bijlage 6: Voorbeeld Major Incident Report 24

Bijlage 7: Change Request Formulier (RFC) 24

1 Inleiding

Het Dossier Afspraken en Procedures (DAP) is een onderdeel van de documentatie behorende bij de Overeenkomst betreffende de ICT Prestatie welke door Leverancier geleverd wordt en afgesloten is met Opdrachtgever. Dit DAP is een verdere uitwerking van de gemaakte serviceafspraken voor het realiseren van de overeengekomen dienstverlening en beschrijft de afspraken, procedures en algemene communicatieafspraken met betrekking tot het operationele beheer.

De gemaakte afspraken hebben onder andere betrekking op:

- De verschillende overlegvormen en hun agenda's;
- De deelnemers aan de overleggen;
- De verbindende afspraken tussen de beheerprocessen van Opdrachtgever en Leverancier;
- De escalatie procedure;
- Verantwoordelijken wijzigingsproces;
- Beveiliging.

[optioneel] Wijzigingen in het DAP kunnen in het Tactisch Overleg tussen Opdrachtgever en Leverancier worden overeengekomen. De nieuw vastgestelde DAP is vanaf moment van vaststelling van toepassing tussen Partijen en vervangt de vorige versie van het DAP.

2 Algemeen

2.1 Doel

Primair heeft dit DAP tot doel het vastleggen en actueel houden van de gemaakte afspraken, procedures en communicatiestructuur met betrekking tot de ICT Prestatie op operationeel niveau ten einde de geleverde dienstverlening zo effectief mogelijk te houden.

Secundair dient dit DAP om optimale afstemming te bereiken en duidelijkheid te scheppen in de te leveren diensten, de kwaliteit daarvan en door de afbakening van taken en verantwoordelijkheden tussen Leverancier en Opdrachtgever helder te maken.

2.2 Looptijd

Het DAP heeft dezelfde looptijd als de SLA.

3 Communicatie –overlegstructuur

3.1 Communicatie

De communicatie tussen Opdrachtgever en Leverancier verloopt in beginsel altijd tussen de de Service Desken van beide partijen.

3.2 Overleg

Tussen Opdrachtgever en Leverancier worden drie overlegvormen onderkend welke in onderstaande tabel zijn uitgewerkt.

Overleg	Onderwerpen	Frequentie	Deelnemers	Documenten
Strategisch	Output tactisch overleg Strategische ontwikkelingen	1x per jaar	Directie Gemeente Lijnmanagement Gemeente Account Director/Service Delivery Manager Leverancier Account Manager Leverancier	Notulen Besluiten/actielijst Ingebrachte stukken tactisch overleg Strategie/beleid Gemeente
Tactisch	Output operationeel overleg Lopende en geplande veranderingen Lopende overeenkomst/ dienstverlening Toekomstige ontwikkelingen	1x per 3 maanden	Lijnmanagement Gemeente Contract Management Gemeente Account Management Leverancier	Notulen Besluiten/actielijst Ingebrachte stukken operationeel overleg Capaciteits prognose Calamiteitenplan D/R Plan Retransitie strategie & Retransistie Plan
Operationeel	Operationele resultaten aan de hand van Service Management rapportage Ernstige problemen of afwijkingen op de geleverde dienstverlening	1x per maand	Service Management Gemeente Leveranciers Management Gemeente Service Management Leverancier	Notulen Actielijst Service Management rapportage

Tijdens het maandelijkse operationele overleg worden alle opgetreden incidenten en gedefinieerde problemen besproken. Aanvullende deelnemers aan dit overleg zijn onder andere de Problem Manager van Opdrachtgever en Leverancier. Indien noodzakelijk of gewenst nemen aan deze meeting ook personen uit de operationele afdelingen deel. Tijdens de incident of problem statusbesprekingen worden geen incidenten of problemen opgelost, maar vindt beoordeling en besluitvorming over de voortgang plaats.

4 Proces afspraken en procedures Beheer

4.1 Afspraken algemeen

Voor de dienstverlening is een Service Window op basis van het gekozen Service Level overeengekomen waarbinnen de dienstverlening bewaakt en beheerd wordt. Dit Service Window bestaat uit klokuren, uitgezonderd het overeengekomen Maintenance Window. Gedurende het Service Window is de Service Desk van Leverancier bereikbaar en heeft personeel gereed om direct te starten met het oplossen van Incidenten. Buiten het Service Window zijn de diensten beschikbaar maar wordt pas bij het aanbreken van het nieuwe Service Window gestart met oplossen van Incidenten.

4.2 Klachten

Indien een klacht of opmerking is op de werkzaamheden van Leverancier dan kan Opdrachtgever zich richten tot de Service Desk van Leverancier. Zij zullen de klantverantwoordelijke informeren en een onderzoek starten. Indien een klacht of opmerking niet naar tevredenheid van Opdrachtgever wordt afgehandeld kan Opdrachtgever escaleren middels de escalatieprocedure.

4.3 Escalatie

Escalaties kunnen op verschillende niveaus ontstaan en verschillende oorzaken hebben. Een escalatie kan bijvoorbeeld ontstaan doordat partijen een geschil hebben over de inhoud van de dienstverlening (waarbij eventuele aanpassingen buiten de competentie van de gesprekspartners liggen), in behandeling genomen Incidenten buiten de toegestane oplostijd (dreigen) te lopen of omdat een klacht van een functioneel beheerder niet naar behoren (binnen de overeengekomen Service Levels) is opgelost.

Het doel van het escalatieproces is het snel en adequaat reageren op (dreigende) verstoringen in het reguliere proces. De doelstelling van escalatie is om het proces, waar nodig, op gang te helpen of te bespoedigen om aan de overeengekomen ServiceLevel van de dienstverlening te kunnen blijven voldoen of om overschrijding van het Service Level tot een minimum te beperken. Bij escalatie wordt een beroep gedaan op additionele functionele kennis en/of hiërarchische bevoegdheid.

Binnen een escalatie worden diverse escalatieniveaus onderkend met als uiterste de crisiscommunicatie op het hoogste hiërarchische niveau van de betrokken organisaties. De escalatieprocedure kent een getrapte opzet naar een steeds hoger (functioneel of hiërarchisch) niveau waarbij onderscheid wordt gemaakt tussen het inlichten van het hogere niveau of interventie door het hogere niveau.

