Bijlage F - Concept Dossier Afspraken Procedures (DAP)

Bijlage F -Concept Dossier Afspraken Procedures (DAP)

Inhoudsopgave

Bijlage F -Concept Dossier Afspraken Procedures (DAP)

1 Inleiding

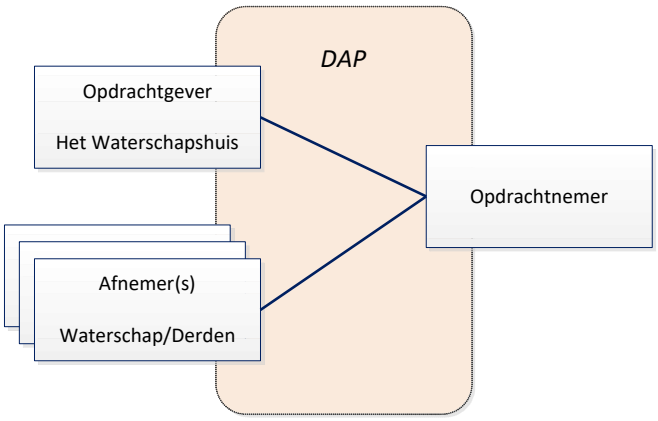
1.1 Doelstelling

Het Dossier Afspraken Procedures (DAP) is een bijlage van de Hoofdovereenkomst <naam overeenkomst> tussen Opdrachtgever Het Waterschapshuis (hWh) en Opdrachtnemer <opdrachtnemer>. De looptijd van de DAP is gelijk aan de looptijd van de Overeenkomst.

Het DAP bevat de uitwerking van afspraken en procedures die betrekking hebben op de dagelijkse samenwerking en interactie bij het uitvoeren van de dienstverlening tussen Opdrachtnemer en de deelnemende partijen, verder benoemd als deelnemers. Hierbij zijn functies, rollen, bevoegdheden en verantwoordelijkheden van betrokkenen vastgesteld en vastgelegd. Het DAP is een levend document dat aansluit bij de dagelijkse praktijk en het zal daarom regelmatig worden bijgesteld op basis van ervaring en nieuwe afspraken.

1.2 Scope

De scope van het DAP betreft de interfaces tussen Opdrachtgever, de Deelnemers en de Opdrachtnemer. Het DAP dekt niet de interne communicatie en werkwijzen van de verschillende partijen af, tenzij deze direct van invloed zijn op de interfaces tussen partijen.



Figuur 1 - Scope DAP

1.3 Gehanteerde begrippen

In de Overeenkomst en in Bijlage A bij deze DAP is een aantal begrippen nader omschreven.

1.4 Beheer en onderhoud DAP

Periodiek zal een evaluatie en eventuele bijstelling van de afspraken en procedures tussen Opdrachtnemer, Opdrachtgever en een delegatie van de Deelnemers plaatsvinden.

De beheerders van de DAP zijn de Service Coördinator van de Opdrachtnemer en de Service Coördinatoren van de deelnemers. Wijzigingsvoorstellen worden door de beheerders van de DAP ter goedkeuring voorgelegd aan de Service Delivery verantwoordelijke van de betreffende deelnemer, de Service Delivery Manager van de Opdrachtgever en aan de Servicemanager van de Opdrachtnemer.

2 Rollen, taken en verantwoordelijkheden

2.1 Deelnemers

2.1.1 Security specialist

Elke deelnemer heeft 1 of meerdere security-specialisten. Het zijn de aanspreekpunten voor de SOC-analisten voor het melden van security incidenten of geconstateerd verdacht gedrag op basis van de logdata. Daarnaast zal de security-specialist deel uitmaken van het use case management team voor onderhoud en uitbreiding van de use cases die door de dienst worden afgedekt.

2.1.2 Delivery coördinator

Binnen elke deelnemer is een Delivery Coördinator actief. De coördinator geeft aan wie geautoriseerd zijn voor de rol Delivery Coördinator. Het overzicht van geautoriseerde delivery coördinatoren wordt up-to-date gehouden door de Helpdesk.

De communicatie over de afhandeling van een melding loopt tussen de melder (de Aanmelder) en Helpdesk. De Delivery Coördinator wordt op de hoogte gehouden van het totaal aan meldingen, de aard van de meldingen en de details van de afhandeling van de meldingen.

Taken en verantwoordelijkheden:

1. Periodiek evalueren van de kwaliteit van de geleverde dienstverlening;
2. Overzicht houden van meldingen, incidenten en wijzigingsverzoeken vanuit de organisatie;
3. Accepteren van (gewijzigde) dienst-functionaliteit namens zijn/haar organisatie ten behoeve van formele acceptatie door hWh richting de Opdrachtnemer.

2.2 Opdrachtnemer

N.B.: verschillende rollen kunnen binnen een organisatie door dezelfde persoon worden vervuld.

2.2.1 Servicedesk (1e lijn)

De Servicedesk binnen de Opdrachtnemersorganisatie is verantwoordelijk voor het aannemen, registreren, prioriteren volgens richtlijnen, (laten) afhandelen, bewaken en afmelden van meldingen. De Servicedesk is gedurende de openstelling het aanspreekpunt voor de deelnemers. De Servicedesk zal meldingen die ze niet direct kan afhandelen doorzetten naar de juiste Afhandelgroep.

Taken en verantwoordelijkheden:

1. Aannemen, registreren, monitoren en terug melden van meldingen.
2. Routeren van meldingen naar de specialisten van de juiste afhandelgroep.
3. Verantwoordelijk voor de bewaking van de afgesproken Servicelevels van de beheerprocessen.
4. Coördinator voor meldingen waarbij een derde is betrokken.

