

Bijlage 20

Dossier Afspraken en Procedures IDMA

tussen
Gemeente Amsterdam
en
<<naam leverancier>>

Opdrachtgever:	Verkeer & Openbare Ruimte Gemeente Amsterdam
Contractnummer:	AI 2021-0047
Versie:	1.0
Datum:	15-06-2021

Colofon

Document geschiedenis

Versie	Datum	Auteur	Status	Commentaar
0.1	23-4-2021	Amsterdam	Concept	

Referentie Documenten

Document naam	Bestand identificatie

Review

Versie	Datum	Naam	Status	Commentaar
Leverancier				
Opdrachtgever				

Distributielijst

Versie	Datum	Naam	Status	Commentaar
Leverancier				
Opdrachtgever				

Inhoudsopgave

1	Over dit document.....	4
2	Algemeen	5
2.1	Doel.....	5
2.2	Looptijd	5
3	Communicatie overlegstructuur	6
3.1	Communicatie	6
3.2	Overleg.....	6
4	Proces afspraken en procedures Beheer	7
4.1	Afspraken algemeen	7
4.2	Klachten	7
4.3	Escalatie	7
4.4	Helpdesk.....	7
4.4.1	Afspraken.....	8
4.4.2	Procedure.....	8
4.5	Incident Management.....	9
4.5.1	Prioriteiten Incidenten	9
4.5.2	Procedure.....	10
4.6	Change Management	11
4.6.1	Algemeen.....	12
4.6.2	Niet –standaard changes	12
4.6.3	Procedure.....	13
4.6.4	Urgente changes	13
4.6.5	Escalatie Change afhandeling	14
4.7	Release Management	14
4.8	Service Window	14
4.9	Beveiliging/Security Management	14
4.9.1	Afspraken.....	14
4.9.2	Procedure.....	15
	Akkoordverklaring.....	17
Bijlage 1:	Communicatie en escalatie.....	18

1 Over dit document

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

De gemaakte afspraken hebben onder andere betrekking op:

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

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

Voor definities en afkortingen wordt verwezen naar het Programma van Eisen en de SLA.

2 Algemeen

2.1 Doel

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

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

2.2 Looptijd

Het DAP heeft dezelfde looptijd als de SLA.

3 Communicatie overlegstructuur

Voor het melden van Incidenten en het doorgeven van wijzigingsverzoeken, maken Opdrachtgever en Leverancier gebruik van de contactgegevens zoals opgenomen in het DAP.

3.1 Communicatie

De dagelijkse communicatie tussen Opdrachtgever en Leverancier verloopt in beginsel altijd tussen de Servicedesk VOR-IN en de Helpdesk van Leverancier.

3.2 Overleg

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

Overleg	Onderwerpen	Frequentie	Deelnemers	Documenten
Tactisch	• Output onderhoudsoverleg • Evaluatie Beheer en Onderhoud • Geplande en uitgevoerde Upgrades • Lopende en toekomstige Ontwikkelingen Leverancier • Gewenste ontwikkelingen Opdrachtgever	1x per jaar	• Assetmanager Gemeente • Contract Manager Gemeente • Account Manager Leverancier • <<aanpassen / aanvullen>>	• Notulen • Besluiten/actielijst • Ingebrachte stukken onderhoudsoverleg • Roadmap • Contactoverzicht • Informatiebeveiliging documenten
Onderhoud	• Operationele resultaten aan de hand van Service Management rapportage • Ernstige problemen of afwijkingen op de geleverde dienstverlening • Wijzigingen aan DAP en DFA	1x per kwartaal	• Functioneel beheerder Gemeente • Service Manager Leverancier • <<aanpassen / aanvullen>>	• Notulen • Besluiten/actielijst • Service Management rapportage • Autorisatiematrix • Releasekalender

Tijdens het onderhoudsoverleg worden alle opgetreden incidenten en gedefinieerde problemen besproken. Indien nodig of gewenst, zijn aanvullende deelnemers aan dit overleg aanwezig, waaronder de Problem Manager van Leverancier. Tijdens de bespreking van de incidenten en Problems worden geen incidenten of problemen opgelost, maar vindt beoordeling en besluitvorming over de voortgang plaats.

4 Proces afspraken en procedures Beheer

4.1 Afspraken algemeen

Voor de dienstverlening zijn Serviceperioden overeengekomen waarbinnen de dienstverlening bewaakt en beheerd wordt, alsmede een Helpdesk beschikbaar is voor ondersteuning. De Service Levels zijn per Serviceperiode en Urgentieniveau overeengekomen.