Ten behoeve van de interfaces op drie niveaus (strategisch, tactisch en operationeel) tussen Opdrachtgever en Leverancier is een escalatieprocedure opgesteld. Middels deze procedure is eenduidig vastgelegd welk escalatiepad gevolgd dient te worden en wie (functie en naam) binnen de organisatie van de wederpartij het gelijkwaardig escalatieniveau is. Indien één der partijen de escalatieprocedure in gang zet, volgt automatisch escalatie bij de wederpartij.

4.3.1 Afspraak

Ten aanzien van het kunnen initiëren van een escalatie zijn concrete criteria overeengekomen. Deze bestaan uit:

- Gemelde Incidenten met prioriteit 1 of 2 die buiten de oplostijd (dreigen) te lopen;
- Ongepland Onderhoud dat niet is aangemeld;
- Doorgevoerde Changes of releases die niet zijn aangemeld;
- Changes die uit de tijd lopen;
- Changes die verkeerd zijn doorgevoerd en tot Incidenten leiden;
- Niet aangemelde Changes vanuit Leverancier;
- Spoedchanges;
- Onbeschikbaarheid van de dienstverlening;
- Niet op tijd aangeleverde rapportages;
- Security breaches (beveiligingsinbreuken, niet nakomen van beveiligingseisen, inbraak op de dienstverlening, etc.);
- Calamiteiten.

4.3.2 Procedure

Indien op basis van een van de criteria een escalatie wordt opgestart zal dit, afhankelijk van het niveau waar de initiatie wordt gedaan, in eerste instantie een functionele escalatie naar de wederpartij betreffen.

4.3.2.1 Interne escalatie

In overleg tussen de direct operationeel betrokkene en de operationele manager binnen de eigen organisatie van Leverancier kan besloten worden tot het opstarten van een escalatieproces. Hierbij kan alleen binnen de eigen organisatie kan naar hoger niveau worden geëscaleerd (hierbij vinden dus geen diagonale escalaties plaats).

4.3.2.2 Externe escalatie

Tussen Opdrachtgever en Leverancier wordt gecommuniceerd op horizontaal niveau. Hiervan kan afgeweken worden indien in overleg wordt besloten tot andere niveaus van communicatie. Informatie van, en besluiten op hoger niveau worden steeds aan het onderliggend niveau doorgegeven. Een centrale rol bij escalatie bij Leverancier wordt ingevuld door de aangewezen regievoerders over de escalatie. Deze regievoerders:

- zorgen voor directe en snelle communicatiemogelijkheden;
- hebben een centrale rol bij het inlichtingen vragen en inlichtingen geven over de status van een incident;
- spreken met elkaar af op welke termijn antwoorden mogen worden verwacht en informatie wordt verstrekt (dit om Leverancier rust te gunnen in het oplossen van de opgetreden escalatie).

4.3.2.3 Escalatiemodel

Het te hanteren escalatiemodel is gelijk aan het governancemodel waarin zowel de horizontale en verticale escalatiepaden zijn aangegeven. De escalatie procedure wordt toegepast indien de ernst van de situatie de directe betrokkenheid van een ander niveau, noodzakelijk maakt. De volgende escalatieniveaus kunnen achtereenvolgens worden doorlopen:

[VOORBEELD] Escalatie niveaus bij Opdrachtgever:

1. Service Desk coördinator en/of Incident Manager
2. Manager Basisdiensten, Proces Manager of Contract Manager
3. Chief Information Officer

Escalatie niveaus bij Leverancier:

1. Service Desk coördinator en/of Incident Manager
2. Service Manager of Account Manager
3. Service Delivery Manager of Account Manager

Alle niveaus escaleren naar het eerstvolgende hogere niveau, naar inzicht van de betreffende medewerker. Niveau 1 en 2 escaleren naar het eerstvolgende hogere niveau wanneer Incidenten met prioriteit 1 niet binnen de afgesproken termijn opgelost dreigen te worden. Om onduidelijkheden te voorkomen worden bereikte overeenstemmingen schriftelijk/via e-mail vastgelegd. Deze bevat de volgende elementen:

- Te bereiken doel;
- Te nemen acties;
- Fasering en planning;
- Uitvoerenden.

4.3.3 Rapportage

Na elke escalatie volgt een escalatierapport en wordt in principe altijd door Leverancier opgesteld. Het rapport dient als input voor het escalatie-evaluatie-overleg dat hierop volgt. Indien meerdere leveranciers betrokken zijn bij de escalatie, zal Opdrachtgever Leverancier aanwijzen voor het opstellen van het rapport. Opdrachtgever zal na het ontvangen van het rapport het overleg initiëren en acties en/of verbeterpunten uitzetten en monitoren op de voortgang. Het escalatierapport wordt binnen 5 werkdagen na beëindiging van de escalatie elektronisch middels e-mail aan Opdrachtgever aangeleverd naar het tactische niveau.

In het rapport is opgenomen en uitgewerkt:

- Identificatie escalatie;
- Naam coördinator Leverancier;
- Naam coördinator van Opdrachtgever;
- Datum en tijd start escalatie;
- Datum en tijd einde escalatie;
- Initiator escalatie;
- Omschrijving escalatie;
- Historie;
- Oplossing en conclusie escalatie;
- Verbeterpunten waarbij aangegeven wordt waar deze zijn belegd en wanneer ingevuld dienen te zijn.

Over het bewaken van de voortgang van de verbeterpunten volgt wekelijks, uiterlijk vrijdagmiddag 12:00, een update door Leverancier aan het operationele escalatieniveau.

4.4 Service Desk

De Service Desk van Leverancier is het centrale en enige contactpunt voor Opdrachtgever Service Desk voor alle operationele communicatie over de dienstverlening en draagt zorg voor het herstel van de afgesproken dienstverlening volgens in de met Opdrachtgever overeengekomen SLA. Alle communicatie en meldingen zoals vragen, Incidenten, opdrachten of klachten die betrekking hebben op de dienstverlening, komen vanaf Opdrachtgever Service Desk. Opdrachtgevers Service Desk medewerkers

en de personen en/of afdelingen uit de tabel in de Communicatie en Escalatie bijlage zijn gerechtigd om Incidentmeldingen te doen.

In uitzonderlijke gevallen kan ook communicatie plaatsvinden tussen een Service Desk van een andere dienst van Opdrachtgever met de Service Desk van Leverancier waarbij altijd de Service Desk van Opdrachtgever over de communicatie wordt geïnformeerd.