2.2.2 Afhandelgroep (2e lijn)/ specialisten

De Afhandelgroepen binnen de Opdrachtnemersorganisatie zijn teams van specialisten die verantwoordelijk zijn voor het afhandelen van meldingen die niet direct door de Servicedesk afgehandeld kunnen worden.

Taken en verantwoordelijkheden:

1. Uitvoeren van specialistische beheer- en onderhoudsactiviteiten.
2. Op peil houden van hun materiedeskundigheid.
3. Nemen van technische, operationele beslissingen binnen de kaders en richtlijnen van de Opdracht en de aanwijzingen van de Service Coördinator.
4. Verantwoordelijk voor het uitvoeren van beheer- en onderhoudsactiviteiten t.a.v. de dienstverlening.

2.2.3 Service Coördinator

De Service Coördinator binnen de Opdrachtnemersorganisatie is verantwoordelijk voor de uitvoering van de Overeenkomst en voor het in overeenstemming brengen van de afgesproken dienstverlening, conform de SLA, met de geboden dienstverlening.

Taken en verantwoordelijkheden:

1. Verantwoordelijk voor de levering van de afgesproken dienstverlening.
2. Zorgen voor de afstemming en coördinatie met de Servicedesk en de afhandelgroepen.
3. Rapporteren aan hWh over de voortgang, eventuele knelpunten signaleren en aandragen van oplossingen.
4. Formuleren van verbetervoorstellen voor de dienstverlening.

2.2.4 Service Manager

1. Aanspreekpunt in de business relatie.
2. Bewaken financiële en juridische verplichtingen uit de Overeenkomst.
3. Eindverantwoordelijk voor de uitvoering van de Overeenkomst namens de Opdrachtnemer.

2.3 Opdrachtgever

N.B.: verschillende rollen kunnen binnen een organisatie door dezelfde persoon worden vervuld.

2.3.1 Service Delivery Manager

De evenknie van de Service Coördinator aan de zijde van Opdrachtgever is de Service Delivery Manager (SDM). Hij/zij ziet, samen met de contractmanager, toe op de kwaliteit van de dienstverlening, de uitvoering van de Overeenkomst en het bewaken van de SLA. De SDM dient als eerste escalatieniveau.

Taken en verantwoordelijkheden:

1. Beoordelen van de geleverde dienstverlening in relatie tot afgesproken dienstverlening.
2. Indienen van opdrachten voor de realisatie van Wensen en Wijzigingen.

2.3.2 Contractmanager

De evenknie van de Service Manager van de Opdrachtnemer aan de zijde van de Opdrachtgever is de contractmanager.

Taken en verantwoordelijkheden:

1. Aanspreekpunt in de business-relatie.
2. Bewaken financiële en juridische verplichtingen uit de Overeenkomst.
3. Eindverantwoordelijk voor de uitvoering van de Overeenkomst namens de Opdrachtgever.

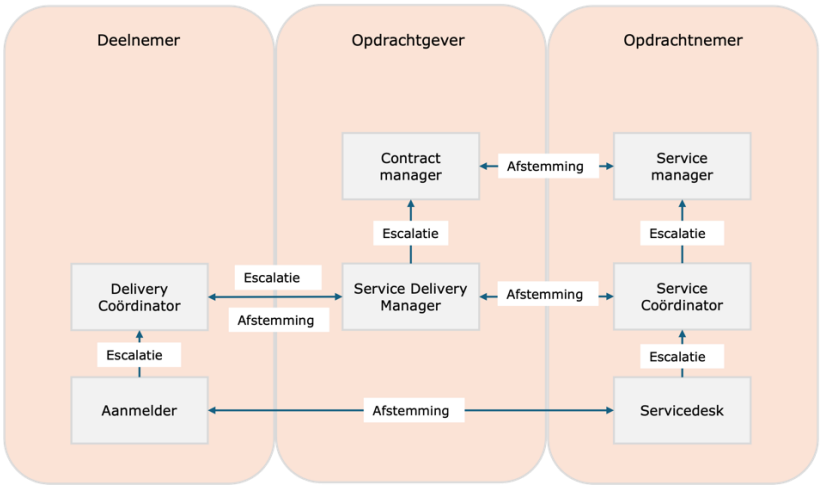
2.4 Escalatie

Escalatie treedt in werking naar aanleiding van:

- Ernstige Verstoringen in de dienstverlening,
- (Dreigende) overschrijding van afhandeltijden van meldingen, met name bij meldingen met Prioriteit 1,
- Disputen over de kwaliteit van de dienstverlening.

Escalatie wordt opgestart door de Service Coördinator en/of SDM'er. Afhankelijk van de aanleiding van de escalatie worden de relevante functionarissen betrokken. Frequentie van escalatie-overleg kan variëren.

Escalatie vindt altijd plaats volgens de gedefinieerde niveaus in de figuur hieronder.



Figuur 2 – Escalatieniveaus

Voor de **escalatie-procedure** worden de volgende stappen doorlopen:

1. Bepalen welke partijen en disciplines betrokken zijn
2. Escalatie-overleg plannen & uitvoeren
3. Resultaat: afspraken incl. planning

Indien nodig wordt het escalatie-overleg herhaald, totdat het onderhavige issue is opgelost.

3 Tooling

3.1 Meldingenregistratietool

In deze paragraaf worden een aantal eisen gesteld aan de meldingenregistratietool, waarmee de processen zoals beschreven in het volgende hoofdstuk worden ondersteund.

