



Dossier Afspraken en Procedures

Tussen Gemeente Amsterdam en < Leverancier> behorende bij de
Overeenkomst Bezwaar en Beroep met contractnummer < xx>

Datum: 16-12-2019

Status: Definitief

Versie: 1.0

Template versie 0.2



Gemeente Amsterdam

Vertrouwelijkheidverklaring

Alle in dit document vermelde informatie is verstrekt op basis van wederzijdse vertrouwelijkheid en zal niet door enige partij geheel of gedeeltelijk worden gepubliceerd noch bekend gemaakt zonder uitdrukkelijke schriftelijke toestemming van de Gemeente Amsterdam en zal op veilige wijze worden bewaard.

Introductie

<Leverancier> houdt zich bezig met <generieke en specifieke vraagstukken> op het gebied van ICT.

Document controle

File Name: Bijlage DAP, ICT Diensten, v.0.3.doc

Document geschiedenis

Auteur	Versie	Datum	Status	Commentaar
Rene Posthumus	0.1	xx/xx/20xx	Concept	Template
Patrick Kamsma	0.2		Concept	Nader ingevuld
Patrick Kamsma	0.3	2-12-2019	Concept	Na overleg ingevuld
Robin Dorsman	0.4	12-12-2019	Concept	Verwerking opmerkingen en wijzigingen
Robin Dorsman	1.0	16-12-2019	Definitief	Definitief gemaakt

Document eigenaar	<Leverancier>
-------------------	---------------

Referentie documentatie

Document Naam	Bestand identificatie

Review

Naam	Versie	Datum	Status	Commentaar
<Leverancier>				
Dienst ICT				

Verspreidingslijst

Naam	Functie	Actie
<Leverancier>		
Dienst ICT		

INHOUDSOPGAVE

Vertrouwelijkheidverklaring	1
Introductie	1
1 Inleiding.....	6
2 Algemeen	6
2.1 Doel.....	6
2.2 Leeswijzer	6
2.3 Relaties met andere documenten	6
2.4 Beheer en evaluatie DAP	7
2.5 Wijzigingen.....	8
2.5.1 Voorstellen tot wijzigingen vanuit de Dienst ICT	8
2.5.2 Voorstellen tot wijzigingen vanuit <Leverancier>	8
2.6 Geldigheidsduur	8
3 Scope van de dienstverlening	9
4 Communicatie overlegstructuur.....	9
4.1 Communicatie	9
4.2 Overleg	9
5 Proces afspraken en procedures Beheer	10
5.1 Afspraken algemeen	10
5.2 Klachten	10
5.3 Escalatie.....	10
5.3.1 Afspraak.....	11
5.3.2 Procedure	12
5.3.3 Rapportage	13
5.4 Service Desk.....	13
5.4.1 Afspraken.....	13
5.4.2 Procedure	14
5.5 Incident Management.....	15
5.5.1 Afspraken.....	15
5.5.2 Procedure	15
5.6 Problem Management.....	17
5.6.1 Afspraken.....	17
5.6.2 Procedure	17
5.7 Change Management.....	18
5.7.1 Algemeen.....	18
5.7.2 Prioriteit, Impact en Urgentie	19
5.7.3 Niet –standaard changes.....	19
5.7.4 Afspraken Niet –standaard changes.....	19
5.7.5 Procedure Niet –standaard changes	19
5.7.6 Standaard changes	20
5.7.7 Afspraken Standaard changes	20
5.7.8 Procedure	20
5.7.9 Urgente changes.....	21
5.7.10 Afspraken.....	21
5.7.11 Procedure	21
5.7.12 Escalatie change afhandeling.....	22
5.8 Release Management.....	22
5.8.1 Afspraken.....	22

5.8.2	Procedure	22
5.9	Configuration Management	22
5.9.1	Afspraken	22
5.9.2	Procedure	23
5.10	Continuity en Availability Management	23
5.10.1	Afspraken	24
5.10.2	Procedure	24
5.11	Capacity Management	25
5.11.1	Afspraken	25
5.11.2	Procedure	25
5.12	Financial Management	25
5.12.1	Afspraken	25
5.12.2	Procedure	25
5.13	Service Level Management	25
5.13.1	Afspraken	25
5.13.2	Procedure	25
5.14	Beveiliging/Security Management	26
5.14.1	Afspraken	26
5.14.2	Procedure	27
5.15	Licentie Management	28
5.15.1	Afspraken	28
5.15.2	Procedure	28
6	Kwaliteit- en verwachtingsmanagement.....	29
6.1	Periodieke controle van de Dienstverlening	29
6.2	Klanttevredenheidsonderzoek	29
6.3	Audits	29
6.3.1	Procedure	29
7	Operationele afspraken en procedures beheer activiteiten	30
7.1	Beheer activiteiten	30
7.2	Monitoring van de Dienstverlening	30
7.3	Back-up van data en installatiegegevens	31
7.3.1	Afspraken	31
7.3.2	Procedure	31
7.4	Onderhoud	32
7.4.1	Gepland onderhoud	32
7.4.2	Afspraken	32
7.4.3	Procedure	32
7.4.4	Ongepland onderhoud	33
7.4.5	Afspraken	33
7.4.6	Procedure	33
8	Afspraken en procedures nieuwe leveringen en projecten	33
8.1.1	Algemeen	33
8.1.2	Acceptatie en start beheerfase	33
8.2	Procedure	34
8.3	Rapportage	34
9	Retransitie.....	34
9.1	Afspraken	34
9.2	Procedure	35
	Akkoordverklaring	35
	Bijlage 1: Rollen en functies.....	36
	Bijlage 2: Communicatie en escalatie	37

Bijlage 3: Afkortingen en begrippenlijsten	38
Bijlage 4: Voorbeeld Service Management rapportage	41
Bijlage 5: Voorbeeld Major Incident Rapportage	41
Bijlage 6: Voorbeeld Major Incident Report	41
Bijlage 7: Change Request Formulier (RFC).....	41

1 Inleiding

Het Dossier Afspraken en Procedures (DAP) is een onderdeel van de documentatie behorende bij de Overeenkomst betreffende de dienstverlening <Dienst> welke door <Leverancier> geleverd wordt en afgesloten is met de Dienst ICT Amsterdam. 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 de Dienst ICT Amsterdam en <leverancier>;
- De escalatie procedure;
- Verantwoordelijken wijzigingsproces;
- Capaciteit, beschikbaarheid en continuïteit van de dienstverlening;
- Beveiliging.

Daar waar verder in dit document "de Dienst ICT" wordt aangeduid wordt hiermee de Dienst ICT Gemeente Amsterdam bedoeld.

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 dienst <Dienst> 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 de Dienst ICT helder te maken.

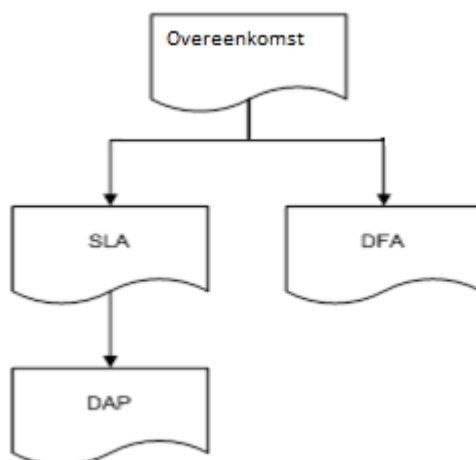
2.2 Leeswijzer

In deze DAP is zover mogelijk een standaardindeling per proces gehanteerd. Deze standaardindeling bestaat uit:

- Afspraken: beschrijving van de afspraken die tussen partijen overeengekomen zijn.
- Procedure: beschrijving van de te hanteren procedure per onderwerp.

2.3 Relaties met andere documenten

De relaties en hiërarchie van de (contractuele) documenten ten aanzien van de dienstverlening (de ICT Prestatie) is als volgt:



Uit dit overzicht valt af te leiden dat de Overeenkomst de hoogste in de hiërarchie van documenten is. De Overeenkomst staat als het ware boven het SLA (welke gevolgd wordt door het DAP), DFA. Dit betekent dat in geval van strijdigheid tussen een bepaling uit de Overeenkomst en een bepaling uit een van de onderliggende documenten de bepaling uit de Overeenkomst prevaleert. In geval van strijdigheid tussen een bepaling uit SLA en een bepaling uit het DAP geldt dat de bepaling uit het SLA, indien aanwezig, prevaleert. Aanvullende afspraken en Prestatie indicatoren welke niet voorkomen in het SLA, maar wel vastgelegd in het DAP, worden gezien als een aanvulling op het SLA en zijn daarom niet strijdig met het SLA.

In het overzicht zijn statische als dynamische documenten te onderscheiden. De statische documenten bestaat uit de Overeenkomst en deze documenten betreffen de contractuele documenten die eenmalig worden opgesteld, getekend en voor de looptijd niet meer kunnen worden aangepast. De dynamische documenten bestaan uit:

- o SLA (Service Level Agreement);
- o DFA (Dossier Financiële Afspraken);
- o DAP (Dossier Afspraken en Procedures).

Deze documenten worden periodiek tijdens de looptijd van de Overeenkomst geëvalueerd en beoordeeld op toepasselijkheid, wijzigingen in de dienstverlening, etc.