4.4.1 Afspraken

De Service Desk voert de Nederlandse taal. Tweede en verdere lijnondersteuning mag anderstalig.

Tijdens het Service Window volgens het overeengekomen Service Level kan de Service Desk van Opdrachtgever bij de Service Desk van Leverancier terecht voor het volgende:

- Aanmaken/melden van Incidenten of Change;
- Indienen van verzoeken tot standaardwijziging;
- Niet standaard wijzigingsverzoeken;
- Terugkoppelen en afmeldingen van incidenten;
- Aanmelden van een klacht;
- Aanmelden van een vraag;
- Escalatie.
- Statusupdates Incident, Change, problem, klacht, escalatie of vraag;
- Opdrachtbevestiging;
- Site Survey rapport;
- Verwachte leverdatum opdracht of Change;
- Opleverdocumentatie;
- Communicatie omtrent gepland Onderhoud;
- Bezwaren/vragen gepland Onderhoud.

De openingstijden en bereikbaarheid op basis van de overeengekomen Service Level van de verschillende Service Desken is als volgt:

	Gemeente	Leverancier
Openingstijden : Telefoon : E-mail :	07:30 - 18:00 020- 2516161	xxxx

Bij telefonisch contact wisselen Opdrachtgever het ticketnummer uit. Bij e-mailcontact wordt onderstaande informatie uitgewisseld, of, indien bij telefonisch contact, verzameld ter beantwoording.

- Referentienummer van de meldende partij;
- Naam en telefoonnummer van de melder;
- Naam en telefoonnummer van de contactpersoon van de klant;
- E-mail adres van de melder;
- Dienst (Service) waarop het incident betrekking heeft:
- Prioriteit (door Opdrachtgever bepaald);
- Omschrijving van het incident;
- Start verstoring;
- Indien mogelijk, om welk configuratie item het gaat;
- De locatie van het configuratie item;
- Naam en telefoonnummer van de contactpersoon op locatie;

- Indien van toepassing de lijnbenaming van de vaste verbindingen en IP-nummers vermelden;
- Reeds ondernomen acties door de leverancier van perceel 2 of Leverancier;
- Bijzondere omstandigheden.

4.4.2 Procedure

De binnengekomen vragen, klachten of Incidentmeldingen worden voorzien van een ticketnummer en geregistreerd in de Service Management tool van Leverancier waarbij de Service Desk van Opdrachtgever bij aanmelden de prioriteit bepaald. Eventueel kan Opdrachtgever op een later tijdstip de prioriteit aanpassen. Een melding wordt afgewezen als de melder niet gerechtigd is een melding te maken en wordt erop gewezen de afgesproken procedure tussen Opdrachtgever en Leverancier te hanteren.

Indien een Incident wordt geconstateerd die de dienstverlening betreft, worden partijen (Opdrachtgever en Leverancier) hierover geïnformeerd. Nadat de informatie door beide partijen is doorgegeven wordt een uniek incidentnummer uitgewisseld waarmee de melding is vastgelegd bij zowel Opdrachtgever en Leverancier.

Binnen 15 minuten wordt een bevestiging van de melding per mail aan Opdrachtgever Service Desk gestuurd onder vermelding van het ticketnummer. Indien het ticket door de Service Desk van Leverancier als incident wordt uitgezet binnen het Incident Management proces van Leverancier zal, afhankelijk van de prioriteit van het incident en het overeengekomen Service Level die voor de dienstverlening is overeengekomen, Leverancier Opdrachtgever in de frequentie volgens het overeengekomen Service Level informatie verstrekken over de voortgang van het opheffen van de gemelde incident.

Indien een Incident is opgelost zal dit door de Service Desk van Leverancier worden doorgegeven aan de Service Desk van Opdrachtgever. In overleg worden het ticket en incident afgesloten waarbij Opdrachtgever het eindoordeel doet.

4.5 Incident Management

Incident Management betreft het zo snel mogelijk herstellen van de functionaliteit van de dienstverlening. Leverancier verzorgt binnen de dienstverlening de eerstelijns, tweedelijns en derdelijns ondersteuning.

Binnen Incident Management wordt onderscheid gemaakt in pro-actieve incident meldingen en reactieve incident meldingen. Pro-actieve incidenten zijn verstoringen die middels monitoring worden opgemerkt vanuit de processen zoals Availibility en Capacity Management maar nog niet leiden tot onderbrekingen. Reactieve incidenten zijn verstoringen aan de dienstverlening die onder andere zijn gemeld bij de Service Desk.

Voor beveiliging/security incidenten geleden afwijkende afspraken. Zie hiervoor het hoofdstuk Beveiliging/Security Management.

4.5.1 Prioriteiten Incidenten

Leverancier heeft een contactpersoon aangesteld die door Opdrachtgever aangesproken kan worden over de voortgang c.q. afhandeling van een melding of incident. Hiernaast heeft Opdrachtgever de mogelijkheid in de voortgang te volgen middels een inkijkmogelijkheid in het Incident management systeem van Leverancier.

Aanmelden van Incidenten en het doen van navraag op de voortgang kan middels:

- Een door de Leverancier geboden webbased applicatie;
- Een E-mail voorziening (inclusief bijlagen);
- Telefoon.

Bij het aanmelden van het Incident bepaalt Opdrachtgever de prioriteit waarmee deze in behandeling genomen dient te worden. De hierbij geldende criteria op de maximale doorlooptijd, klokuren, etc. zijn op basis van het afgenomen Service Level en de SLA. Het bepalen van de prioriteit gebeurt aan de hand van de tabel in de SLA.

Opmerking: indien Leverancier zelf een onderbreking signaleert terwijl Opdrachtgever deze niet meldt, geldt dezelfde Hersteltijd.

4.5.2 Procedure

Het afhandelen van Incidenten kent de volgende stappen:

- Aanmelden en registreren van incident middels de Service Desk;
- Voortgang van een Incident;
- Afsluiten van een Incident.

4.5.2.1 Aanmelden en registreren Incident

Bij het aanmelden van Incidenten worden de volgende twee situaties onderscheiden:

1. Een Incident is geconstateerd door Opdrachtgever en wordt door aangemeld bij Leverancier. Hier is sprake van een reactieve melding.
2. Een Incident is geconstateerd door Leverancier zelf. Hier is sprake van een proactieve melding.