1. De tool is Nederlandstalig en is via het internet te benaderen door de deelnemers;
2. Deelnemers kunnen via het internet de meldingen aanmaken;
3. Aanmelder krijgt een email nadat de status van de melding is aangepast;
4. Deelnemers kunnen via het internet de melding updaten met nieuwe informatie nadat Opdrachtnemer de Melding heeft aangepast.
5. Deelnemers kunnen alleen hun eigen meldingen zien.
6. Een overall rapportage zonder inhoudelijke details is beschikbaar voor Opdrachtgever;
7. De tool geeft inzicht in het verloop van het proces van de melding;
8. De tool bevat door de Opdrachtnemer opgestelde rapportages zoals beschreven in de SLA. De tool biedt de mogelijkheid om Prioriteit en Urgentie in te kunnen vullen door de Aanmelder;

3.2 Toegang

Per deelnemer zal op aangeven van de Delivery Coördinator een of meerdere useraccounts voor het raadplegen van meldingen in het meldingenregistratietool door de Servicedesk worden aangemaakt. Deze gebruikers ontvangen per email daartoe een gebruikersnaam en wachtwoord.

3.3 Rapportages

De tool bevat rapportages zoals in de SLA aangegeven.

4 Meldingen

Er kan sprake zijn van verschillende typen meldingen die de Indiener kan indienen:

- Incident;
- Wijzigingsverzoek;
- Serviceverzoek.

Al deze meldingen komen binnen bij hetzelfde loket: de Servicedesk.
Wijzigingsverzoeken: alleen de Delivery Coördinator van deelnemers of de Service Delivery Manager van de Opdrachtgever zijn geautoriseerd om Wijzigingsverzoeken in te dienen.

In de behandeling van de meldingen wordt gebruikt gemaakt van de in de markt gangbare ITIL-processen. Voor deze DAP betekent dit:

- Incident & Service Request Management (incidenten en serviceverzoeken)
- Change Management

In het verdere document wordt gerefereerd aan de gangbare ITIL termen.

5 Incident en Service Request management

5.1 Type Service aanvragen

5.1.1 Incident

Aanmelders van deelnemers kunnen incidenten opvoeren in het serviceportaal van Opdrachtnemer. Een incident omvat iedere gebeurtenis die geen onderdeel is van de standaard werking van de dienst en een onderbreking of vermindering van de kwaliteit van de dienst veroorzaakt.

5.1.2 Service Request

Aanmelders van deelnemers kunnen service requests opvoeren in het serviceportaal. Een service request is geen verstoring van de dienstverlening, maar omvat verzoeken om een taak uit te voeren of een vraag te beantwoorden. Een voorbeeld van een service request is het verzoek tot het aansluiten van een nieuwe of gewijzigde data bron.

5.2 Servicedesk

5.2.1 Korte beschrijving van de taak van de servicedesk

De servicedesk is verantwoordelijk voor het aannemen en de opvolging van meldingen. Hiertoe behoort de verantwoordelijkheid om binnenkomende meldingen aan de juiste personen toe te wijzen, zodat deze succesvol kunnen worden afgehandeld. Het contact tussen een deelnemer en de servicedesk verloopt primair via het serviceportaal. Bij onduidelijkheden of meldingen met een hoge prioriteit kan er ook aanvullend telefonisch contact zijn met de servicedesk. Als het telefonische contact een verzoek of andersoortige werkzaamheden tot gevolg heeft, dient de deelnemer altijd een request in het serviceportaal aan te maken.

5.2.2 Korte beschrijving hoe de communicatie verloopt

Meldingen worden gedaan door een aanmelder in het beschikbaar gestelde serviceportaal. Een servicedeskmedewerker stuurt (al dan niet geautomatiseerd) bij het ontvangen van de melding een bevestiging. Indien nodig neemt de servicedesk contact op met de aanmelder voor extra informatie. Zodra de melding is afgerond wordt een update naar de aanmelder gestuurd met de vraag of de melding naar verwachting is afgerond. De aanmelder accepteert de geboden oplossing en de melding wordt gesloten. Indien de melding niet naar verwachting is afgerond neem de servicedesk de melding opnieuw in behandeling. Bij het melden van een prioriteit 1 incident (noodgeval), is de afspraak dat de aanmelder ook telefonisch contact opneemt met de servicedesk. Indien het uitvoeren van een melding dreigt langer te gaan duren dan de daarvoor geldende SLA tijden, dan neemt Opdrachtnemer tijdig contact op met de betreffende deelnemer.

5.2.3 Telefonisch

Naast het serviceportaal is de servicedesk telefonisch bereikbaar voor vragen, in het geval van een prioriteit 1 incident en overige zaken waarvoor telefonisch contact noodzakelijk is. Het algemene telefoonnummer van de servicedesk is:
<Telefoonnummer>

5.2.4 E-mail

De mailbox van de servicedesk wordt van maandag t/m vrijdag van 08.00 tot 18.00 uur voortdurend in de gaten gehouden voor nieuwe mail. Hier sturen deelnemers aankondigingen en informatie naartoe die relevant is voor de dienst. Hieronder vallen bijvoorbeeld het aankondigen van wijzigingen aan de kant van een deelnemer, het aankondigen van zogenaamde change-freezes bij een deelnemer, personele wisselingen en andere zaken die relevant zijn.

Voor communicatie via email is het volgende e-mailadres is beschikbaar: <emailadres>

5.3 Geautoriseerde medewerkers per deelnemer

Niet alle medewerkers zijn geautoriseerd om changes door te geven of een service request te accorderen met financiële consequenties. Een overzicht van de geautoriseerde personen is te vinden in de bijlage.