Ten behoeve van de te leveren dienstverlening zullen tevens de Overeenkomst toegevoegd:

- Retransitiestrategie;
- Retransitieplan;
- Nader in te vullen.

In deze documenten worden bij de bijbehorende (beheer)processen toegelicht.

2.4 Beheer en evaluatie DAP

Het DAP wordt beheerd door <Leverancier> en wordt minimaal 1 maal per jaar, of op verzoek van een van de partijen, geëvalueerd. Beide partijen kunnen voorstellen doen om het DAP aan te passen. Aanpassingen op het DAP worden door <Leverancier> verwerkt.

Tijdens deze evaluatie wordt het DAP in ieder geval getoetst op de bruikbaarheid in achterliggende periode van het DAP, contactpersonen en hun functie, scope van de dienstverlening of de lopende

procedures. Indien nodig, kunnen additionele onderwerpen voor de evaluatie uiterlijk 2 weken voor het evaluatieoverleg ingediend worden.

Onder het beheer van de DAP wordt verstaan:

- Versiebeheer (waaronder bijhouden wijzigingshistorie, versienummering, etc.);
- Beschrijven en updaten van verantwoordelijkheden en taakverdeling;
- Benoemen van de beheerprocessen en het actualiseren van dit DAP op basis van doorontwikkeling van deze beheerprocessen;
- Rapportage over de bruikbaarheid van het DAP;
- Organiseren van overleg, communicatie en waar nodig escalatie over het DAP, op tactisch en operationeel niveau. Eventueel additioneel overleg tussen specialisten over specifieke onderwerpen, zoals beveiliging en kwaliteit;
- Voorstellen voor verbeteringen c.q. wijzigingen in het DAP.

2.5 Wijzigingen

De toegewezen Service Manager van <Leverancier> ten behoeve van de dienstverlening <Dienst> is verantwoordelijk voor het actualiseren van dit DAP. Wijzigingen dienen door beide partijen, de Dienst ICT en <Leverancier>, te worden geaccordeerd en worden pas van kracht na ondertekening van de nieuwe versie van het gewijzigde document.

Indien bij een van de partijen de contactpersonen wijzigt zal die partij dat aan de andere partij schriftelijk meedelen.

2.5.1 Voorstellen tot wijzigingen vanuit de Dienst ICT

Voorstellen tot wijzigingen op dit DAP worden door de Contract Manager van de Dienst ICT aangemeld aan de <contactpersoon leverancier>. Afhankelijk van de noodzaak en urgentie om het DAP direct aan te passen zal de <contactpersoon leverancier> hiervoor de benodigde overleggen ten behoeve van verdere afstemming en uitwerking inplannen.

Indien geen directe noodzaak of urgentie aanwezig is om het DAP aan te passen zal de <contactpersoon leverancier> het wijzigingsverzoek bewaren en inbrengen in het eerstvolgende evaluatieoverleg.

2.5.2 Voorstellen tot wijzigingen vanuit <Leverancier>

Voorstellen tot wijzigingen op dit DAP worden door de <contactpersoon leverancier> aan de Contract Manager van de Dienst ICT. Afhankelijk van de noodzaak en urgentie om het DAP direct aan te passen zal de <contactpersoon leverancier> hiervoor de benodigde overleggen ten behoeve van verdere afstemming en uitwerking inplannen.

Indien geen directe noodzaak of urgentie aanwezig is om het DAP aan te passen zal de <contactpersoon leverancier> het wijzigingsverzoek bewaren en inbrengen in het eerstvolgende evaluatieoverleg.

2.6 Geldigheidsduur

Het DAP is telkens maximaal 1 jaar geldig en dient automatisch jaarlijks op de agenda van het tactisch overleg te komen.



3 Scope van de dienstverlening

De scope van de dienstverlening is in de leidraad vermeld en zal nader met de Leverancier worden ingevuld.

4 Communicatie overlegstructuur

4.1 Communicatie

De communicatie tussen de Dienst ICT en <Leverancier> verloopt in beginsel altijd tussen de Service Desken van beide partijen.

4.2 Overleg

Tussen <Leverancier> en de Dienst ICT 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 Dienst ICT Lijnmanagement Dienst ICT Account Director / Service Delivery Manager <Leverancier> Account Manager <Leverancier>	Notulen Besluiten/actielijst Ingebrachte stukken tactisch overleg Strategie/beleid Dienst ICT
Tactisch	Output operationeel overleg Lopende en geplande veranderingen Lopende overeenkomst/dienstverlening Toekomstige ontwikkelingen	1x per 3 maanden	Lijnmanagement Dienst ICT Contract Management Dienst ICT Account Management <Leverancier>	Notulen Besluiten/actielijst Ingebrachte stukken operationeel overleg Capaciteitsprognose Calamiteitenplan D/R Plan Retransitie strategie & Retransitie Plan
Operationeel	Operationele resultaten aan de hand van Service Management rapportage Ernstige problemen of afwijkingen op de geleverde	1x per maand	Service Management Dienst ICT Leveranciers Management	Notulen Actielijst Service Management rapportage

Overleg	Onderwerpen	Frequentie	Deelnemers	Documenten
	dienstverlening		Dienst ICT Service Management <Leverancier>	

Tijdens het maandelijks operationele overleg worden alle opgetreden incidenten en gedefinieerde problemen besproken. Aanvullende deelnemers aan dit overleg zijn onder andere de Problem Manager van de Dienst ICT 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.

5 Proces afspraken en procedures Beheer

5.1 Afspraken algemeen

De beheerprocessen van <Leverancier> zijn op basis van ITIL 2 ingericht.

Voor de dienstverlening is een Service Window op basis van het gekozen Service Niveau 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 de <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.

Het Service Niveau <Service Niveau> voor de dienstverlening <Dienst> is tussen <Leverancier> en de Dienst ICT overeengekomen en zijn voor alle beheerprocessen van toepassing. Het Service Niveau <Service Niveau> is op basis van in de PDC beschreven niveau.

5.2 Klachten

Indien een klacht of opmerking is op de werkzaamheden van <Leverancier> dan kan de Dienst ICT 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 de Dienst ICT wordt afgehandeld kan de Dienst ICT escaleren middels de escalatieprocedure.

5.3 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 Service Niveau van de dienstverlening te kunnen blijven voldoen of om overschrijding van het Service Niveau tot een minimum te beperken. Bij escalatie wordt een beroep gedaan op additionele functionele kennis en/of hiërarchische bevoegdheid.

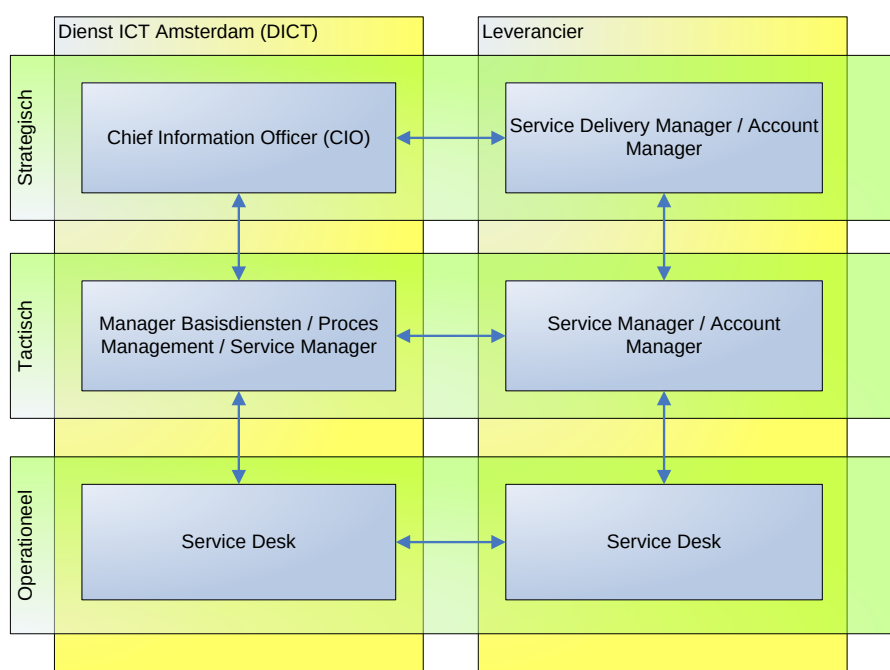
Binnen een escalatie worden diverse escalatieniveaus onderkend met als uiterste de crisiscommunicatie op het hoogste hiërarchische niveau van de betrokken organisaties. De

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 de Dienst ICT 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.

Navolgend schema geeft op hoofdniveau de Governance structuur weer die in geval van escalatie gevolgd wordt.

<Navolgend voorbeeld van een Governance structuur kan hierbij opgenomen worden.>



In geval (of het vermoeden) van een beveiligingsincident vindt altijd escalatie plaats (zie voor de procedure paragraaf 5.14.2.1). Ook zal de escalatieprocedure in werking treden indien sprake is van een crisis of ramp.

5.3.1 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.

5.3.2 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.

5.3.2.1 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).

5.3.2.2 Externe escalatie

Tussen de Dienst ICT 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).

5.3.2.3 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:

Escalatie niveaus bij de Dienst ICT:

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.