Een Incidentmelding vanaf Opdrachtgever wordt altijd bij de Service Desk van Leverancier gedaan. De Service Desk van Leverancier onderzoekt de melding of deze door de Service Desk zelf opgelost kan worden. Indien de Service Desk de melding niet zelf kan oplossen wordt de melding "doorgezet" naar het Incident Management proces van Leverancier waarna het incident in behandeling wordt genomen. In dit stadium zijn twee registraties aanwezig:

1. De Call (melding) bij de Service Desk van Leverancier en welke voorzien is van een Call-nummer; en

2. Het aangemaakte incident door de Service Desk van Leverancier en welke voorzien is van een incidentnummer.

Beide nummers worden aan de Service Desk van Opdrachtgever gecommuniceerd.

4.5.2.2 Voortgang van een Incident

Over de voortgang bij het oplossen van een Incident wordt de Service Desk van Opdrachtgever volgens de tijdsinterval behorende bij het overeengekomen Service Level en de prioriteit die aan het Incident is toegekend, geïnformeerd. Dit gebeurt totdat het Incident is opgelost naar het oordeel van Opdrachtgever en de dienstverlening weer volledig beschikbaar is.

Wanneer het Incident niet binnen de overeengekomen Hersteltijd kan worden opgelost wordt de Service Desk van Opdrachtgever hier zo snel mogelijk van in kennis gesteld. Vervolgens zal in overleg worden besloten welke vervolgacties genomen moeten worden om het Incident al dan niet tijdelijk of permanent te verhelpen en de geschatte tijdsduur hierin. De Incident Manager van Opdrachtgever zal als gevolg van het overschrijden van de oplostijd eventueel besluiten om te escaleren.

Over de voortgang van een Incident wordt door beide partijen de volgende informatie uitgewisseld:

- Het Incidentnummer waaronder het Incident is geregistreerd;
- Een beschrijving van de verrichte handelingen sinds de laatste statusmelding en de vervolgacties;
- Indien mogelijk wordt een tijdsindicatie voor een oplossing gegeven.

4.5.2.3 Afmelden van een Incident

Een Incident wordt in overleg met Opdrachtgever definitief afgesloten waarbij Opdrachtgever het eindoordeel doet. De afmelding wordt gedaan per e-mail afgemeld bij de Service Desk van Opdrachtgever. Indien het een Incident met de prioriteit 1 betreft wordt deze tevens telefonisch afgemeld en volgt binnen 3 werkdagen een Major Incident Rapportage welke door Leverancier wordt opgesteld. Binnen 1 werkdag heeft Opdrachtgever de mogelijkheid het Incident te laten heropenen indien de oplossing niet volstaat.

4.5.2.4 Wederkerende Incidenten

Elk Incident wordt door Leverancier geregistreerd met een uniek Incident nummer. Een gesloten Incident nummer wordt niet heropend maar, indien het gesloten Incident weer optreedt, wordt hiervoor een nieuw Incident aangemaakt. De Incident nummers van repeterende Incidenten worden vervolgens aan elkaar gekoppeld. Hiermee kan Leverancier zien of dit als een probleem behandeld moet worden.

Indien sprake is van periodieke of terugkerende storingen zal Leverancier na overleg met Opdrachtgever een aanvullend gericht onderzoek uitvoeren om te bepalen welke maatregelen genomen dienen te worden om de periodieke storingen in de toekomst te voorkomen. Dit onderzoek wordt uitgevoerd indien binnen een week tweemaal een storing wordt gemeld op dezelfde dienstverlening en de oorzaak van de storing bij Leverancier ligt. Waar mogelijk zal Leverancier een alternatief aanbieden wanneer geen duidelijke storingsoorzaak kan worden vastgesteld.

Van repeterende Incidenten wordt een Problem ticket aangemaakt welke bij Problem Management voor nader onderzoek wordt belegd. De Service Desk van Opdrachtgever wordt door de Service Desk van Leverancier geïnformeerd dat een Problem ticket is aangemaakt en de wijze waarop tot een oplossing van de repeterende incidenten wordt gewerkt.

4.5.2.5 Escalatie Incident Management

De escalatieprocedure kan door één van de partijen opgestart worden en treedt in werking indien één van de partijen (Opdrachtgever of Leverancier) van oordeel is dat:

- De maximum doorlooptijd (volgens de SLA) is bereikt, maar het Incident niet is opgelost en/of het betreft een Incident met een prioriteit 1;
- De (oorspronkelijke) maximum doorlooptijd is overschreden en/of de nieuw opgegeven doorlooptijd is niet acceptabel en/of de verstoring blijft;
- De dienstverlening is in zeer ernstige mate verstoord, een mogelijke Hersteltijd kan niet worden afgegeven.

Na afloop zal, conform het escalatieproces, een escalatierapport worden opgesteld waarin oorzaak en genomen stappen toegelicht worden. Tevens zal naar rato en conform SLA worden beoordeeld welke acties genomen dienen te worden op operationeel vlak.

In geval van escalatie treedt het in dit DAP beschreven escalatieproces in werking. Daarbij wordt onderscheid gemaakt tussen interne escalatie (onderdeel van de procesgang) en externe escalatie (waarbij de klant wordt geïnformeerd).

4.6 Change Management

Changes zijn verzoeken tot wijziging van de IT omgeving. Deze kunnen bijvoorbeeld betrekking hebben op applicatie programmatuur (fixes, patches in productie zetten), Systeem software (inzetten nieuwe release), beheer (aanpassen scripts en productie wijzigingen) of infrastructuur (wijzigingen hardware componenten).

Changes kunnen zowel door Opdrachtgever of Leverancier geïnitieerd worden.

4.6.1 Algemeen

Change management betreft het gecontroleerd doorvoeren van wijzigingen (Changes) in de dienstverlening. Voor alle soorten van wijzigingen geldt dat deze via het Change Management proces worden uitgevoerd. In dit proces wordt onderscheid gemaakt in Changes die betrekking hebben op een onderdeel van de geleverde dienst en Changes die betrekking hebben op de gehele dienstverlening.

Hiernaast wordt onderscheid gemaakt in niet-standaard Changes, standaard Changes die ingediend kunnen worden op basis van de lijst standaard Changes of Urgente Changes.

Om een Change initieel bij Leverancier aan te melden wordt het RFC formulier zoals in de bijlage van dit DAP is opgenomen, door de Service Desk van Opdrachtgever middels e-mail aangeleverd.