5.4 Aan-en afmelden van meldingen

Meldingen worden geregistreerd in het serviceportaal. Hieronder staat per aanvraag type vermeld welke informatie nodig is om een melding adequaat af te handelen:

Incident:

- Samenvatting: Een omschrijving van het incident in één regel;
- Indien van toepassing klant-referentienummer (bijv. Het ticket vanuit service managementsysteem van deelnemer);
- Omschrijving: Een zo volledig mogelijke omschrijving van het incident. Denk hierbij aan de volgende punten:
    - Omschrijving van het incident;

- Sinds wanneer speelt het incident;
- Heeft dit wel gewerkt;
- Wat zijn de stappen om het incident te kunnen reproduceren;
- Voorbeelden van het incident;
- Omschrijving van de impact en urgentie van het incident;

- Componenten: Hier kunnen de componenten waarop het incident van toepassing is geselecteerd worden;
- Bijlage: Hier kunnen bijlages worden toegevoegd, bijvoorbeeld screenshots of bestanden;
- Urgentie: Hier kan de urgentie worden ingegeven zoals die omschreven staat in het SLA document;
- Impact: Hier kan de impact worden ingegeven zoals die omschreven staat in het SLA document.

Service request:

- Samenvatting: Een omschrijving van het service request in één regel;
- Indien van toepassing klant-referentienummer (bv het ticket vanuit service managementsysteem van deelnemer);
- Omschrijving: Een zo volledig mogelijke omschrijving van het service request;
- Componenten: Hier kunnen de componenten waarop het service request van toepassing is geselecteerd worden;
- Bijlage: Hier kunnen bijlages worden toegevoegd, bijvoorbeeld screenshots of bestanden;
- Impact: Hier kan de impact worden ingegeven, let wel, dit is om een indruk te geven van de impact. Een service request heeft nooit een hogere prioriteit dan 4;
- Urgentie: Hier kan de urgentie worden ingegeven, let wel, dit is om een indruk te geven van de urgentie. Een service request heeft nooit een hogere prioriteit dan 4.

Zodra het incident is opgelost of het request uitgevoerd, wordt de aanmelder geïnformeerd en gevraagd of de melding naar wens is afgehandeld en of de aanmelder het resultaat accepteert. Op basis van de acceptatie wordt de aanvraag gesloten.

5.5 Incidentproces

Het incidentproces bestaat uit vier stappen:

- Incident ticket
- Incident beoordelen
- Incident oplossen
- Incident evalueren/opvolgen

Hieronder worden de vier stappen in meer detail besproken.

5.5.1 Incident ticket

Voor het aanmelden van een incident registreert deelnemer een incident in het serviceportaal. Hierin dient voldoende informatie opgenomen (zie 2.5 Aan-en afmelden van aanvragen) te worden zodat de servicedesk het incident adequaat kan opvolgen. Indien het een prioriteit 1 incident betreft, oftewel impact hoog en urgentie hoog, dan belt de aanmelder na het opvoeren van het incident ticket de servicedesk om het incident ook telefonisch onder de aandacht te brengen. Op

het ontvangen van de incidentmelding wordt een ontvangstbevestiging gestuurd, aan de aanmelder van het incident.

5.5.2 Incident beoordelen

Na ontvangst beoordeelt de servicedesk het incident. In deze fase wordt gecontroleerd of er voldoende informatie is om de incidentmelding op te pakken. Indien de informatie onvoldoende of onduidelijk is, wordt om aanvullende informatie gevraagd. Daarnaast wordt beoordeeld of de melding wel een incident is. Als het geen incident is, dan zijn er twee mogelijkheden, het gaat om een service request of het gaat om een change verzoek. Als het een service request is, wordt het afgehandeld. Als het een change verzoek is, wordt de melder gevraagd om een change in te dienen en wordt de incidentmelding gesloten met vermelding van de reden. Daarnaast beoordeelt de servicedesk of de prioriteit, die gebaseerd is op de door de melder gekozen impact en urgentie, correct is. Indien de servicedesk de prioriteit als niet passend beoordeelt, wordt deze aangepast en toegelicht aan de melder. Indien hierover een verschil van mening bestaat, wordt dit op operationeel niveau afgestemd tussen de servicedesk en de service coördinator van de deelnemer, om zo tot overeenstemming te komen.

5.5.3 Incident oplossen

In deze fase worden de werkzaamheden uitgevoerd die nodig zijn om de verstoring weg te nemen. De servicedesk voert een diagnose uit en lost het incident op. De oplossing kan een permanente oplossing zijn of een tijdelijke workaround. Bij een tijdelijke workaround wordt een ‘probleem’ aangemaakt (problem management) om de achterliggende oorzaak te onderzoeken en een permanente oplossing te vinden en toe te passen.

5.5.4 Incident evalueren/opvolgen

Zodra het incident is opgelost of een tijdelijke workaround beschikbaar is, wordt de oplossing of workaround aangeboden aan de aanmelder ter acceptatie. Als het resultaat wordt geaccepteerd, wordt de incidentmelding afgesloten. Als het resultaat niet geaccepteerd wordt, wordt de melding opnieuw opgepakt door de servicedesk. Afhankelijk van het incident en de geboden oplossing/workaround kan ervoor gekozen worden om het incident op te volgen in de vorm van een ‘problem’. Dit gebeurt in de volgende gevallen:

- Een incident met priority 1 wordt opgevolgd met een problem. Vanuit dit problem wordt er een root cause analyse opgesteld en worden eventuele structurele verbeteringen in de dienst voorgesteld;
- Een incident dat regelmatig voorkomt wordt opgevolgd met een problem. Vanuit dit problem wordt er onderzocht welke structurele oplossingen voor het incident er mogelijk zijn;
- Een incident is opgelost met een tijdelijke workaround. Vanuit dit problem wordt er onderzocht welke structurele oplossingen er mogelijk zijn om de tijdelijke workaround te vervangen.