5.3.3 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 de Dienst ICT <Leverancier> aanwijzen voor het opstellen van het rapport. De Dienst ICT 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 de Dienst ICT aangeleverd naar het tactische niveau.

In het rapport is opgenomen en uitgewerkt:

- Identificatie escalatie;
- Naam coördinator <Leverancier>;
- Naam coördinator van de Dienst ICT;
- 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.

5.4 Service Desk

De Service Desk van <Leverancier> is het centrale en enige contactpunt voor de Dienst ICT Service Desk voor alle operationele communicatie over de dienstverlening en draagt zorg voor het herstel van de afgesproken dienstverlening volgens in het met de Dienst ICT overeengekomen SLA en Diensten Niveau. Alle communicatie en meldingen zoals vragen, incidenten, opdrachten of klachten die betrekking hebben op de dienstverlening, komen vanaf de Dienst ICT Service Desk. De Dienst ICT 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 de Gemeente Amsterdam met de Service Desk van <Leverancier> waarbij altijd de Service Desk van de Dienst ICT over de communicatie wordt geïnformeerd.

5.4.1 Afspraken

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

Tijdens het Service Window volgens het overeengekomen Service Niveau kan de Service Desk van de Dienst ICT 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 Niveau van de verschillende Service Desks is als volgt:

	Dienst ICT	<Leverancier>
Openingstijden :	07:30 - 18:00	
Telefoon :	020- 2516161	
E-mail :	servicedesk@dict.amsterdam.nl	

(Omwille van de eenvoud zijn hier de overeengekomen openingstijden behorende bij het Service Niveau, overgenomen).

Bij telefonisch contact wisselen de Dienst ICT 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-mailadres van de melder;
- Dienst (Service) waarop het incident betrekking heeft;
- Prioriteit (door de Dienst ICT 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.

5.4.2 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 de Dienst ICT bij aanmelden de prioriteit bepaald. Eventueel kan de Dienst ICT 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 de Dienst ICT en <Leverancier> te hanteren.

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

Binnen 15 minuten wordt een bevestiging van de melding per mail aan de Dienst ICT Service Desk gestuurd onder vermelding van het ticketnummer. Indien het ticket door de Service Desk van <Leverancier> als incident wordt uitgezet binnen het Incident Managementproces van <Leverancier> zal, afhankelijk van de prioriteit van het incident en het overeengekomen Service Niveau die voor de dienstverlening is overeengekomen, <Leverancier> de Dienst ICT in de frequentie volgens het overeengekomen Service Niveau 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 de Dienst ICT. In overleg worden het ticket en incident afgesloten waarbij de Dienst ICT het eindoordeel doet.

5.5 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 proactieve incident meldingen en reactieve incident meldingen. Proactieve incidenten zijn verstoringen die middels monitoring worden opgemerkt vanuit de processen zoals Availability 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 gelden afwijkende afspraken. Zie hiervoor het hoofdstuk Beveiliging/Security Management.

5.5.1 Afspraken

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

<Leverancier> garandeert een maximale responsetijd van 10 minuten op binnenkomende meldingen en incidenten middels e-mail of telefoon. Dit betreft zowel door de Dienst ICT aangemelde incidenten als door de <Leverancier> zelf geconstateerde Incidenten.

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 bepaald de Dienst ICT 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 Niveau en de SLA. Het bepalen van de prioriteit gebeurt aan de hand van onderstaande tabel:

Prioriteit	Criteria
1	Incidenten die leiden tot volledige uitval van één of meer bedrijfskritische applicaties. Deze Incidenten komen in de Service Management rapportage tot uiting in een verlaagd beschikbaarheid percentage.
2	Incidenten die ernstig impact hebben op de dienstverlening en die leiden tot een uitval of verminderde dienstverlening voor een groot deel van de gebruikers.
3	Incidenten die een beperkte impact hebben, die slechts voor enkele gebruikers merkbaar zijn, uitval van niet-bedrijfskritische applicatie.

Opmerking: indien <Leverancier> zelf een onderbreking signaleert terwijl de Dienst ICT deze niet meldt, geldt dezelfde oplostijd.

5.5.2 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.

5.5.2.1 Aanmelden en registreren Incident

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

1. Een incident is geconstateerd door de Dienst ICT 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 de Dienst ICT 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 de Dienst ICT gecommuniceerd.

5.5.2.2 Voortgang van een incident

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

Wanneer het incident niet binnen de overeengekomen oplostijd kan worden opgelost wordt de Service Desk van de Dienst ICT 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 de Dienst ICT 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.

5.5.2.3 Afmelden van een incident

Een incident wordt in overleg met de Dienst ICT definitief afgesloten waarbij de Dienst ICT het eindoordeel doet. De afmelding wordt gedaan per e-mail afgemeld bij de Service Desk van de Dienst ICT. 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 de Dienst ICT de mogelijkheid het incident te laten heropenen indien de oplossing niet volstaat.

5.5.2.4 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 de Dienst ICT 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 de Dienst ICT 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.

5.5.2.5 Escalatie Incident Management

De escalatieprocedure kan door één van de partijen opgestart worden en treedt in werking indien één van de partijen (de Dienst ICT 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 oplostijd 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).

5.6 Problem Management

Problem Management betreft het voorkomen/minimaliseren van negatieve effecten van fouten in de dienstverlening of onderliggende infrastructuur en is verantwoordelijk voor het vinden van de oorzaak van hiervan. Incidenten en problemen kunnen betrekking hebben op de door <Leverancier> aangeboden dienstverlening en/of op de door de Dienst ICT ontwikkelde applicaties.

5.6.1 Afspraken

Problem Management van <Leverancier> beoordeelt of een (meerdere) incidenten een probleem worden zodat een onderzoek naar de oorzaak opgestart dient te worden.

Problem Management van <Leverancier> zorgt voor een correcte en bruikbare vastlegging van een probleem, de status gedurende de oplostijd en de gegevens over de oplossing zodat uit deze administratie informatie over problemen en oplossingen gehaald kunnen worden en vastgelegd in een Known Error Database.

Indien bij een definitieve oplossing beide partijen (<Leverancier> en de Dienst ICT) betrokken zijn dan wordt de coördinatie door Problem Management van <Leverancier> verzorgd. Het uitzetten van acties binnen de Dienst ICT wordt door het Problem Management van de Dienst ICT geregeld.

5.6.2 Procedure

Onder verantwoordelijkheid van de Problem Manager van <Leverancier> vindt dagelijks een controle plaats op de in het afgelopen 24 uur opgetreden incidenten en zal, indien hiertoe aanleiding bestaat,

deze uitzetten als een problem voor nader onderzoek. Het onderzoek en voortgang vindt bij <Leverancier> plaats waarbij Problem Management van de Dienst ICT over de voortgang wordt geïnformeerd en eventueel geraadpleegd.

5.6.2.1 Aannemen en registreren

Naast de dagelijkse controle op de incidenten die mogelijk als problem onderzocht dienen te worden kan ook de Dienst ICT een problem bij <Leverancier> initiëren. Het initiëren van een problem wordt gedaan door de Service Desk van de Dienst ICT waarbij de volgende gegevens aangeleverd worden:

- Problem nummer van de Dienst ICT;
- Klantnaam;
- Contactgegevens;
- Technisch contact persoon (optioneel);
- Service/Dienstverlening;
- Impact;
- Urgentie;
- Omschrijving van het probleem;
- Gerelateerde incidenten en changes (optioneel);
- Referentienummer.

5.6.2.2 Tussentijdse informatievoorziening

Over de voortgang bij het oplossen van een problem wordt Problem Management van de Dienst ICT volgens de tijdsinterval behorende bij het overeengekomen Service Niveau en de prioriteit die aan het problem is toegekend, geïnformeerd. Tevens kan via mail of telefonisch een statusverzoek ingediend worden bij de Service Desk van <Leverancier>.

5.6.2.3 Afsluiting

De Problem Manager van <Leverancier> bespreekt de gevonden oorzaken met Problem Management van de Dienst ICT en hoe het problem te verhelpen. Hierbij kan besloten worden dat het problem middels een change wordt verholpen of dat het problem blijft bestaan en opgenomen wordt in de Known Error Database welke beschikbaar is voor de Service Desk van <Leverancier> en de Dienst ICT. Hierna wordt in overleg het problem afgesloten waarbij de Dienst ICT het eindoordeel doet. Vervolgens verschijnt de definitieve versie van het problemreport welke door <Leverancier> wordt opgesteld en aan de Dienst ICT aangeleverd.

5.7 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 de Dienst ICT of <Leverancier> geïnitieerd worden.

5.7.1 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 (die leiden tot aanpassing van de PDC).

Hiernaast wordt onderscheid gemaakt in niet-standaard Changes, standaard Changes die ingediend kunnen worden op basis van de lijst standaard Changes zoals gedefinieerd in de PDC 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 de Dienst ICT 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.

5.7.2 Prioriteit, Impact en Urgentie

Afhandeling van changes vindt plaats op basis van het volgens het Service Niveau 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. Als leidraad voor het bepalen zijn de onderstaande globale criteria van toepassing.