Bij elke Change wordt zonder uitzondering een implementatie draaiboek opgesteld wat volledig gemaakt en afgestemd alvorens de Change uitgevoerd wordt. Wanneer het implementatie draaiboek ontbreekt, kan de Change niet in behandeling genomen worden.

4.6.2 Prioriteit, Impact en Urgentie

Afhandeling van Changes vindt plaats op basis van het volgens het Service Level dat voor de dienstverlening is overeengekomen en de prioriteit die aan de Change is toegekend.

De prioriteit van een Change wordt bepaald door de combinatie van de impact en urgentie.
De prioriteiten van de verschillende soorten Changes zijn opgenomen in de SLA.

4.6.3 Niet –standaard changes

Niet-standaard changes zijn alle wijzigingen die niet zijn gedefinieerd in de lijst standaard changes en geen urgent karakter hebben.

4.6.4 Afspraken Niet –standaard changes

De RFC's (Request for Changes, ofwel: wijzigingsverzoeken) komende van Opdrachtgever worden aangemeld bij de Service Desk van Leverancier waarbij Opdrachtgever aangeeft met welke prioriteit deze uitgevoerd dient te worden. Per prioriteit en op basis van het overeengekomen Service Level is een vaste doorlooptijd overeengekomen.

4.6.5 Procedure Niet –standaard changes

Voor iedere wijziging stelt Leverancier een impactanalyse inclusief kostencalculatie op. De impactanalyse plus kostencalculatie worden teruggestuurd naar Change en Contract Management van Opdrachtgever. Change Management van Opdrachtgever verzorgt de verdere afstemming binnen Opdrachtgever en zal Leverancier informeren over de uitkomst van de afstemming.

Ten behoeve van de afstemming is het mogelijk dat het wijzigingsverzoek wordt doorgeleid naar de Change Advisory Board (CAB) van Opdrachtgever waarvoor Leverancier wordt uitgenodigd. In dit gremium (voorgezeten door de Change Manager van Opdrachtgever) zitten vertegenwoordigers van

Leverancier en specialisten van Opdrachtgever. In het CAB wordt besloten over de change, rekening houdend met kosten, impact, planning en andere lopende wijzigingsprocedures. Na goedkeuring wordt de Change uitgevoerd, conform de procedure zoals in de procedure Standaard Change in dit DAP (paragraaf 5.7.7.4).

4.6.6 Standaard changes

Leverancier heeft voor de veel voorkomende werkzaamheden (o.a. Standaardwijzigingen en aanvragen) standaard formulieren en procedures tegen standaardprijzen en met een vaste, beperkte doorlooptijd. Deze worden in overleg met Opdrachtgever opgesteld en afgestemd.

4.6.7 Afspraken Standaard changes

De standaard RFC's komende van Opdrachtgever worden aangemeld bij de Service Desk van Leverancier. De prioriteit, doorlooptijd en beprijzing van Standaard Changes zijn van te voren middels de DFA vastgesteld en worden door Leverancier gehanteerd. Afwijkingen hierop zijn niet mogelijk.

4.6.8 Procedure

4.6.8.1 RFC vanuit Opdrachtgever

In het geval dat een RFC vanuit Opdrachtgever wordt geïnitieerd, wordt deze door de Service Desk van Opdrachtgever aangemeld bij de Service Desk van Leverancier onder gebruikmaking van het RFC formulier zoals in de bijlage van deze DAP is opgenomen. Na ontvangst wordt door Leverancier contact opgenomen met de Change Coördinator van Opdrachtgever. Vervolgens wordt het wijzigingsverzoek inhoudelijk geverifieerd.

Na acceptatie door Change Management van Leverancier wordt een changenummer toegekend. Het changenummer wordt per E-mail aan Change Management van Opdrachtgever. Zodra het changenummer is toegekend start de doorlooptijd van de change.

4.6.8.2 RFC vanuit Leverancier

In het geval dat een RFC vanuit Leverancier wordt geïnitieerd, wordt deze door de Service Desk van Leverancier aangemeld bij de Service Desk van Opdrachtgever onder gebruikmaking van het RFC formulier zoals in de bijlage van deze DAP is opgenomen.

De RFC zal onderbouwd worden met een argumentatie waarna Change Management van Opdrachtgever na beoordeling eventueel zal overgaan tot goedkeuring van de Change. Het verdere verloop van de change is conform het Standaard Change proces.

4.6.8.3 Goedkeuring van Changes

Changes met prioriteit 1 en 2 dienen door het CAB goedgekeurd te worden alvorens deze uitgevoerd kunnen worden. Urgente changes kunnen tussentijds worden uitgevoerd na goedkeuring van Opdrachtgever Change Manager en de Service Delivery manager van Leverancier.
Changes met prioriteit 3 en 4 kunnen procedureel zonder goedkeuring van het CAB worden uitgevoerd. En worden begeleid door de toegewezen Change Coördinator.

4.6.8.4 Planning van de Change

De uitvoering van de change wordt vervolgens gepland. Leverancier informeert Change Management van Opdrachtgever hierover per email. De planning bevat ondermeer:

- Geplande start van de wijzigingswerkzaamheden;
- Gepland einde van de wijzigingswerkzaamheden;
- Changenummer waaronder de wijziging is geregistreerd bij Change Management van Leverancier.

4.6.8.5 Tussentijdse informatievoorziening

Change Management van Opdrachtgever wordt volgens de tijdsinterval behorende bij het overeengekomen Service Level en de prioriteit die aan de change is toegekend geïnformeerd over inhoudelijke wijzigingen in de voortgang van een Change en is bereikbaar om vragen, informatie te ontvangen en te verschaffen binnen het Support Window.

4.6.8.6 Implementatie van de Change

Change management van Leverancier coördineert de implementatie van de wijziging. Op het moment dat met de implementatie wordt gestart, wordt dit aan Change Management van Opdrachtgever gemeld. Betreft het een omvangrijke wijziging dan wordt regelmatig over de voortgang van de implementatie gecommuniceerd naar Opdrachtgever.

Nadat de implementatie is voltooid wordt de uitgevoerde wijziging ter acceptatie aangeboden aan Change Management van Opdrachtgever en wordt afgesloten met een vooraf tussen beide partijen afgesproken test- en acceptatie traject. Bij problemen met de acceptatie volgt nader overleg tussen Change Management van Opdrachtgever en Change Management van Leverancier over de eventuele vervolgstappen.