4.2 Klachten

Opdrachtgever kan zich bij een klacht of opmerking op de werkzaamheden van Leverancier richten tot de Helpdesk van Leverancier. Indien een klacht of opmerking niet naar tevredenheid van Opdrachtgever wordt afgehandeld kan Opdrachtgever escaleren middels de escalatieprocedure.

4.3 Escalatie

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

De volgende escalatieniveaus kunnen achtereenvolgens worden doorlopen <<aanpassen indien nodig>>:

Niveau	Opdrachtgever	Leverancier
Operationele escalatie	Functioneel beheerder	Service manager
Tactische escalatie	Assetmanager	Business Unit Manager
Strategische escalatie	Hoofd Stedelijk Beheer	Directeur

De namen behorende bij de functies zijn opgenomen in bijlage 1: Communicatie en Escalatie.

4.4 Helpdesk

In beginsel is de Helpdesk van Leverancier het centrale en enige contactpunt voor Opdrachtgever Servicedesk VOR-IN voor alle operationele communicatie over de dienstverlening. De Helpdesk draagt zorg voor het herstel van de afgesproken dienstverlening, volgens in de met Opdrachtgever overeengekomen SLA.

Communicatie en meldingen zoals vragen, Incidenten, opdrachten of klachten die betrekking hebben op de dienstverlening, komen vanaf Opdrachtgever Servicedesk VOR-IN. Servicedesk VOR-IN medewerkers en de personen en/of afdelingen uit de tabel in bijlage 1: Communicatie en Escalatie zijn gerechtigd om Incidentmeldingen te doen.

4.4.1 Afspraken

De Helpdesk voert de Nederlandse taal. De tweede en verdere lijnondersteuning mag in het Engels.

Tijdens de serviceperioden volgens het overeengekomen Service Level kunnen de daartoe geautoriseerde personen en afdelingen van Opdrachtgever bij de Helpdesk van Leverancier terecht voor het volgende:

- Aanmaken/melden van Incidenten of Change
- Terugkoppelen en afmeldingen van incidenten;
- Aanmelden van een klacht;
- Aanmelden van een vraag;
- Ondersteuning in het gebruik;
- Statusupdates Incident, Change, Problem, klacht, escalatie of vraag;
- Verwachte leverdatum opdracht of Change;
- Opleverdocumentatie;
- Communicatie, bezwaren of vragen omtrent gepland Onderhoud.

De openingstijden en bereikbaarheid op basis van de overeengekomen Service Level van de verschillende Servicedesk VOR-IN en Helpdesk Leverancier is als volgt:

	Opdrachtgever	Leverancier
Openingstijden :	<<invullen>>	<<invullen>>
Telefoon :		
E-mail :		

Bij onderling contact wordt onderstaande informatie uitgewisseld, of verzameld ter beantwoording.

- Incidentnummer van de meldende partij;
- titel van het incident met daarin systeemonderdeel en gebeurtenis;
- het urgentieniveau van het Incident;
- beschrijving van het Incident;
- melder van het Incident;
- indien bekend: de oorzaak en de oplossing van het Incident.

Tevens kunnen de Helpdesk en de Servicedesk VOR-IN een passend tijdsinterval afspreken waarbinnen de Servicedesk VOR-IN door de Helpdesk wordt geïnformeerd over de voortgang van de oplossing.

4.4.2 Procedure

Binnengekomen vragen, klachten of Incidentmeldingen worden voorzien van een ticketnummer en geregistreerd in de Service Management tool van Leverancier waarbij de Servicedesk VOR-IN bij aanmelden de urgentie bepaalt. Eventueel kan Opdrachtgever op een later tijdstip de urgentie aanpassen.

Indien Leverancier een Incident constateert, informeert hij de Servicedesk VOR-IN.

Servicedesk VOR-IN registreert een incident in de Service Management Tool van Opdrachtgever.

Nadat de informatie door beide partijen is uitgewisseld, wordt een uniek incidentnummer uitgewisseld waarmee de melding is vastgelegd bij zowel Opdrachtgever en Leverancier.