Bepaling Urgentie:

1. **Urgent**; inzet zo spoedig mogelijk (bijvoorbeeld in verband met productie verstoring of dreigende productie verstoring);
2. **Standaard**; inzet volgens het overeengekomen Service Niveau (Prioriteit 1,2 of 3).

Bepaling Impact Level

1. Zeer complex en omvangrijk, (hoge) impact voor gebruikers, veel resources, eventueel onbeschikbaarheid;
2. Complex en omvangrijk, impact voor gebruikers, relatief veel resources, geen onbeschikbaarheid;
3. Relatief eenvoudig en weinig omvang, impact voor gebruikers, relatief weinig resources, geen onbeschikbaarheid;
4. Eenvoudig en weinig omvang, geen impact voor gebruikers, weinig resources, geen onbeschikbaarheid.

Elementen voor de bepaling van het Impact Level:

- De complexiteit en omvang van de change;
- De benodigde resources (capaciteit, hoeveelheid werk, systeemgebruik e.d.);
- De hoeveelheid benodigde kennis en ervaring;
- Onbeschikbaarheid van b.v. netwerk, systemen en applicaties;
- Mate van veranderingen voor de gebruikers.

5.7.3 Niet –standaard changes

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

5.7.4 Afspraken Niet –standaard changes

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

5.7.5 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 de Dienst ICT. Change Management van de Dienst ICT verzorgt de verdere afstemming binnen de Dienst ICT 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 de Dienst ICT waarvoor <leverancier> wordt uitgenodigd. In dit gremium (voorgezeten door de Change Manager van de Dienst ICT) zitten vertegenwoordigers van <Leverancier> en specialisten van de Dienst ICT. 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).

5.7.6 Standaard changes

<Leverancier> heeft voor de veel voorkomende werkzaamheden (o.a. Standaardwijzigingen en aanvragen) standaardformulieren en procedures tegen standaardprijzen en met een vaste, beperkte doorlooptijd. Deze worden in overleg met de Dienst ICT opgesteld en afgestemd waarna deze worden opgenomen in de PDC.

Een standaard change betreft derhalve een wijziging in de dienstverlening die is beschreven en geprijsd in de PDC.

5.7.7 Afspraken Standaard changes

De standaard RFC's komende van de Dienst ICT worden aangemeld bij de Service Desk van <Leverancier>. De prioriteit, doorlooptijd en beprijzing van Standaard Changes zijn van tevoren middels de PDC en DFA vastgesteld en worden door <Leverancier> gehanteerd. Afwijkingen hierop zijn niet mogelijk.

5.7.8 Procedure

5.7.8.1 RFC vanuit de Dienst ICT

In het geval dat een RFC vanuit de Dienst ICT wordt geïnitieerd, wordt deze door de Service Desk van de Dienst ICT 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 de Dienst ICT. 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 de Dienst ICT. Zodra het changenummer is toegekend start de doorlooptijd van de change.

5.7.8.2 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 de Dienst ICT 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 de Dienst ICT na beoordeling eventueel zal overgaan tot goedkeuring van de Change. Het verdere verloop van de change is conform het Standaard Change proces.

5.7.8.3 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 de Dienst ICT 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.

5.7.8.4 Planning van de Change

De uitvoering van de change wordt vervolgens gepland. <Leverancier> informeert Change Management van de Dienst ICT 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>.

5.7.8.5 Tussentijdse informatievoorziening

Change Management van de Dienst ICT wordt volgens de tijdsinterval behorende bij het overeengekomen Service Niveau 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.

5.7.8.6 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 de Dienst ICT gemeld. Betreft het een omvangrijke wijziging dan wordt regelmatig over de voortgang van de implementatie gecommuniceerd naar de Dienst ICT.

Nadat de implementatie is voltooid wordt de uitgevoerde wijziging ter acceptatie aangeboden aan Change Management van de Dienst ICT 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 de Dienst ICT en Change Management van <Leverancier> over de eventuele vervolgstappen.

5.7.8.7 Afsluiten van de Change

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

5.7.9 Urgente changes

Urgente changes zijn RFC's met een spoedeisend karakter 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.

5.7.10 Afspraken

Om een Urgente Change zo snel mogelijk ten uitvoer te kunnen brengen wordt direct tussen de Dienst ICT 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 tevoren 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 de Dienst ICT.

5.7.11 Procedure

De beslissing of een Change de stempel "Urgent" krijgt, ligt bij de Change Manager van de Dienst ICT. 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 de Dienst ICT de urgentie bevestigt aan de hand van de argumenten wordt een "urgent CAB" bijeengeroepen. 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 managementlaag 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.

5.7.12 Escalatie change afhandeling

Indien Changes de overeengekomen Service Niveau niet halen of duidelijk is dat deze niet gehaald kunnen worden kan Change Management van de Dienst ICT escaleren bij <Leverancier> volgens de Escalatieprocedure.

5.8 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.,

5.8.1 Afspraken

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

5.8.2 Procedure

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

5.9 Configuration Management

Configuration Management betreft het vastleggen, bijhouden en controleren van informatie over alle configuratie items die ingezet zijn om de overeengekomen dienstverlening mogelijk te maken.

5.9.1 Afspraken

<Leverancier> zal aan het begin van elke nieuwe maand en/of op aanvraag een actueel overzicht geven van de CI's (Configuration Items) welke ingezet zijn voor het leveren van de dienstverlening. De overzichten zijn zowel in grafische vorm als in de vorm van lijsten beschikbaar en in verschillende mate van detaillering.

5.9.1.1 Naamgevingconventie en identificatie Configuratie Items

Elk onderdeel uit de door <Leverancier> te leveren dienst zoals beschreven in de scope van de dienstverlening wordt aangemerkt als een Configuratie Item (CI) en wordt geregistreerd in de Configuratie Management Data Base (CMDB). Voor het eenduidig identificeren en registeren van de CI's is hiervoor een naamgevingconventie afgesproken. Deze naamgevingconventie is als volgt opgebouwd: **PDC-identificatie – volgnummer**.

De PDC-identificatie is terug te vinden in de PDC die door <Leverancier> middels een web-portal is ontsloten. De uitgifte van de volgnummers wordt door de Dienst ICT gedaan en dient door <Leverancier> bij elke nieuwe levering opgevraagd te worden alvorens tot uitlevering over te gaan. Bij het uitvragen van het volgnummer wordt door <Leverancier> de PDC-identificatie aangeleverd alsmede de verdere benodigde gegevens:

- CI-nummer (bij het opvragen van het volgnummer zal dit nog niet compleet zijn, echter kan <Leverancier> wel de PDC-identificatie al aanleveren);

- Type (B.v. Server of NAS);
- Sub-type (B.v. Virtuele Server of Fysieke server);
- Status;
- Omgeving (Productie, Test, Ontwikkel of Acceptatie)
- CI-nummer <Leverancier>;
- Omschrijving;
- Locatie;
- IP-adres 1
- IP-adres 2
- Ordernummer waaronder het CI besteld is;
- Leverancier van het CI;
- Leverancier onderhoud op het CI;
- Onderhoudscontract;
- Merk;
- Fabrikant;
- Serienummer;
- Eigenaar van het CI;
- Relaties met andere CI's.

Elk nieuw CI dat uitgegeven en door <Leverancier> geïnstalleerd zal worden, wordt door <Leverancier> voorzien van een sticker met een barcode dat het CI-nummer inhoud.

5.9.2 Procedure

5.9.2.1 Registratie CI's

Nieuwe CI's worden aangemeld en geregistreerd zoals aangegeven in de paragraaf "*Naamconventie en Identificatie CI's*". CI's waar geen PDC-identificatie voor aanwezig is worden in overleg met de Dienst ICT eerst opgenomen in de PDC waarna het CI aan de CMDB kan worden toegevoegd.

5.9.2.2 Actualiteit CMDB

<Leverancier> draagt er zorg voor dat de CMDB te allen tijde voor minimaal het Service Niveau dat voor de dienstverlening is overeengekomen, up-to-date is. Up-to-date wil zeggen: betrouwbare en juiste gegevens bevat en bijgewerkt.

5.9.2.3 Uitwisseling CMDB-gegevens

Ten einde de CMDB in de Service Managementsoftware van de Dienst ICT te synchroniseren en over de juiste laatste gegevens te beschikken, levert <Leverancier> in elektronische vorm maandelijks een bestand met CI's die door <Leverancier> zijn geregistreerd aan Configuration Management van de Dienst ICT aan. Deze elektronische vorm is dusdanig opgezet dat de informatie in de CMDB van de Dienst ICT automatisch verwerkt kan worden en bevat minimaal de informatie zoals in de paragraaf "*Naamconventie en Identificatie CI's*" beschreven.

5.9.2.4 Jaarlijkse controle

Minimaal 1 keer per jaar voert <Leverancier> een interne controle uit op de actualiteit en status van de geregistreerde CI's in de CMDB. Van deze controle wordt een rapportage opgesteld en aangeleverd aan de Dienst ICT waarna deze wordt besproken en, indien nodig, acties uitgezet om de vereiste percentage actualiteit volgens het Service Niveau dat voor de dienstverlening is overeengekomen te halen en behouden.

5.10 Continuity en Availability Management

Continuity Management betreft het waarborgen van de continuïteit en de beschikbaarheid van de dienstverlening. De continuïteit en de beschikbaarheid worden hierbij door <Leverancier> geleverd tegen het Service Niveau dat voor de dienstverlening is overeengekomen.