4.6.8.7 Afsluiten van de Change

Changes worden per mail afgemeld bij Change Management van Opdrachtgever. Binnen 3 werkdagen heeft Change Management van Opdrachtgever de mogelijkheid de Change te laten heropenen mits de oplossing niet volstaat. Hierna sluit Change Management van Leverancier de wijziging af.

4.6.9 Urgente changes

Urgente changes zijn RFC's met een spoedeisend karaker om deze zo snel mogelijk door te voeren en welke niet door het niet-standaard change proces afgehandeld kunnen worden. Veelal vormen ernstige verstoringen (incidenten met een prioriteit 1) of Escalaties de reden van voor een Urgente Change.

4.6.10 Afspraken

Om een Urgente Change zo snel mogelijk ten uitvoer te kunnen brengen wordt direct tussen Opdrachtgever en Leverancier contact gezocht om overeenstemming te krijgen over het uitvoermoment en de beprijzing van de Urgente Change. Omwille de snelheid te behouden kan eventueel door Leverancier van te voren een globale prijs afgegeven worden waarbij de marge niet meer bedraagt dan 10% meer of minder van de uiteindelijke beprijzing. De uitvoer van de Urgente Change vindt altijd pas plaats na goedkeuring van Change Management van Opdrachtgever.

4.6.11 Procedure

De beslissing of een Change de stempel "Urgent" krijgt, ligt bij de Change Manager van Opdrachtgever. Urgent in deze context is dat een Incident met prioriteit 1 of mogelijk te verwachten Incident met prioriteit 1 aan ten grondslag ligt of ongepland Onderhoud dat zo snel mogelijk uitgevoerd dient te worden.

Indien de Change Manager van Opdrachtgever de urgentie bevestigd aan de hand van de argumenten wordt een "urgent CAB" bijeen geroepen. Onder andere door middel van mail en sms worden de deelnemers geïnformeerd over de te nemen stappen.

In geval een Urgente Change buiten kantooruren aangevraagd wordt dan gaat de Escalatieprocedure in. Dit betekent dat de autorisatie één management laag hoger gebracht wordt en daar de beslissing wordt genomen of de Change desondanks uitgevoerd mag worden. Inclusief het nemen van de verantwoordelijkheid.

Na de uitvoering van een urgente Change volgt altijd een evaluatie in het reguliere CAB.

4.6.12 Escalatie Change afhandeling

Indien Changes de overeengekomen Service Level niet halen of duidelijk is dat deze niet gehaald kunnen worden kan Change Management van Opdrachtgever escaleren bij Leverancier volgens de Escalatieprocedure.

4.7 Release Management

Release Management bestaat uit het doorvoeren van gebundelde Changes welke onder andere hoofdzakelijk bestaan uit (security) patches, applicaties, upgrades van het Operating Systems van de in gebruik zijnde routers en switches of servers, etc.,

4.7.1 Afspraken

Doordat vooraf niet in te schatten is wat de consequenties van een Release kan zijn voor de dienstverlening van Opdrachtgever worden Releases gemeld aan Change Management van Opdrachtgever. De classificatie van een Release is hierbij een Niet-Standaard Change in de categorie Release en wordt middels het Change Management proces afgehandeld.

Evenals bij Change Management wordt zonder uitzondering voor elke Release een Implementatie Draaiboek opgesteld wat volledig gemaakt en afgestemd alvorens de Release uitgevoerd wordt. Wanneer het Implementatie Draaiboek ontbreekt, kan de Release niet in behandeling genomen worden.

Releases vallen niet onder gepland of ongepland onderhoud maar worden wel tijdens het Maintenance Windows uitgevoerd.

4.7.2 Procedure

Voor het indienen, implementeren of afsluiten van een Release, wordt de Niet-Standaard Change procedure gevolgd.

4.8 Beveiliging/Security Management

Security management richt zich op het door de Leverancier te bieden proces, procedures en werkwijzen rondom (informatie)beveiliging. Hierbij is de (informatie)beveiliging van de geleverde dienstverlening gericht op het waarborgen van de vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van de te leveren diensten. De beveiliging is mede gebaseerd op beveiligingsnormen conform het internationale ISO27001.

4.8.1 Afspraken

4.8.1.1 Compliancy en TPM

Leverancier heeft een ISMS (Information Security Management System) volgens ISO 27001 en wat is gecertificeerd tegen ISO 27001. Dit ISMS dekt minimaal de dienstverlening aan Opdrachtgever af. Ten behoeve van het door Opdrachtgever hebben van inzicht (eis 4.3.2.f) welke controls uit het ISO 27001 door Leverancier zijn afgedekt is een "Verklaring van Toepasselijkheid" (Statement of Applicability, eis 4.3.1.j) afgegeven.

Leverancier waarborgt dat de informatiebeveiliging geïmplementeerd en beheerst is. Indien op ingangsdatum van de Overeenkomst Leverancier geen ISMS volgens IS27001 heeft wat minimaal de geleverde dienstverlening aan Opdrachtgever afdekt, zal dit binnen een 6 maanden na ingangsdatum van het Overeenkomst opgezet, geïmplementeerd en werkend zijn. Indien niet aan deze voorwaarde wordt voldaan zal de Overeenkomst beëindigd worden en heeft Opdrachtgever de mogelijkheid om een claim wegens het niet komen van de contractuele voorwaarden bij Leverancier neer te leggen.

Jaarlijks geeft Leverancier een Third Party Mededeling (TPM) af welke wordt opgesteld door een onafhankelijke deskundige partij. De TPM is gebaseerd op het normenkader ISO 27001. In de TPM wordt een mededeling gedaan over opzet, bestaan en werking van de beheersmaatregelen.

De TPM dient een positieve strekking te hebben. Indien de TPM geen positieve strekking heeft, maken Opdrachtgever en Leverancier bindende afspraken over te nemen verbeteracties. Hierbij wordt over de verbeteracties regelmatig rapportage gedaan over de voortgang.

4.8.1.2 Security logging en monitoring

Leverancier biedt Opdrachtgever de mogelijkheid om de beveiliging van de dienstverlening te monitoren. Hieraan zijn de minimaal de volgende eisen van toepassing:

- Leverancier logt beheerdershandelingen op de applicaties en infrastructuur. De logmeldingen worden geregistreerd in een audit trail;
- Leverancier ondersteunt de mogelijkheid voor applicaties om een audit trail van gebruikershandelingen aan te maken;
- Leverancier biedt de mogelijkheid om de inhoud van de audit trails minimaal dagelijks te kopiëren naar een centrale logserver van Opdrachtgever;
- Audit trails worden na één jaar gewist in verband met privacy-overwegingen.