5.6 Service request proces

Het service request proces bestaat uit vier stappen:

- Service request ticket

- Service request beoordelen
- Service request uitvoeren
- Service request evalueren

Hieronder worden de vier stappen in meer detail besproken.

5.6.1 Service request ticket

Voor het aanmelden van een service request registreert deelnemer een service request melding in het serviceportaal. Hierin dient voldoende informatie opgenomen (zie 2.5 Aan-en afmelden van aanvragen) te worden zodat de servicedesk het service request adequaat kan opvolgen. Na het ontvangen van de service request-melding wordt een ontvangstbevestiging aan de aanmelder van het service request gestuurd.

5.6.2 Service request beoordelen

Na ontvangst beoordeelt de servicedesk het service request. In deze fase wordt gecontroleerd of er voldoende informatie is om de service request-melding op te pakken. Indien de informatie onvoldoende is of onduidelijk, zal de servicedesk om aanvullende informatie vragen. Daarnaast wordt er beoordeeld of de melding wel een service request is. Als het geen service request is, dan zijn er twee mogelijkheden, het gaat om een incident dat vervolgens afgehandeld wordt of het gaat om een change verzoek. Als het om een change verzoek gaat zal de servicedesk de melder verzoeken om een change in te dienen en sluit de service request-melding. Indien hierover een verschil van mening bestaat, wordt dit op operationeel niveau afgestemd tussen de servicedesk en de service coördinator van de deelnemer, om zo tot overeenstemming te komen.

5.6.3 Service request uitvoeren/beantwoorden

In deze fase worden de werkzaamheden uitgevoerd of wordt de vraag die is gesteld beantwoord door de servicedesk.

5.6.4 Service request evalueren

Nadat de werkzaamheden zijn uitgevoerd of nadat de vraag is beantwoord, wordt het resultaat ter acceptatie aangeboden aan de aanmelder. Als het resultaat wordt geaccepteerd, dan wordt de service request melding afgesloten. Als het resultaat niet wordt geaccepteerd, wordt de service request opnieuw in behandeling genomen door de servicedesk.

6 Change management

Gemachtigde medewerkers kunnen change-verzoeken indienen in het serviceportaal. Changes omvatten alle wijzigingen die niet afgevangen worden binnen de Service Requests. Een voorbeeld van een change is het verzoek voor het bouwen van een nieuw rapportage-dashboard.

Naast de changes die geïnitieerd worden vanuit een deelnemer zullen er ook changes zijn die geïnitieerd worden vanuit de Opdrachtnemer.

6.1 Change redenen

Er zijn meerdere redenen om een change uit te voeren. Hieronder staat een overzicht van deze redenen.

- Herstel: Om iets te herstellen dat eerder voor een verstoring in de dienstverlening heeft gezorgd. De aanleiding hiervan is een incident of problem. Deze changes worden geïnitieerd vanuit de Opdrachtnemer;
- Upgrade: Om te voorkomen dat er een verstoring komt. Deze changes worden geïnitieerd vanuit Opdrachtnemer;
- Nieuwe functionaliteit: Om nieuwe functionaliteit aan de dienst toe te voegen of op andere wijze een aanpassing op de dienst te doen. Deze changes worden geïnitieerd vanuit een deelnemer of hWh. Voor dit soort changes wordt altijd door de Opdrachtnemer een impact/offerte afgegeven ter beoordeling.
- Overig: Alle redenen die niet in bovenstaande vier redenen afgevangen worden.

6.2 Type changes

We onderscheiden drie type changes. Hieronder staat een overzicht van deze types.

1. Standaard change: Een standard change is een change gerelateerd aan de service, die zonder aanvullende toestemming kan worden uitgevoerd. Akkoord is vooraf gegeven, op basis van het type change. Hierbij zijn vaste procedures van toepassing. Een voorbeeld is het uitvoeren van OS-patches;
2. Emergency change: Een emergency change is een change die bedoeld is om een fout in de dienstverlening die in grote mate impact heeft op de productieomgeving, te herstellen. Een dergelijke change moet zo snel mogelijk worden uitgevoerd om verdere impact op de productieomgeving te beperken. De change wordt door de operationele contactpersonen aan de kant van Opdrachtnemer en hWh beoordeeld en geaccordeerd. Indien er aan de kant van hWh na 15 minuten geen contactpersoon beschikbaar is voor het beoordelen en accorderen van de change, dan is Opdrachtnemer gemachtigd om deze change te accorderen zonder beoordeling van de Opdrachtgever;
3. Normale change: Hieronder vallen overige changes. Voor deze changes is er, vanuit zowel Opdrachtgever als Opdrachtnemer, een akkoord nodig voor de inhoud en de planning van de change.

6.3 Change risico categorieën

We onderscheiden vier risicocategorieën voor changes. De risicocategorie geeft aan wat het risico is van een change. De risicocategorie van een change is onafhankelijk van het change type. Zo kan zowel een normale change als een spoed change de risicocategorie kritiek krijgen en een emergency change hoeft niet altijd risico categorie kritiek te krijgen.

- Laag
- Gemiddeld
- Hoog
- Kritiek

6.4 Aanmelden van changes

Changes worden geregistreerd in het serviceportaal. Hieronder staat welke informatie nodig is om changes adequaat af te handelen:

- Samenvatting: Een omschrijving van de change in één regel.
- Indien van toepassing een klant-referentienummer (bv het ticket vanuit service managementsysteem van Opdrachtgever).
- Omschrijving: Een zo volledig mogelijke omschrijving van de change.
- Componenten: Hier kunne de componenten waarop de change van toepassing is geselecteerd worden;
- Bijlage: Hier kunnen bijlages worden toegevoegd, bijvoorbeeld screenshots of bestanden.
- Approvers: Indien er sprake is van nieuwe functionaliteit waarvoor een impact/offerte moet worden afgegeven, dient hier de contactpersoon ingegeven te worden met wie de impact/offerte afgestemd kan worden voor akkoord.
- Impact: Hier kan de impact worden ingegeven, let wel, SLA afspraken worden gehanteerd op incidenten en service requests.
- Urgentie: Hier kan de urgentie worden ingegeven, let wel, SLA afspraken worden gehanteerd op incidenten en service requests.