5.10.1 Afspraken

<Leverancier> draagt zorg voor continuïteit en beschikbaarheid, ook in geval van calamiteiten, waarbij proactieve maatregelen zijn getroffen om de vereiste beschikbaarheid, performance en beveiliging van de dienstverlening te garanderen. Hiertoe heeft <Leverancier> een Calamiteitenplan beschikbaar wat aangeeft hoe de continuïteit is geregeld, welke betrokken partijen betrokken zijn bij een calamiteit en het escalatieteam dat gevormd dient te worden gevormd met de benodigde bevoegdheden. Hiernaast heeft <Leverancier> een D/R Plan (Disaster/Recovery Plan) opgesteld wat aangeeft hoe (procedures, techniek, herstel en prioriteit), in geval van een calamiteit, zo snel mogelijk de dienstverlening kan worden hervat (al zij dit tegen een lagere beschikbaarheid).

Het kan voorkomen dat een omvangrijke en complexe storing in de dienstverlening optreedt of belangrijke delen van de infrastructuur door externe oorzaken worden beschadigd waardoor herstel niet binnen de afgesproken Service Niveau voor het afhandelen van incidenten mogelijk is. In een dergelijke situatie dat <Leverancier> niet zonder meer aan de eisen volgens het Service Niveau kan voldoen, wordt dit gezien als een Calamiteit. Bij het optreden van een Calamiteit brengt <Leverancier> de Dienst ICT zo spoedig mogelijk hiervan op de hoogte en geeft daarbij, indien mogelijk, aan wat de verwachte hersteltijd is.

Wanneer de dienstverlening middels het D/R Plan beschikbaar is gesteld maar nog steeds deze uitwerking wordt geleverd, zijn de overeengekomen Service Levels niet van toepassing. Pas dan wanneer de volledige dienstverlening naar de oude situatie van voor de opgetreden calamiteit is hersteld gaan de overeengekomen Service Levels weer in. Tijdens de Disaster/Recovery periode wordt periodiek door <Leverancier> naar de Dienst ICT gerapporteerd over de voortgang naar het herstel van de oude situatie voor de calamiteit. De frequentie en aan wie wordt per calamiteit bepaald.

Minimaal 1x per jaar wordt in samenwerking met de Dienst ICT de werking van het Calamiteitenplan en het D/R Plan getest. De uitkomst van deze test wordt aan de Dienst ICT gerapporteerd en, indien noodzakelijk, verbeteracties uitgezet teneinde de werking van het Calamiteitenplan en het D/R Plan zo optimaal te laten functioneren. Het Calamiteitenplan en het D/R Plan worden tijdens het Tactisch Overleg besproken en gemonitord op de voortgang c.q. ontwikkeling.

5.10.1.1 Uitwijkvoorziening voor de 'backend'

Ook voorzieningen aan de 'backend' zijde van de dienstverlening (rekencentrum, hardware en applicaties) die gehost zijn bij de concernonderdelen van de Dienst ICT zelf kunnen de gevolgen van een calamiteit ondergaan. In voorkomende gevallen kan de Dienst ICT opdracht geven om uitwijkvoorzieningen voor in huis gehoste voorzieningen aan te bieden. Ook voor dit scenario heeft <Leverancier> een globaal Calamiteitenplan en D/R Plan en zal 1x per jaar worden getest, over gerapporteerd en eventuele verbeteracties uitgezet.

5.10.2 Procedure

De start van een Calamiteit begint met een reactieve incident melding bij de Service Desk. Doordat de ernst van de verstoring snel bekend zal zijn en de Calamiteit wordt geconstateerd, gaat dit verder over in het Continuity en Availability proces en eventueel treedt het Calamiteitenplan van <Leverancier> in werking. Eventueel kan dit proces ondersteund worden door het Escalatie proces.

Het reactieve incident wordt geregistreerd als een prioriteit 1 incident waarbij alle overige incidentmeldingen die aan de calamiteit gerelateerd kunnen worden en ook de prioriteit 1 krijgen, aan het incident gekoppeld worden. Deze incidenten worden pas gesloten wanneer het Calamiteitenplan en D/R Plan in werking zijn getreden en een Crisisteam ingericht. In de oplossing van de incident(en) wordt hierbij verwezen naar de calamiteit.

Nadat een calamiteit is verholpen en de dienstverlening weer hersteld is naar de oude situatie van voor de calamiteit wordt door <Leverancier> in samenwerking met de Dienst ICT een onderzoek ingesteld wat de oorzaak/aanleiding tot de calamiteit is geweest, hoe deze toekomstig te voorkomen en welke verbeteringen in de dienstverlening hiertoe ingevoerd dienen te worden.

5.11 Capacity Management

Capacity Management betreft het waarborgen dat de capaciteit en performance van de dienstverlening blijvend voldoet aan de eisen uit het Service Niveau dat voor de dienstverlening is overeengekomen.

5.11.1 Afspraken

Middels systeem-monitoring bewaakt <Leverancier> of de geleverde capaciteit voor de dienstverlening tegen het Service Niveau dat voor de dienstverlening is overeengekomen, geleverd wordt. Bij onvoorziene knelpunten (afwijkingen of tekorten) in de capaciteit en/of de prestaties gemeten over 1 werkdag neemt <Leverancier> contact op met de Dienst ICT en adviseert over te nemen maatregelen.

Eens per jaar stelt <Leverancier> een capaciteitsprognose op. Op basis hiervan kan de capaciteit van de in beheer zijnde voorzieningen worden bijgesteld. In de capaciteitsprognose wordt aangegeven wat de trends zijn in de systeembelasting en de prestatieparameters. <Leverancier> heeft, waar nodig, prestatie modellen ontwikkeld om de correlatie van de werklast, prestatieparameters en capaciteit te kunnen verklaren. Indien een structureel tekort of overschot aan capaciteit ten opzichte van de prognose in het capaciteitsplan wordt geconstateerd, wordt door <Leverancier> aanpassingen van de capaciteit voorgesteld. De aanpassingen worden na opdracht van de Dienst ICT uitgevoerd. De capaciteitsprognose wordt tijdens het tactisch overleg besproken en gemonitord op de voortgang c.q. ontwikkeling.

5.11.2 Procedure

Indien een ernstige afwijking op de capaciteit van de geleverde dienstverlening door <Leverancier> en/of de Dienst ICT wordt geconstateerd, wordt dit gemeld bij zowel de Service Desk van de Dienst ICT als van de Service Desk van <Leverancier> en krijgt prioriteit 1. Dit ten einde zo snel mogelijk naar de juiste en benodigde capaciteit te komen. Vervolgens wordt het incident middels het Incident Managementproces afgehandeld. Indien duidelijk wordt dat de capaciteit niet binnen de overeengekomen oplostijd volgens het overeengekomen Service Niveau bij een van de prioriteit 1 incident hersteld kan worden, treedt het Escalatie proces in werking.

5.12 Financial Management

Financial management betreft het vaststellen van tarieven, doorbelasten van kosten, opleveren van financiële informatie.

5.12.1 Afspraken

De afspraken ten aanzien van het Financial Management zijn vastgelegd in het Dossier Financiële Afspraken (DFA).

5.12.2 Procedure

De procedures ten aanzien van het Financial Management zijn vastgelegd in het Dossier Financiële Afspraken (DFA).

5.13 Service Level Management

Service Level Management betreft het bewaken en verbeteren van het niveau van de overeengekomen KPI's ten aanzien van de dienstverlening en welke zijn vastgelegd in de SLA.

5.13.1 Afspraken

<Leverancier> monitort de geleverde dienstverlening of deze voldoet aan de gestelde KPI's behorende bij het overeengekomen Service Niveau en welke zijn vastgelegd in de overeengekomen SLA. In geval van dreigende of structurele overschrijding van de KPI's onderneemt <Leverancier> proactief acties om de overschrijding tegen te gaan.

5.13.2 Procedure

Maandelijks wordt door <Leverancier> een Service Management rapportage aan de Dienst ICT aangeleverd. In deze rapportage wordt onder andere aangegeven of de overeengekomen Service Levels behorende bij het overeengekomen Service Niveau zijn behaald. De Service Management

rapportage wordt door <Leverancier> en de Dienst ICT in het maandelijkse Operationele Overleg besproken en eventuele acties ter opvolging uitgezet.

5.14 Beveiliging/Security Management

Securitymanagement 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.

5.14.1 Afspraken

5.14.1.1 Compliance 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 de Dienst ICT af. Ten behoeve van het door de Dienst ICT 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 ISO27001 heeft wat minimaal de geleverde dienstverlening aan de Dienst ICT 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 de Dienst ICT 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 de Dienst ICT en <Leverancier> bindende afspraken over te nemen verbeteracties. Hierbij wordt over de verbeteracties regelmatig rapportage gedaan over de voortgang.

5.14.1.2 Security logging en monitoring

<Leverancier> biedt de Dienst ICT 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 de Dienst ICT;
- Audit trails worden na één jaar gewist in verband met privacy-overwegingen.

5.14.1.3 Beveiligingsorganisatie, logische beveiliging

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

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

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.