Binnen de reactietijd wordt een bevestiging van de melding per mail aan Servicedesk VOR-IN gestuurd onder vermelding van het ticketnummer. Indien het ticket door de Helpdesk van Leverancier als incident wordt uitgezet binnen het Incident Management proces van Leverancier zal Leverancier Opdrachtgever pro-actief informatie verstrekken over de voortgang van het opheffen van de gemelde incident.

Na herstel van het Incident informeert de Helpdesk van Leverancier de Servicedesk VOR-IN, binnen de hersteltijd, desgewenst telefonisch maar in ieder geval ook per e-mail met daarin de volgende informatie:

- het interne incidentnummer;
- titel van het incident met daarin systeemonderdeel en gebeurtenis;
- het urgentieniveau van het Incident;
- de hersteltijd van het Incident;
- de oorzaak van het Incident;
- de oplossing van het Incident.

Opdrachtgever bepaalt op basis van door Leverancier geleverde informatie of documentatie over het incident of het herstel geaccepteerd is en het ticket wordt afgesloten.

4.5 Incident Management

Incident Management betreft het zo snel mogelijk herstellen van de functionaliteit van de dienstverlening.

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

Voor beveiliging/security incidenten gelden afwijkende afspraken.

Zie hiervoor de paragraaf Beveiliging/Security Management.

4.5.1 Prioriteiten Incidenten

Leverancier heeft een contactpersoon aangesteld die door Opdrachtgever aangesproken kan worden over de voortgang c.q. afhandeling van een melding of incident.

Bij het aanmelden van het Incident bepaalt Opdrachtgever de urgentie waarmee deze in behandeling genomen dient te worden. De hierbij geldende criteria op de maximale reactietijd en hersteltijd zijn op basis van de SLA. Het bepalen van de prioriteit gebeurt aan de hand van de tabel in de SLA.

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

4.5.2 Procedure

Het afhandelen van Incidenten kent de volgende stappen:

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

Aanmelden en registreren Incident

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

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

Een Incidentmelding vanaf Opdrachtgever wordt altijd bij de Helpdesk van Leverancier gedaan. De Helpdesk van Leverancier onderzoekt de melding of deze door de Helpdesk zelf opgelost kan worden. Indien de Helpdesk de melding niet zelf kan oplossen wordt de melding "doorgezet" naar het Incident Management proces van Leverancier waarna het incident in behandeling wordt genomen, conform de procedure onder 4.4.2

Voortgang van een Incident

Over de voortgang bij het oplossen van een Incident wordt de Servicedesk VOR-IN volgens het afgesproken tijdsinterval geïnformeerd. Dit gebeurt totdat het Incident is opgelost naar het oordeel van Opdrachtgever en de dienstverlening weer volledig beschikbaar is.

Wanneer het Incident niet binnen de overeengekomen Hersteltijd kan worden opgelost wordt Servicedesk VOR-IN 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. Opdrachtgever zal als gevolg van het overschrijden van de oplostijd eventueel besluiten om te escaleren.

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

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

Afmelden van een Incident

Een Incident wordt in overleg met Opdrachtgever definitief afgesloten waarbij Opdrachtgever het eindoordeel doet. De afmelding wordt in ieder geval gedaan per e-mail bij Servicedesk VOR-IN. Indien het een Incident met Urgentieniveau Kritiek betreft, wordt deze tevens telefonisch afgemeld en volgt binnen 3 werkdagen een Root Cause Analyse (RCA) welke door Leverancier wordt opgesteld. Binnen 1 werkdag heeft Opdrachtgever de mogelijkheid het Incident te laten heropenen indien de oplossing niet volstaat.

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 Problem behandeld moet worden.

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

Van repeterende Incidenten wordt een Problem ticket aangemaakt welke bij Problem Management voor nader onderzoek wordt belegd. De Servicedesk VOR-IN wordt door de Helpdesk van Leverancier geïnformeerd dat een Problem ticket is aangemaakt en de wijze waarop tot een oplossing van de repeterende incidenten wordt gewerkt.

Escalatie Incident Management

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

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

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

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

4.6 Change Management

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

Changes kunnen zowel door Opdrachtgever of Leverancier geïnitieerd worden. Patches, bugfixes en Updates behoren opgenomen te zijn in de Vergoeding. Dit geldt tevens voor de security patches.

4.6.1 Algemeen

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

Hiernaast wordt onderscheid gemaakt in Niet-Standaard Changes, Standaard Changes of Urgente Changes.