6.5 Change proces

Het change proces bestaat uit vier stappen:

- Change verzoek
- Change beoordelen en plannen
- Change goedkeuring
- Change implementatie en evaluatie

Hieronder worden de vier stappen in meer detail besproken.

6.5.1 Change registreren

Een changeverzoek wordt geregistreerd in het serviceportaal. Het registreren van een changeverzoek wordt gedaan door Opdrachtgever of Opdrachtnemer, afhankelijk van de reden van de change (zie 3.1 change redenen). In het change-verzoek dient voldoende informatie opgenomen te worden zodat de servicedesk de change adequaat kan beoordelen. De change wordt beoordeeld en eventueel missende informatie aangevuld door de servicedesk waar nodig in samenspraak met de aanvrager. Op basis van die informatie kent de servicedesk een risicocategorie toe aan de change (zie 3.3 change risico categorieën).

6.5.2 Change beoordelen en plannen

In deze stap wordt door de servicedesk een stappenplan opgesteld. In het overzicht staat vermeld op welke onderdelen van de dienst het uitvoeren van de change impact heeft. Daarnaast doet de servicedesk een eerste voorstel voor een change-venster.

6.5.3 Change goedkeuring

Voor emergency en normale changes wordt het stappenplan voor het uitvoeren van de change en het voorstel voor het change-venster worden ter goedkeuring voorgelegd. Voor changes met de

risicocategorie hoog of kritiek wordt de beoordeling hiervan gedaan door het change advisory board (CAB). Voor de changes met andere risicocategorieën wordt de goedkeuring en planning op operationeel niveau afgestemd tussen Opdrachtgever en de Servicedesk. Als het voorstel akkoord is, dan wordt het planningsvoorstel definitief (zie 6.2 voor details over type changes).

6.5.4 Change implementatie en evaluatie

In deze stap worden de werkzaamheden die nodig zijn voor het implementeren van de change uitgevoerd, indien van toepassing samen met Opdrachtgever. Deze werkzaamheden worden binnen het afgesproken change-venster uitgevoerd. Als de werkzaamheden buiten de afgesproken change-venster dreigen te lopen dan wordt er op operationeel niveau afgestemd of het acceptabel is, dat het uitvoeren van de werkzaamheden langer duurt dan gepland. Indien dit niet mogelijk is, wordt het uitvoeren van de change afgebroken, waar nodig een roll-back uitgevoerd en wordt de change opnieuw ingepland. Zodra de werkzaamheden zijn uitgevoerd wordt het resultaat ter acceptatie voorgelegd aan aanvrager. Als deze het opgeleverde resultaat accepteert, wordt de change afgesloten.

6.5.5 Afsluiten

Bij Acceptatie van de afhandeling door de Aanmelder wordt de melding afgesloten in de meldingenregistratie. Ook indien de Aanmelder niet binnen 10 Werkdagen terugkoppeling heeft gegeven of de oplossing werkt. De Aanmelder wordt hierover per e-mail geïnformeerd.

Mocht op enig moment alsnog blijken dat de Servicedesk de melding onterecht heeft afgesloten, wordt de melding heropend.

7 Klachten en escalaties

7.1 Klachten

Bij klachten over de dienstverlening kan er per mail contact opgenomen worden met de Service Manager van Opdrachtnemer EN de Service Delivery Manager van hWh. Op klachten wordt alert gereageerd en er wordt binnen 1 werkdag contact opgenomen met de indiener van de klacht.

7.2 Definitie van een escalatie

Escalatie is een middel dat spaarzaam moet worden ingezet en kan worden gebruikt in de volgende situaties:

- Om extra aandacht te vestigen op een knelpunt in de dienstverlening dat naar oordeel van de deelnemer niet snel genoeg wordt opgelost.
- Bij vraagstukken waar de beantwoording te lang op zich laat wachten.

8 Contactgegevens

8.1 Contactgegevens Opdrachtnemer

Naam	Functie/rol	Telefoonnummer	E-mailadres
	Service Manager		
	Service Coordinator		
	ServiceDesk		

8.2 Geautoriseerde personen Deelnemer

Naam	Functie/rol	Telefoonnummer	E-mailadres
	Delivery Coördinator		

8.3 Contactgegevens Opdrachtgever

Naam	Functie/rol	Telefoonnummer	E-mailadres
	Service Delivery Manager		
	Contractmanager		

Bijlage A: Begrippen en definities

Ten opzichte van de begrippenlijst in de Overeenkomst, worden de volgende aanvullende begrippen gehanteerd:

Term	Definitie
Aanmelder	Persoon die geautoriseerd is om een melding bij de Servicedesk in te dienen.
Afnemer = deelnemer	De partij die de dienst deels of volledig afneemt, waterschappen en waterschap gerelateerde organisaties Afnemer wordt gelijkgesteld aan Deelnemer. Daar waar in dit document 'afnemer' staat vermeld kan ook worden gelezen 'deelnemer'.
Alarmering	Reactie op een gedetecteerd cyberbeveiligingsincident. Het detecteren wordt onmiddellijk gevolgd door een analyse en prioritering van het incident. Een triage levert oplossingsrichtingen en een advies aan de betreffende afnemer hoe het incident kan worden gemitigeerd. Het feitelijk oplossen van het incident (recover) is verantwoordelijkheid van de afnemer. Advies en hulp worden verleend, door CERT-WM en Opdrachtnemer. (zie ook "Respond" uit het NIST Cybersecurity Framework 2.0.
Automatisering	Automatisering definiëren we al het vervangen van menselijke arbeid door machines of computers en computerprogramma's. De drijfveer is economisch: de som van arbeid en grondstofverbruik is na automatisering kleiner dan daarvoor. Er zijn verschillende vormen van automatisering. In deze leidraad gebruiken we de vormen: kantoorautomatisering (KA) en Industriële automatisering (IA). De overige vormen van automatisering laten we buiten beschouwing.
APT	Geavanceerde Persistente Dreigingsgroepen (Advanced Persistent Threat groups)
CIRT	Gartner definitie: Cyber Incident Response Team
CSIR	Cyber Security Implementatie Richtlijn (https://www.cert-wm.nl/csir)
CSIRT	Computer Security Incident Response Team ook wel CIRT genoemd

CERT-WM	Computer Emergency Response Team Water Management
Converged OT & IT SOC	Een 'converged OT & IT SOC' is een SOC dat als één geïntegreerde organisatorische eenheid vanuit een integrale aanpak de OT- en IT-SOC diensten verleent en de OT- en IT-omgeving van de Afnemers beschermt, waarbij: • Door de integratie van OT- en IT-SOC kennis en integratie van het OT- en IT-detectie en -reactieproces incidenten niet tussen separate IT- en OT-teams hoeven te worden overgedragen; • Sprake is van een compleet situationeel bewustzijn van de SOC-teamleden om rekening te houden met de unieke kenmerken en kwetsbaarheden van beide soorten systemen; én • Zowel met de bescherming van de OT als IT kant van de organisatie rekening wordt gehouden, om beveiligingsproblemen adequaat en snel op te lossen.
Deelnemer = afnemer	De partij die de dienst deels of volledig afneemt, waterschappen en waterschap gerelateerde organisaties Afnemer wordt gelijkgesteld aan Deelnemer.
Dienst	De SOC-dienst (Monitoring & Alarmering) die kan worden afgenomen van de Opdrachtnemer. De dienst is voorzien van een dienstbeschrijving, inclusief een indicator voor de eenheid van de af te nemen dienst en een prijs per eenheid (P x Q moet berekend kunnen worden)
Dienstverlener	De partij die diensten aanbiedt, de Opdrachtnemer. In het kader van dit document maken we het volgende onderscheid: • Het Waterschapshuis is Opdrachtgever voor de Opdrachtnemer (zie definitie); • De Opdrachtnemer is de externe SOC-dienst leverancier die SOC-dienstverlening levert aan de deelnemers, verder genoemd Opdrachtnemer.
DVO	Dienstverleningsovereenkomst. Contractuele afspraken tussen Het Waterschapshuis en • Waterschappen; • Waterschap gerelateerde organisaties.
FAT	Fabrieks Acceptatie Test voor Industriële Controle Systemen (ICS). Deze test vindt plaats voordat systemen verzonden worden naar een klant.

Gebeurtenissen	Vertaling van het Engelse woord 'events'. Vanuit de werking van componenten (servers, firewalls, PCLS') worden gebeurtenissen weggeschreven in een log bestand. Deze gebeurtenissen zijn de invoer voor security monitoring.
Gele pas	Er zijn verschillende beveiligingslegitimaties die op basis van kleur van elkaar onderscheiden kunnen worden. Elke kleur staat voor een categorie aan werkzaamheden die de beveiliger (de houder van de beveiligingspas) mag uitvoeren. Voor dit ontwerp is de GELE PAS van toepassing. Deze gele beveiligingspas is bedoeld voor particuliere onderzoekers. Hiervoor is een speciale vergunning nodig, namelijk de vergunning Particulier Onderzoeker. Een particulier onderzoeker houdt zich bezig met het onderzoeken van bedrijven en personen, volgen strikte wet- en regelgeving.
Gezondheid	In dit ontwerp wordt onder gezondheid verstaan een weergave van de kwaliteit van dienstverlening, kwantiteit van incidenten en waarschuwingen m.b.t. incidenten die mogelijk kunnen optreden, statusmelding van databronnen, component werking of andere nader te bepalen status informatie.
Helpdesk of Servicedesk	Het eerste loket binnen de Opdrachtnemer waar een geautoriseerde persoon een melding kan indienen.
ICS	Industrial Control Systems (Proces Automatisering) Een industrieel besturingssysteem is een elektronisch besturingssysteem en bijbehorende instrumenten die worden gebruikt voor industriële procescontrole. Besturingssystemen kunnen in grootte variëren van enkele modulaire, op een paneel gemonteerde controllers tot grote onderling verbonden en interactieve gedistribueerde besturingssystemen met vele duizenden veldverbindingen.
IEC 62443	Een reeks normen die zich richten op de beveiliging van industriële automatisering en controlesystemen (OT/ICS/SCADA).
Impact	De uitwerking en/of gevolgen van een Verstoring dan wel een ingediend Verzoek, mede rekening houdend met aard en aantal van de betrokken gebruikers en kritische componenten.
Incident	Een (cyber)incident is een ICT-verstoring in de dienstverlening (beschikbaarheid van systemen of informatie) en/of het ongeoorloofd