5.14.1.4 Vervanging en afvoer defecte Hardware

Defecte gegevensdragers zoals harde schijven, tapes of CD/DVD's, USB-sticks, etc., welke informatie bevatten volgens WBP2 of WBP3 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 de Dienst ICT afgegeven.

5.14.2 Procedure

5.14.2.1 Beveiligingsincident

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 incidentproces afgehandeld en worden de Security Managers van de Dienst ICT 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 de Dienst ICT. Op basis van de volgend criteria worden de beveiligingsincidenten als volgt geprioriteerd:

Prioriteit	Criteria
1	- Openbaar worden van vertrouwelijke gegevens - Aanval op de Amsterdamse infrastructuur d.m.v. virus, ddos, of actieve hackpogingen e.d. - Uitval of ernstige verstoring van cruciale netwerkservices zoals, firewall, virusscanners en dns services e.d.
2	- Manipulatie van bedrijfsvertrouwelijke gegevens of financiële informatie waardoor de gemeente benadeeld wordt en/of tot onterechte besluiten komt - In handen van derden komen van vertrouwelijke gegevens zonder dat deze openbaar worden gemaakt; - Beschadiging van bedrijfsgegevens waardoor de betrouwbaarheid van bedrijfsprocessen in gevaar komt.
3	- In handen van derden komen van vertrouwelijke gegevens zonder dat derden hiervan kennis kunnen nemen (versleuteld); - Beschadiging van bedrijfsgegevens waardoor de betrouwbaarheid van bedrijfsprocessen niet direct gevaar komt.

De incidenten met prioriteit 3 hoeven niet direct telefonisch te worden gemeld. Deze dienen wel in de maandrapportages te worden meegenomen en per dienst per maand op individueel niveau herkenbaar te worden gemaakt.

5.14.2.2 Beveiligingsprobleem

Beveiligingsincidenten die niet binnen de SLA kunnen worden opgelost worden geclassificeerd als beveiligingsprobleem waarbij de prioriteit van het incident ongewijzigd blijft. De beveiligingsproblemen worden middels het reguliere probleem proces afgehandeld en worden de Security Managers van de Dienst ICT en <Leverancier> betrokken bij de afhandeling/opvolging. De beveiligingsproblemen zullen afhankelijk van de mogelijke impact direct worden geëscaleerd na overleg met de Dienst ICT Security Manager.

Bij een beveiligingsprobleem zal te allen tijde de Security Managers van de Dienst ICT en <Leverancier> worden betrokken voor het bepalen van de impact en de afhandeling c.q. opvolging

waarbij ieder beveiligingsprobleem zal worden afgesloten met een rapport. De rapportage over beveiligingsprobleem's is verwerkt in de Service Management rapportage.

5.15 Licentie Management

Ten behoeve van de dienstverlening zijn voor de diverse applicaties die in gebruik zijn en de dienstverlening mogelijk maken, licenties benodigd om de functionaliteit te kunnen leveren. Deze in gebruik zijnde licenties zijn geregistreerd en overzichten kunnen op aanvraag aangeleverd worden.

Binnen de in gebruikte zijnde licenties wordt hierin onderscheid gemaakt tussen de licentie-overeenkomsten die de Dienst ICT zelf heeft afgesloten met de leveranciers van de software en de licentie-overeenkomsten die door <Leverancier> zijn afgesloten (en welke binnen het raamcontract vallen) om de gevraagde dienstverlening mogelijk te maken.

<Leverancier> heeft een geautomatiseerd systeem wat bijhoudt welke licenties aanwezig zijn, door wie gebruikt en waar deze zich logisch bevinden.

5.15.1 Afspraken

De benodigde en aangeschafte licenties voor de applicaties die nodig zijn om de dienstverlening, welke door <Leverancier> wordt geleverd, mogelijk te maken, worden door <leverancier> bijgehouden. Maandelijks wordt door <Leverancier> een overzicht aan de Dienst ICT aangeleverd van de in gebruik zijnde licenties. Hierbij wordt onderscheid gemaakt in de licenties die door de Dienst ICT zijn aangeschaft en de licenties die door <Leverancier> zijn aangeschaft ten behoeve de dienstverlening aan de Dienst ICT.

5.15.2 Procedure

Maandelijks wordt het licentie-overzicht over de afgelopen maand aangeleverd bij de Licentie Beheerder van de Dienst ICT. De Licentie Beheerder controleert de aangeleverde licenties en neemt, in geval van twijfel of onduidelijkheid, contact op met <Leverancier>. Vervolgens wordt in gezamenlijkheid het issue uitgezocht en opgelost.

6 Kwaliteit- en verwachtingsmanagement

6.1 Periodieke controle van de Dienstverlening

De Dienst ICT heeft de mogelijkheid om op periodieke basis (tweemaal per jaar) en indien hier concrete aanleiding toe ontstaat een controle uit te voeren op de kwaliteit van de dienstverlening door <Leverancier>. Deze controle heeft niet het karakter van een audit en leidt niet tot maatregelen. Het doel van de controle is om de Dienst ICT de gelegenheid te bieden zich te vergewissen van de kwaliteit van de dienstverlening.

6.2 Klanttevredenheidsonderzoek

De Dienst ICT voert voor eigen kosten jaarlijks een klanttevredenheidsonderzoek uit en kan <Leverancier> om advies vragen over de aanpak en te hanteren normen.

6.3 Audits

De Dienst ICT kan bij <Leverancier> een of meerde audits laten uitvoeren. De Dienst ICT en <Leverancier> komen hiervoor gezamenlijk tot een selectie van de onafhankelijke partij(en) voor genoemde audits. Beide partijen zijn hierbij verantwoordelijk voor het verstrekken van informatie en het op eigen kosten beschikbaar stellen van toegang tot resources voor de audits.

De audit(s) heeft(hebben) als doel om:

- Tussentijds te verifiëren of <Leverancier> de verplichtingen ten aanzien van de te leveren dienstverlening nakomt;
- Te verifiëren of herstel van geconstateerde gebreken in de dienstverlening heeft plaatsgevonden.

6.3.1 Procedure

6.3.1.1 Opstellen en uitvoeren auditprogramma.

Voorafgaand aan een audit wordt door de Dienst ICT in overleg met de <Leverancier> een auditprogramma opgesteld over de te auditeren processen. Een audit kan plaatsvinden op diverse (deel) processen c.q. afdelingen zoals:

- Regiedesk (Delivery);
- Service desk (service);

Het auditprogramma bevat minimaal:

- Doel en scope van de audit;
- Looptijd auditperiode;
- Namen van het auditteam;
- Deelnemers interviews;
- Locatie en tijdstip van de interview

Het auditteam voert de audit uit door middel van een documentatiebeoordeling en/of het houden van interviews met auditees.

6.3.1.2 Rapportage

Het auditteam geeft na afloop van een interview een korte mondelinge terugkoppeling van de belangrijkste bevindingen aan de geauditeerde. Aan het einde van de audit wordt een schriftelijke rapportage opgesteld. Het concept wordt gestuurd naar de Dienst ICT. Zodra de Dienst ICT heeft aangegeven akkoord te zijn met de inhoud van het auditrapport wordt het definitief gemaakt.

Het auditrapport omvat tenminste:

- Het auditprogramma
- Algemene bevindingen en bevindingen t.a.v. het Kwaliteitsmanagementsysteem
- Rapportage over verbeter-maatregelen op bevindingen.

6.3.1.3 Verbetermaatregelen

Op basis van de definitieve rapportage wordt, ingeval van tekortkomingen c.q. bevindingen, door <Leverancier> een verantwoordelijke aangesteld die verbetermaatregelen voorstelt. Na afstemming van de voorgestelde verbetermaatregelen met de betrokken afdelingen worden deze geregistreerd en voor opvolging bewaakt door <Leverancier>.

6.3.1.4 Controle

Na melding door de verantwoordelijke dat de verbetermaatregelen zijn geïmplementeerd wordt via een intern <Leverancier> proces geverifieerd of de tekortkomingen inderdaad zijn opgelost. Het resultaat van deze controle wordt geregistreerd en gerapporteerd aan de Dienst ICT.

6.3.1.5 Verantwoordelijkheden

De verantwoordelijke accordeert namens de betrokken afdelingen het auditplan en is medeverantwoordelijk voor het vervolg geven aan het oplossen van de geconstateerde Non Conformity Notes (NCN's) en observaties.

De verantwoordelijke:

- Realiseert (plannen, uitvoeren en rapporteren) het geaccordeerde auditplan;
- Registreert verbetermaatregelen en bewaakt opvolging daarvan;
- Voert controle uit door toetsing op het toepassen en de effectiviteit van de verbetermaatregelen;
- Archiveert audit documenten.

De betrokken afdelingen zijn verantwoordelijk voor het opvolgen van de in hun bedrijfsonderdeel/afdeling geconstateerde bevindingen. De verantwoordelijke, het management, de te interviewen personen, de kwaliteitsmanager en het auditteam, zijn gezamenlijk verantwoordelijk voor het resultaat van de audit.