4.8.1.3 Beveiligingsorganisatie, logische beveiliging

Ten behoeve van beveiliging een is contactpersoon aangewezen voor Opdrachtgever Security Officer. Deze contactpersoon is op de hoogte van de beveiligingsrisico's binnen de dienstverlening aan Opdrachtgever en van de getroffen beveiligingsmaatregelen.

Leverancier legt ten behoeve van Opdrachtgever een lijst aan van alle beheerders die handelingen uitvoeren op de systemen van Opdrachtgever en onderhoud deze. Al deze beheerders beschikken over een VOG (Verklaring Omtrent het Gedrag). Bij de eerste inzet van een beheerder toont Leverancier de originele VOG van deze beheerder aan Opdrachtgever.

De logische toegang tot de housing & hosting dienstverlening is beperkt tot daarvoor geautoriseerd personeel. Dit zijn medewerkers die uit hoofde van hun functie technische werkzaamheden ten behoeve van de dienstverlening moeten verrichten.

4.8.1.4 Vervanging en afvoer defecte Hardware

Defecte gegevensdragers zoals harde schijven, tapes of CD/DVD's, USB-sticks, etc., welke informatie bevatten volgens WBP_2 of WBP_3 worden na vervanging direct fysiek vernietigd. Deze gegevensdragers worden door Leverancier hiervoor aangeboden aan een hiertoe gespecialiseerde onderneming. Als bewijs dat de defecte gegevensdrager vernietigd is wordt door Leverancier hiertoe een verklaring aan Opdrachtgever afgegeven.

4.8.2 Procedure

4.8.2.1 Beveiligingsincident en Prioriteiten

Binnen de categorie Incidenten nemen beveiligingsincidenten een specifieke plaats in. Dit soort Incidenten kunnen als gevolg veroorzaken dat de beschikbaarheid, vertrouwelijkheid en/of betrouwbaarheid van de informatievoorziening worden aangetast.

Beveiligingsincidenten worden middels het reguliere Incident proces afgehandeld en worden de Security Managers van Opdrachtgever en Leverancier betrokken bij de afhandeling/opvolging. Als Leverancier constateert dat mogelijk sprake is van een Incident met als gevolg van een "Security-breach" (inbraak op

de beveiliging) dan dient direct contact opgenomen te worden met de Security Manager van Opdrachtgever. Beveiligings incidenten worden geprioriteerd op basis van de tabel in de SLA.

4.8.2.2 Beveiligingsprobleem

Beveiligingsincidenten die niet binnen de SLA kunnen worden opgelost worden geclassificeerd als beveiligingsproblem waarbij de prioriteit van het Incident ongewijzigd blijft. De beveiligingsproblems worden middels het reguliere problem proces afgehandeld en worden de Security Managers van Opdrachtgever en Leverancier betrokken bij de afhandeling/opvolging. De beveiligingsproblems zullen afhankelijk van de mogelijke impact direct worden geëscaleerd na overleg met Opdrachtgever Security Manager.

Bij een beveiligingsproblem zal te allen tijde de Security Managers van Opdrachtgever en Leverancier worden betrokken voor het bepalen van de impact en de afhandeling c.q. opvolging waarbij ieder beveiligingsproblem zal worden afgesloten met een rapport. De rapportage over beveiligingsproblem's is verwerkt in de Service Management rapportage.

5 Akkoordverklaring

Middels ondertekening verklaren beide partijen dit DAP te hebben gelezen, afspraken en procedures te hebben geïmplementeerd in de eigen organisatie en zich hieraan te verbinden.

Aldus overeengekomen te Amsterdam en in tweevoud ondertekend,

	Leverancier		**Gemeente**
Datum		Datum	
Naam		Naam	
Functie		Functie	
Handtekening Leverancier		Handtekening Opdrachtgever	

Bijlage 1: Rollen en functies

Rol/Afdeling	Activiteiten

Bijlage 2: Communicatie en escalatie

Algemene escalatie contacten

Niveau	Gemeente	Leverancier
Operationele escalatie		
Tactische escalatie		
Strategische escalatie		

Contacten en escalatie Service Desk

Niveau	Gemeente	Leverancier
Operationeel contact binnen kantoortijden (07:30 - 18:00)		
Operationeel contact buiten kantoortijden (18:00 - 07:30)		
1e Escalatie		
2e Escalatie		
3e Escalatie		
4e Escalatie		

Contacten en escalatie Incident proces

Niveau	Gemeente	Leverancier
Operationeel contact binnen kantoortijden (07:30 - 18:00)		
Operationeel contact buiten kantoortijden (18:00 - 07:30)		
1e Escalatie		
2e Escalatie		
3e Escalatie		
4e Escalatie		