Leverancier maakt voor elke Urgente en Standaard Change (Update) een inschatting van de impact op de operationele status en het risico op nieuwe Incidenten en legt deze vast in het RFC formulier. Hierin is ook een risicoanalyse van de Change opgenomen en te nemen mitigerende maatregelen. Leverancier stelt tevens voor of de wijziging direct in de productieomgeving kan plaatsvinden of eerst in de acceptatieomgeving getest moet worden. Opdrachtgever beoordeelt het RFC formulier.

Leverancier maakt voor elke Niet-Standaard Change (grotere wijziging of Upgrade) een impactanalyse en legt deze vast in het RFC formulier. Het uitgangspunt is dat Upgrades eerst worden getest in de acceptatieomgeving. Vóór elke Upgrade voert leverancier een penetratietest en vulnerability scan uit, met als doel aan te tonen dat er geen kwetsbaarheden in de software zitten. Hierbij wordt de OWASP® top 10 voor applicaties en API's gehanteerd.

Het RFC van een Niet-Standaard Change wordt behandeld in de CAB van Opdrachtgever. Pas na akkoord van de CAB wordt de Change ingepland. Opdrachtgever kan op basis van de impactanalyse besluiten van dit proces af te wijken.

4.6.2 Niet –standaard changes

Voor iedere wijziging stelt Leverancier een impactanalyse op, bij Upgrades inclusief kostencalculatie. De impactanalyse plus kostencalculatie worden verstuurd naar Opdrachtgever. Opdrachtgever verzorgt de verdere afstemming binnen Opdrachtgever en zal Leverancier informeren over de uitkomst van de afstemming.

Ten behoeve van de afstemming is het mogelijk dat het wijzigingsverzoek wordt doorgeleid naar de Change Advisory Board (CAB) van Opdrachtgever waarvoor Leverancier kan worden uitgenodigd. In het CAB wordt besloten over de change, rekening houdend met kosten, impact, planning en andere lopende wijzigingsprocedures. Na goedkeuring wordt de Change in gang gezet.

Niet-standaard Changes, worden eerst door de Leverancier getest in de testomgeving. De resultaten worden in een testrapport vastgelegd en beschikbaar gesteld aan Opdrachtgever.

Niet-standaard Changes worden eerst getest in de acceptatie omgeving. Pas na geslaagde testen vindt de wijziging plaats in de productie omgeving. Standaard Changes waarbij geen lage impact en laag risico worden voorzien, worden eveneens getest eerst in de Acceptatieomgeving getest.

4.6.3 Procedure

Niet-standaard Changes worden minimaal 5 werkdagen vooraf ingepland in overleg met de functioneel beheerder van Opdrachtgever. Standaard Changes worden minimaal 2 werkdagen vooraf ingepland. Urgente Changes ten gevolge van Kritieke Incidenten kunnen in overleg op kortere termijn worden doorgevoerd.

Een Change wordt door Helpdesk van Leverancier aangemeld bij de Servicedesk VOR-IN. Daarbij wordt ten minste de geplande start- en eindtijd van de wijzigingswerkzaamheden opgenomen, alsmede de release notes (zie hieronder). De Servicedesk VOR-IN registreert wijzigingen in het service management systeem van Opdrachtgever en monitort de voortgang in afstemming met de functioneel beheerder en Leverancier.

Van alle wijzigingen aan de IDMA houdt Leverancier een historie bij in de vorm van release notes. Deze release notes worden bij elke aankondiging van een wijziging verstuurd naar de Servicedesk VOR-IN en de functioneel beheerder.

Implementatie van de Change

Change management van Leverancier coördineert de implementatie van de wijziging.

Er worden geen Changes uitgevoerd zonder dat hiervoor toestemming door Opdrachtgever is verleend. Indien er bedienongemak ontstaat wordt kort voor aanvang van de Change afgestemd met Verkeersgeleiding of de Change kan plaatsvinden. Dit kan er toe leiden dat de Change op een later tijdstip of datum moet plaatsvinden.

Betreft het een omvangrijke wijziging dan wordt regelmatig over de voortgang van de implementatie gecommuniceerd naar Opdrachtgever.

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

Afsluiten van de Change

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

4.6.4 Urgente changes

Urgente changes zijn RFC's met een spoedeisend karakter om deze zo snel mogelijk door te voeren. Veelal vormen ernstige verstoringen (incidenten met een Urgentieniveau Kritiek) of Escalaties de reden voor een Urgente Change.