7 Operationele afspraken en procedures beheer activiteiten

7.1 Beheer activiteiten

De Dienst ICT heeft de mogelijkheid om duidelijk afgebakende onderdelen van het Technisch Beheer van de dienstverlening welke gehuisvest zijn bij <Leverancier>, zelf uit te voeren. Hiervoor is door <Leverancier> de mogelijkheid gecreëerd voor de technisch beheerders welke in dienst zijn van de Dienst ICT, om de beheerwerkzaamheden vanuit de werkplek bij de Dienst ICT uit te voeren. De betrokken de Dienst ICT beheerders krijgen op aanvraag van de Dienst ICT rechten om queries en/of updates op databases uit te voeren. Daarbij wordt een passend beveiligde netwerktoegang voor betreffende beheerders gehanteerd.

De Dienst ICT heeft de mogelijkheid om zelf nieuwe software te deployen op omgevingen die gehost worden bij <Leverancier>. Echter: <Leverancier> zorgt voor installatie en configuratie van systemen en heeft processen en faciliteiten voor het aanbrengen van software-updates.

7.2 Monitoring van de Dienstverlening

De beschikbaarheid, performance, capaciteitsbeslag en de beschikbare capaciteit van de dienstverlening wordt gemonitord door <Leverancier>. De resultaten van deze monitoring worden maandelijks aan de Dienst ICT ter beschikking gesteld.

De Dienst ICT heeft toegang tot de monitoring-faciliteiten en de gegevens die <Leverancier> hanteert voor het monitoren van de dienstverlening. <Leverancier> heeft hiertoe aan de Dienst ICT beschikbaar gesteld (bijvoorbeeld een web interface met een overzicht). Hiernaast biedt <Leverancier> faciliteiten (bijv. agents) om de beschikbaarheid van de dienstverlening of specifieke functionaliteiten te monitoren door de Dienst ICT zelf.

Op basis van de monitoring onderneemt <Leverancier>, waar nodig, proactief actie om het niet beschikbaar zijn van de dienstverlening te voorkomen. Deze acties worden gemeld als incidenten en worden begeleid middels het Incidentproces.

7.3 Back-up van data en installatiegegevens

<Leverancier> heeft hardware en software om data back-up van productiegegevens te maken. Dit omvat tevens middelen om de opgeslagen gegevens te verifiëren en het herstel van gegevens naar productiesystemen uit te voeren. Het uitvoeren van backups maakt geen inbreuk op de beschikbaarheid van de dienstverlening.

De navolgende afspraken met betrekking tot de backup en restore zijn van toepassing op het normale, reguliere beheer. In geval een calamiteit gaande is waarbij naar een uitwijklocatie uitgeweken moet worden waarbij een restore van de laatste backup gedaan moet worden, gelden de navolgende afspraken niet. Tijdens de calamiteit worden aanvullende afspraken gemaakt ten aanzien van de backup tijdens de uitwijk.

7.3.1 Afspraken

Data back-ups worden in een beveiligde omgeving opgeslagen in een andere locatie dan waar de media zich bevindt waarmee de geback-upte gegevens zijn opgeslagen. De meest recente installatie-images van alle systemen worden ge-backupd en worden in een beveiligde omgeving in een andere locatie opgeslagen dan waar de betreffende systemen zich bevinden.

<Leverancier> biedt de mogelijkheid voor de Dienst ICT om op aanvraag een restore uit te voeren. Deze extra back-ups worden aangevraagd als een RFC. Bij het aanvragen van extra back-ups dient gespecificeerd te worden wat de bewaartijd van de back-up is.

De recovery time objective is volgens het Service Niveau dat voor de dienstverlening is overeengekomen. Dit houdt in dat maximaal na het indienen van de aanvraag volgens het Service Niveau de restore is uitgevoerd. De recovery time objective geldt vanaf het moment dat de locatie waar de restore op uitgevoerd wordt beschikbaar is.

De recovery point objective is volgens het Service Niveau dat voor de dienstverlening is overeengekomen. Dit houdt in, dat de te restoren data maximaal volgens de overeengekomen Service Niveau oud mag zijn (gerekend vanaf het moment van indienen van de call).

De locatie / omgeving waar de restore op uitgevoerd dient te worden moet bij aanvraag van de restore beschikbaar zijn en moet geschikt zijn om de restore op uit te voeren. Het inrichten van een eventuele omgeving waar de restore wordt teruggezet is geen onderdeel van het restoreproces. Als de restore wordt teruggezet op de oorspronkelijke locatie dan worden de bestaande gegevens overschreven.

Opmerking: met name kunnen restores van geclusterde omgevingen niet zonder meer op ongeclusterde omgevingen gezet worden.

7.3.2 Procedure

<Leverancier> is verantwoordelijk voor het maken van de back-up en controleert dagelijks of deze gelukt is. Wanneer het de back-up mislukt is wordt dit als een incident gemeld en afgehandeld. Tenzij afwijkende afspraken gemaakt zijn wordt bij het mislukken van een back-up contact opgenomen met de Service Manager van de Dienst ICT.

Restores kunnen worden aangevraagd als een standaard RFC. De recovery time objective en recovery point objective is afhankelijk van het afgenomen Dienstenniveau:

De back-up en restoretest is onderdeel van de standaard dienstverlening en elke 6 maanden wordt een back-up en restoretest uitgevoerd. Het initiatief hiervoor wordt door <Leverancier> genomen waarbij de test vooraf wordt doorgesproken met de Service Manager van de Dienst ICT welke tevens gedurende en na de test inzage in de resultaten krijgt. De eindresultaten worden in een rapport aan de Dienst ICT geleverd en besproken. In het overleg geconstateerde verbeterpunten worden als acties voor <Leverancier> uitgezet en opgepakt. Over de voortgang van de verbeteringen/lopende acties wordt de Dienst ICT maandelijks middels de Service Rapportage op de hoogte gehouden.

7.4 Onderhoud

7.4.1 Gepland onderhoud

Gepland onderhoud betreft onderhoudswerkzaamheden die vooraf ingepland kunnen worden. Voor deze onderhoudswerkzaamheden is een Maintenance Window afgesproken volgens het Service Niveau dat voor de dienstverlening is overeengekomen.

7.4.2 Afspraken

Aan het begin van elk kalenderjaar zal <Leverancier> aan de Dienst ICT een onderhoudskalender voor het betreffende jaar afgeven. Gedurende het maintenance window kan vanuit de Dienst ICT ook Changes doorgevoerd worden.

Indien <Leverancier> gepland onderhoud zal verrichten wordt de Dienst ICT daarvan volgens het Service Niveau dat voor de dienstverlening is overeengekomen van tevoren op de hoogte gebracht. <Leverancier> geeft aan welke onderhoudswerkzaamheden verricht zullen worden, welk Maintenance Window gehanteerd wordt en welk effect dit op de dienstverlening zal hebben.

De melding zal minimaal de volgende gegevens bevatten:

- Wat;
- Wanneer;
- Hoe lang;
- Impact op welke dienst;
- Onderhoudsplan;
- Roll back;
- Communicatie voor en na het onderhoud;
- Afmelding.

7.4.3 Procedure

Gepland onderhoud wordt door <Leverancier> aangemeld bij het Change Managementproces van de Dienst ICT. De Change Manager van de Dienst ICT beoordeelt of de Change impact heeft op de dienstverlening. Indien dit het geval is worden de betrokken via mail geïnformeerd en maakt een Change aan voor de uit te voeren onderhoudswerkzaamheden. <Leverancier> stelt vervolgens een Implementatiedraaiboek op, stemt deze af en levert deze aan bij Change Management van de Dienst ICT.

Indien de Dienst ICT bezwaar heeft tegen de geplande datum en tijdstip dan zal de Dienst ICT dit binnen 48 uur na ontvangst van de aankondiging melden aan <Leverancier> die een dergelijk bezwaar in overweging nemen en zal in ieder geval binnen 1 dag na ontvangst van het bezwaar een reactie geven.

Indien de werkzaamheden zonder goedkeuring van de Dienst ICT toch zijn uitgevoerd en leiden tot verstoringen aan de dienstverlening van de Dienst ICT zal <Leverancier> een rapportage opstellen waarom de werkzaamheden zijn uitgevoerd, reden waardoor de verstoring is opgetreden en welke initiatieven ondernomen worden om dit soort verstoringen te voorkomen. Tevens wordt van deze verstoring een incident aangemaakt en verder afgehandeld door het Incident Managementproces.

7.4.4 Ongepland onderhoud

Ongepland onderhoud betreft onderhoudswerkzaamheden die niet vooraf ingepland kunnen worden en om spoedeisende redenen op korte termijn uitgevoerd moeten worden.

7.4.5 Afspraken

Indien <Leverancier> (ongepland) urgent onderhoud dient uit te voeren wordt dit bij Change Management van de Dienst ICT aangemeld als een Urgente Change. <Leverancier> dient met een onderbouwing aan te geven waarom het onderhoud urgent is, welke onderhoudswerkzaamheden verricht zullen worden en welk effect dit op de dienstverlening zal hebben. Het is uiteindelijk aan de Dienst ICT om de uitvoering van het urgente onderhoud goed te keuren.

De melding zal minimaal de volgende inhoud bevatten:

- Wat;
- Wanneer;
- Hoe lang;
- Impact op welke dienst;
- Onderhoudsplan;
- Roll back;
- Communicatie voor en na het onderhoud;
- Afmelding.