Bijlage 3: Afkortingen en begrippenlijsten

Afkorting	Omschrijving
CAB	Change Advisory Board, gremium waarin besluiten over ingediende changes worden gedaan.
CI	Configuration Item, een identificeerbaar onderdeel uit de dienstverlening en geregistreerd in de CMDB.
CMDB	Configuration Management DataBase, DataBase waarin de CI's worden geregistreerd.
D/R Plan	Disaster / Recovery Plan
DAP	Dossier Afspraken en Procedures, document waarin operationele afspraken en procedures tussen de leverancier en Opdrachtgever zijn uitgewerkt en vastgelegd.
DFA	Dossier Financiële Afspraken, document waarin de financiële afspraken zijn vastgelegd over de dienstverlening.
ITIL 2	Information Technology Infrastructure Library versie 2. Een procesgericht raamwerk om grip te krijgen en houden op de kwaliteit van de IT-dienstverlening.
KPI	Key Performance Indicator (Kritieke Prestatie-Indicator), meeteenheid voor het meten van een prestatie.
Prince 2	PRojects IN Controlled Environments versie 2. Een gestructureerde methode voor projectmanagement gericht op het krijgen en houden op de kwaliteit van de IT-projecten. Deze methode is gericht op het management, de besturing en de organisatie van een project.
RFC	Request for Change (wijzigingsverzoek). Een verzoek tot wijziging wat beoordeeld wordt alvorens dit verder als change (wijziging) wordt afgehandeld.
SLA	Service Level Agreement, document afspraken bevat tussen Leverancier en Opdrachtgever over de te leveren niveau van dienstverlening.
TPM	Third Party Mededeling, een goedkeurende verklaring dat door een onafhankelijke certificerende instantie wordt gegeven dat de processen in een organisatie voldoen aan vooraf opgestelde criteria. Aantoonbaarheid staat hierin centraal. De norm is: - Opzet - is er een ontwerp? - Bestaan - zijn de processen er? - Werking - werken ze zoals bedoeld?
VOG	Verklaring Omtrent Gedrag, een verklaring omtrent het onderzoek naar het strafrechtelijke verleden van een natuurlijke persoon of rechtspersoon. Hiermee wordt gekeken of er bepaalde bezwaren bestaan tegen de persoon om bijvoorbeeld een bepaald beroep uit te oefenen. Wettelijke tekst: "*Een verklaring omtrent gedrag is een verklaring van Onze Minister dat uit een onderzoek met betrekking tot het gedrag van de betrokken natuurlijke persoon of rechtspersoon ingesteld, gelet op het risico voor de samenleving in verband met het doel waarvoor de afgifte is gevraagd en na afweging van het belang van betrokkene, niet is gebleken van bezwaren tegen die natuurlijke persoon of rechtspersoon. De verklaring bevat geen andere mededelingen*"

WBP 2	Wet Bescherming Persoonsgegevens risicoklasse 2 (Verhoogd Risico). De wet die de beveiliging van persoonsgegevens regelt waarmee wordt bedoeld alle informatie die betrekking heeft op identificeerbare personen en waarbij risicoklasse 2 van toepassing is.
WBP 3	Wet Bescherming Persoonsgegevens risicoklasse 3 (Hoog Risico). De wet die de beveiliging van persoonsgegevens regelt waarmee wordt bedoeld alle informatie die betrekking heeft op identificeerbare personen en waarbij risicoklasse 2 van toepassing is.

Definities:

Begrip	Omschrijving
Audit trail	Zodanige vastlegging van gegevens dat de verwerkingsresultaten achteraf door de accountantsdienst kunnen worden gecontroleerd. De records in een logboek-bestand die een bepaalde computeractiviteit bewijzen.
Backup	Kopie van een of meer bestanden naar een ander geheugenmedium om deze veilig te stellen in geval de oorspronkelijke bestanden beschadigd raken of verloren gaan.
Calamiteit	Een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van een of meer IT-diensten de afgesproken drempelwaarden zal overschrijden.
Escalatie	Het ernstiger worden van een conflictsituatie. Bij escalatie wordt een beroep gedaan op de organisatie om meer kennis ter beschikking te stellen of beslissingen te nemen. Dit is nodig wanneer bij het betreffende organisatieonderdeel onvoldoende kennis of bevoegdheden aanwezig zijn.
Governance	Begrip dat duidt op de handeling of de wijze van besturen, de gedragscode, het toezicht op organisaties. Het wordt in verband gebracht met beslissingen die verwachtingen bepalen, macht verlenen of prestaties verifiëren.
Klokuren	Alle uren van de dag, van 00.00 – 24.00 uur, zowel Werkdagen als niet-Werkdagen.
Known Error DataBase	DataBase waarin bekende fouten in opgeslagen wordt. Een Known Error is conditie in de IT infrastructuur waarbij een bepaald configuratieitem geïdentificeerd is als de oorzaak van een (potentiële) degradatie van het overeengekomen serviceniveau.
Licentie (software)	Een softwarelicentie is een vergunning om een computerprogramma van iemand anders te gebruiken.
Maintenance Window	Periode waarin Leverancier gepland onderhoud kan verrichten.
Non Conformity Notes	Geïdentificeerde issues komende vanuit een gehouden audit die beschrijven waarin de dienstverlening tekort schiet.
Openingsuren	De periode waarin de dienstverlening beschikbaar is. Het Service Window is de periode binnen de openingsuren waarin de dienstverlening beheerd en bewaakt wordt.

Begrip	Omschrijving
Prioriteit	Relatieve waardering van een activiteit ten opzichte van andere activiteiten. Eigenschap van vooraf te gaan aan of voorrang te hebben boven iets of iemand anders. De prioriteit wordt bepaald op basis van de Impact en Urgentie.
Problem	Een conditie van de dienstverlening of IT infrastructuur geidentificeerd uit incidenten met overeenkomstige symptonen, of een significant incident, indicatief voor een fout waarvan de oorzaak nog onbekend is.
Restore	Het terugzetten van een of meerdere bestanden waarvan middels de Backup een reservekopie is gemaakt en opgeslagen op een ander geheugenmedium.
Retransitie	Na contractbeëindiging van de dienstverlening volgt de insourcing van de dienstverlening naar: - de eigen organisatie (dienstverlening weer in eigen beheer van Opdrachtgever) (Retransitie); - een transitie van de dienstverlening naar een nieuwe leverancier (Retransitie); - het niet meer afnemen van de dienst omdat de behoefte verdwenen is.
Service Level	Gedefinieerde set van KPI's en criteria waartegen de dienstverlening afgenomen kan worden.
Service Window	De periode waarbinnen Leverancier de beschikbaarheid van haar dienstverlening bewaakt en waarin zij ondersteuning biedt om de overeengekomen beschikbaarheid te behalen.
Site Survey	Onderzoek op locatie.
Support Window	De periode waarin de Dienst gegarandeerd conform deze SLA beschikbaar is en waarin de leverancier benaderd kan worden voor het melden en afhandelen van incidenten, changes, etc.
Technisch Beheer	Het Technisch Beheer omvat activiteiten die gericht zijn op de instandhouding van de technische infrastructuur.
Ticketnummer	Nummer van de melding dat geautomatiseerd wordt gegenereerd door het Service Management systeem waarin meldingen van gebruikers wordt vastgelegd.

Bijlage 4: Voorbeeld Service Management rapportage



Template Service Management Rapport

Bijlage 5: Voorbeeld Major Incident Rapportage



Template Major Incident Rapportage,

Bijlage 6: Voorbeeld Major Incident Report



Template Major Incident Rapportage,

Bijlage 7: Change Request Formulier (RFC)



Template Request for Change, Dienst IC

Bijlage 8 : Voorbeeld Implementatie Draaiboek



Template Implementatie Draaib