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

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

4.6.5 Escalatie Change afhandeling

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

4.7 Release Management

Leverancier draag zorgt voor releasemanagement. Dit houdt in dat Changes zo mogelijk worden gecombineerd om de impact op de operatie zoveel mogelijk te beperken. Daartoe stelt Leverancier een releasekalender planning op met minimaal:

- (periodieke) Updates van de Applicatie;
- Voorziene aanpassingen aan- danwel toevoeging van koppelingen;
- Updates aan licenties en noodzakelijke software derden.

De releasekalender wordt door Opdrachtgever aangevuld met perioden waarin geen releases mogen plaatsvinden, wegens geplande evenementen of andere voorziene situaties waarin onbeschikbaarheid van de applicatie ongewenst is.

4.8 Service Window

Geplande downtime van de applicatie vindt plaats tijdens het service window van Opdrachtgever, namelijk op werkdagen tussen 10:00 en 15:00 uur, na instemming van Opdrachtgever én mits er op het daadwerkelijke moment dat de werkzaamheden plaatsvinden geen bezwaren zijn vanuit de operatie (verkeersleiding).

<<nadere beschrijving van de wijze waarop contact met verkeersleiding plaatsvindt>>

Het is mogelijk dat Opdrachtgever op termijn andere service windows vaststelt. Opdrachtgever en Leverancier treden dan in overleg over de consequenties.

4.9 Beveiliging/Security Management

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

4.9.1 Afspraken

Leverancier heeft een ISMS (Information Security Management System). Dit ISMS dekt minimaal de dienstverlening aan Opdrachtgever af.

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

Beveiligingsorganisatie, logische beveiliging

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

Leverancier legt ten behoeve van Opdrachtgever een lijst aan van alle beheerders die handelingen uitvoeren op de systemen van Opdrachtgever en onderhoudt deze. Al deze beheerders beschikken over een VOG (Verklaring Ontremd het Gedrag) en een getekende integriteit- en geheimhoudingsverklaring (I&G) van de gemeente Amsterdam. Bij de eerste inzet van een beheerder toont Leverancier de originele VOG van deze beheerder aan Opdrachtgever.

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

4.9.2 Procedure

Beveiligingsincident en Prioriteiten

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

Beveiligingsincidenten worden middels het reguliere Incident proces afgehandeld met Urgentieniveau Kritiek en worden de Security Officers van Opdrachtgever en Leverancier betrokken bij de afhandeling/opvolging. Als Leverancier constateert dat mogelijk sprake is van een Incident met als gevolg van een "Security-breach" (inbraak op de beveiliging) dan dient direct contact opgenomen te worden met de Security Officer van Opdrachtgever. Elk beveiligingsincident wordt afgesloten met een Root Cause Analysis (RCA). De rapportage over beveiligingsincidenten is verwerkt in de Service Management rapportage. Daarnaast rapporteert Leverancier maandelijks separaat over de opvolging van beveiligingsincidenten en -problems.

Beveiligingsprobleem

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

Bij een beveiligings-Problem zal te allen tijde de Security Managers van Opdrachtgever en Leverancier worden betrokken voor het bepalen van de impact en de afhandeling c.q. opvolging waarbij ieder beveiligings-Problem zal worden afgesloten met een Root Cause Analysis (RCA). De rapportage over beveiligings-Problems is verwerkt in de Service Management rapportage.

De bevindingen uit penetratie- en hacktesten, audits en vulnerability scans worden door Leverancier gerapporteerd en met Opdrachtgever besproken. Leverancier en Opdrachtgever dragen op eigen kosten zorg voor het oplossen van de bevindingen in de eigen omgeving, die naar oordeel van Opdrachtgever niet acceptabel zijn.

Akkoordverklaring

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

Aldus overeengekomen te <<locatie>> en in tweevoud ondertekend,

	Leverancier		Opdrachtgever
Datum		Datum	
Naam		Naam	
Functie		Functie	
Handtekening Leverancier		Handtekening Opdrachtgever	

Bijlage 1: Communicatie en escalatie

Algemene communicatie contacten

Partij	Naam	Rol / functies	Telefoon	E-mail

Escalatie matrix

Niveau	Opdrachtgever	Leverancier
Operationele escalatie		
Tactische escalatie		
Strategische escalatie		

Geautoriseerde personen en afdeling voor het doen van meldingen

Medewerker / Afdeling	Rol	Telefoon	E-mail