7.4.6 Procedure

Ongepland onderhoud wordt gezien als een urgente change en volgens dit proces afgehandeld.

8 Afspraken en procedures nieuwe leveringen en projecten

Binnen de dienstverlening zal regelmatig sprake zijn van projecten of opdrachten waarbij de dienstverlening aangevuld of gewijzigd zal worden. Deze projecten of opdrachten kunnen of door <Leverancier> zelfstandig worden uitgevoerd danwel in samenwerking met de Dienst ICT. Afhankelijk van de afgesproken rolverdeling in deze projecten of opdrachten zal meer of minder inspanning van <Leverancier> verwacht worden.

8.1.1 Algemeen

Projecten worden uitgevoerd volgens de Prince2 methodiek.

8.1.2 Acceptatie en start beheerfase

Een opgeleverd project of opdracht wordt door de Dienst ICT geaccepteerd op het moment waarop de dienstverlening van <Leverancier> plaatsvindt conform de overeengekomen Service Levels. Dit is het moment waarop:

- De Dienst ICT de dienstverlening accepteert;
- De fase van beheer start;
- De facturering van de dienstverlening conform overeengekomen Service Levels begint.

Voor een acceptatie door de Dienst ICT wordt door <Leverancier> aan de volgende criteria voldaan:

- De dienstverlening vindt plaats conform overeengekomen Service Levels en besturing volgens dit DAP;
- De eerste Service Management rapportage, waarin is aangegeven dat gedurende één rapportageperiode aan de Service Levels is voldaan, is uitgebracht;
- Indien nodig zijn de PDC en SLA aangepast en door beide partijen afgestemd en bekrachtigd;
- Indien nodig de overlegstructuren zijn ingeregeld;

- Alle projectdocumentatie is opgeleverd (waaronder een decharge en een overzicht van restpunten).

Indien <Leverancier> niet aan deze criteria heeft voldaan volgt geen acceptatie door de Dienst ICT en zal <Leverancier> alsnog zorgdragen om aan de criteria te voldoen.

8.2 Procedure

Een project of een opdracht wordt altijd door de Dienst ICT verstrekt middels een getekende opdracht. Vanaf dit moment zal in continue afstemming <Leverancier> het project of de opdracht uitvoeren. Indien tijdens de uitvoering knelpunten ontstaan welke niet door de direct betrokkenen opgelost kunnen worden, treed de Escalatieprocedure uit dit DAP in werking.

Een project of een opdracht wordt door <Leverancier> per e-mail aan de Dienst ICT gereed gemeld. De e-mail wordt voorzien van het ondertekende document uit bijlage <X>. Vervolgens zal de Dienst ICT controleren of aan het gevraagde binnen het project of opdracht en gestelde criteria door <Leverancier> is voldaan. Indien de Dienst ICT tot acceptatie overgaat zal een Protocol van Oplevering worden opgesteld waarmee het project of de opdracht formeel wordt geaccepteerd.

8.3 Rapportage

De status van projectopdrachten en orders en worden door <Leverancier> geregistreerd en de status hiervan in de Service Management Rapportage gerapporteerd welke maandelijks door <Leverancier> aangeleverd wordt.

9 Retransitie

9.1 Afspraken

Na het beëindigen van de Overeenkomst zal <Leverancier> volledige medewerking verlenen zodat de dienstverlening succesvol overgenomen kan worden (retransitie) door een andere partij (andere leverancier of de Dienst ICT zelf) en heeft hiervoor een Retransitie Strategie en een initieel Retransitieplan opgesteld. Het Retransitieplan wordt na elke wijziging aan de geleverde dienstverlening door <Leverancier> bijgewerkt en, indien het ingrijpende wijzigingen aan de dienstverlening betreft, afgestemd met de Dienst ICT. Gedurende de looptijd van de Overeenkomst wordt het Retransitieplan door <Leverancier> actueel gehouden.

Uitgangspunten voor het Retransitieplan zijn onder andere:

- De overeengekomen Service Niveau en service levels voor de dienstverlening blijven gegarandeerd tot het moment van overname van de dienstverlening door een andere partij. <Leverancier> geeft deze garantie voor een periode van ten minste 18 maanden, gerekend vanaf de datum van einde Overeenkomst;
- Contracten met derde partijen, die noodzakelijk zijn voor de continuïteit van de dienstverlening, zullen worden overgedragen naar de nieuwe dienstverlener (of naar de Dienst ICT);
- Alle kennis over de Dienst ICT, diens processen en administratieve gegevens ter beschikking gesteld aan de nieuwe dienstverlener;
- Alle CI's waarop de dienstverlening is gebaseerd wordt overgedragen aan de nieuwe dienstverlener (of de Dienst ICT). Dit betreft onder meer (maar niet uitsluitend) de hard- en software, contracten en eventuele licenties die van belang zijn voor de dienstverlening;
- <Leverancier> levert na afronding van de migratie een exitplan op aan de Dienst ICT waarin beschreven wordt hoe de retransitie is verlopen.

Ten slotte: <Leverancier> conformeert zich aan de "Gedragscode Retransitie" versie 0.9 zoals deze is opgesteld door het Platform Outsourcing Nederland.

9.2 Procedure

Vanaf het moment dat de Overeenkomst tussen <Leverancier> en de Dienst ICT is bekrachtigd en de dienstverlening wordt geleverd, wordt binnen 2 maanden het eerste concept van het Retransitieplan bij de Dienst ICT aangeleverd. Indien tijdens de aanbesteding geen Retransitie Strategie is geleverd, zal dit alsnog gebeuren.

Tijdens de looptijd van de Overeenkomst zal de Retransitie Strategie, indien nodig, worden aangepast en afgestemd met de Dienst ICT. Vanuit deze strategie wordt het Retransitieplan uitgewerkt en afgestemd met de Dienst ICT. Belangrijk onderdeel uit het Retransitieplan is de correcte, bijgehouden en betrouwbare CMDB. De CMDB dient immers inzicht te geven welke componenten zijn ingezet voor de dienstverlening en bij een retransitie gemigreerd dienen te worden. <Leverancier> zal daarom zorgdragen dat nieuwe CI's ook automatisch in het retransitieplan worden verwerkt.

Indien de retransitie opportuun wordt zal de Dienst ICT dit bij <Leverancier> aangeven. Vanaf dat moment zal een project worden gestart welke de retransitie zal uitvoeren. Acceptatie van dit project door de Dienst ICT vindt plaats zoals beschreven in paragraaf 8.1.2.

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>		Dienst ICT	
Datum		Datum	
Naam		Naam	
Functie		Functie	
Handtekening		Handtekening	
Leverancier		Opdrachtgever	



Bijlage 1: Rollen en functies

Rol/Afdeling	Activiteiten
--------------	--------------



Bijlage 2: Communicatie en escalatie

Algemene escalatie contacten

Niveau	Dienst ICT	<Leverancier>
Operationele escalatie		
Tactische escalatie		
Strategische escalatie		

Contacten en escalatie Service Desk

Niveau	Dienst ICT	<Leverancier>
Operationeel contact binnen kantoortijden (07:30 - 18:00)		
Operationeel contact buiten kantoortijden (18:00 - 07:30)		
1 ^e Escalatie		
2 ^e Escalatie		
3 ^e Escalatie		
4 ^e Escalatie		

Contacten en escalatie Incident proces

Niveau	Dienst ICT	<Leverancier>
Operationeel contact binnen kantoortijden (07:30 - 18:00)		
Operationeel contact buiten kantoortijden (18:00 - 07:30)		
1 ^e Escalatie		
2 ^e Escalatie		
3 ^e Escalatie		
4 ^e 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 de Dienst ICT 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.
PDC	Producten en Diensten Catalogus, document waarin een vertaling is gemaakt van de afgesproken dienstverlening in concrete producten en diensten.
Prince 2	PRjects 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 de Dienst ICT 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.
Change	Een overeengekomen wijziging op de geleverde dienstverlening.
Diensten, Dienstverlening	De door Leverancier op basis van de overeenkomst ten behoeve van de Dienst ICT te verlenen diensten, te verrichten werkzaamheden en in het kader daarvan te leveren prestaties die voldoen aan de gestelde functionaliteiten, de kwaliteitseisen en randvoorwaarden van Opdrachtgever.
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.
Incident	Elke gebeurtenis afwijkend van de (verwachte) standaardwerking van de dienstverlening. Het heeft invloed op de dienstverlening hoewel deze invloed klein of zelfs transparant kan zijn voor de gebruiker van dit systeem. Na het incident vertoont het object een fout.
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.
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 geïdentificeerd uit incidenten met overeenkomstige symptomen, of een significant incident, indicatief voor een fout waarvan de oorzaak nog onbekend is.
Recovery Point Objective (RPO)	Punt in de tijd tot waar maximaal teruggekeerd moeten kunnen worden bij het "restoren" van gegevens.
Recovery Time Objective (RTO)	Maximum toelaatbare tijd dat een systeem, applicatie of netwerk onbeschikbaar mag zijn.



Begrip	Omschrijving
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 de Dienst ICT) (Retransitie); - een transitie van de dienstverlening naar een nieuwe leverancier (Retransitie); - het niet meer afnemen van de dienst omdat de behoefte verdwenen is.
Service Niveau	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