	openbaren, verkrijgen en/of wijzigen van informatie (vertrouwelijkheid of integriteit van informatie of systemen).
ISEA3402 Type 2 verklaring	ISAE 3402 staat voor International Standard for Assurance Engagements en is een auditstandaard voor rapportage over beheersing van processen die zijn uitbesteed. Er zijn twee verschillende typen ISAE 3402 verklaringen, namelijk type 1 en type 2. ISAE 3402 type 2: Hier wordt gekeken naar de manier waarop de maatregelen hebben gewerkt om de doelstellingen te behalen. Daarvoor is het van belang dat er over een periode van minimaal zes maanden bewijs wordt verzameld.
ISO27001/ ISO27002	De ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. ISO 27001 certificering geeft aan dat je voldoet aan alle eisen rondom informatiebeveiliging 27002 biedt een implementatierichtlijn. In deze norm wordt namelijk gedetailleerd aangegeven welke maatregelen je kan nemen om aan de normeisen van ISO 27001 te voldoen.
KA	Kantoorautomatisering. De term "kantoorautomatisering" verwijst naar de uitrusting van een kantoor met moderne gegevensverwerking. Het gaat vooral om het rationaliseren van interne processen met behulp van software. Dit betekent het verhogen van de arbeidsproductiviteit en het verlagen van de totale kosten om de winst te maximaliseren. Het doel is om de efficiëntie van een bedrijf te verhogen door automatisering, mechanisatie en veranderingen in werkprocessen, waardoor kosten en uitgaven aanzienlijk worden verlaagd.
MaGMA	Een Use Case Framework. MaGMa staat voor Management, Growth, Metrics & Assessment. Dit zijn de pijlers van het raamwerk die het use case managementproces helpen begeleiden (zie definitie UCF)
Monitoring	Het vinden en analyseren van mogelijke cyberbeveiligingskwetsbaarheden, -aanvallen en -incidenten (conform “Detect” uit het NIST Cybersecurity Framework 2.0)
Melding	Vraag, Verzoek, Wens of storingsmelding
Mitre (organisatie) ATT&CK Framework	ATT&CK, dat staat voor Adversarial Tactics, Techniques, and Common Knowledge. Het is een gedocumenteerde verzameling informatie over het kwaadaardige gedrag dat ATP-groepen in verschillende stadia van echte cyberaanvallen hebben gebruikt. Het bevat gedetailleerde beschrijvingen van de waargenomen tactieken van ATP-groepen (de technische

	doelstellingen die ze proberen te bereiken), technieken (de methoden die ze gebruiken) en procedures (specifieke implementaties van technieken), gewoonlijk TTP's genoemd.
MS	Microsoft
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
Opdrachtgever	De partij die het raamcontract afsluit met een externe Opdrachtnemer voor de levering van diensten. De Opdrachtgever, tevens contracthouder handelt namens de afnemers en is voor de afnemers het centrale aanspreekpunt voor de levering van de dienst.
Opdrachtnemer	De inschrijver aan wie de opdracht voor het leveren van de dienst wordt gegund.
OT	Operational Technology (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld voor het aansturen en monitoren van industriële apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie.
Overeenkomst	Het getekende contract tussen Opdrachtgever en Opdrachtnemer voor het leveren van de SOC-dienstverlening 'Monitoring & Alarmering'.
PA	Proces Automatisering. Hanteren we als algemene term. OT is een onderdeel van PA. IOT is afhankelijk van het object een onderdeel van PA of KA (denk aan HACV of WIFI)
PvE	Document waarin de functionele en technische specificaties van de Opdracht worden beschreven, waaraan de Inschrijving dient te voldoen.
Raamoverkomst (ROK)	Het document waarin afspraken tussen Opdrachtgever en Opdrachtnemer worden opgenomen met betrekking tot de (uitvoering van de) opdracht op basis van de aanbestedingsstukken en de inschrijving van de Opdrachtnemer.
RWS	Rijkswaterstaat
SAT	Locatie Acceptatie Test - Site Acceptance Test. Deze test vindt plaats op de locatie van de klant na inbedrijfsstelling van een systeem. Het dient te borgen dat een systeem op een juiste, betrouwbare en veilige manier is geïnstalleerd en geconfigureerd.

SCADA	Supervisory Control and Data Acquisition, is een controlesysteem dat data verzamelt, analyseert en visualiseert van OT-componenten en procesdata (PA).
Security Use Case	Een use case is een security monitoring scenario dat gericht is op het detecteren van uitingen van een cyberdreiging. Het beschrijft een aanvalsscenario dat de uitkomst van een aanval weergeeft en beschrijft door welke beveiligingscontrole, beveiligingsbeleid of beveiligingsrichtlijn deze uitkomst voorkomen kan worden of beperkt. Een use case heeft een strategische, tactische en operationele bestanddeel. 1. Bedrijfslaag. De bedrijfslaag van de use case beschrijft hoe de use case aansluit op de zakelijke behoeften van de organisatie. 2. Bedreigingslaag. De dreigingslaag van de use case beschrijft de dreiging waarvoor de use case bedoeld is. Verschillende aspecten van de dreiging zijn belangrijk. 3. Implementatielaag. Dit is de operationele laag, waar aspecten worden beschreven die relevant zijn voor de implementatie van de use case in de operationele security monitoring architectuur.
SOC	Security Operations Centre. In dit document geldt als vereiste voor een SOC, de definitie van 'Converged OT & IT SOC'.
SOC 2 rapportage	In deze context staat SOC voor Service Organization Control. Een SOC-rapportage is opgesteld volgens SOC-rapportagenormen en gaat in op de opzet, het bestaan en de werking van beheersmaatregelen die zijn getroffen met betrekking tot uitbestede processen. Er zijn drie soorten SOC-rapportages, namelijk SOC 1, SOC 2 en SOC 3. SOC 2: Rapporteert over vastgestelde principes (Trust Services Criteria) in relatie tot de opzet, het bestaan en de werking van operational IT-controls met betrekking tot uitbestede processen.
SOC-CMM	Security Operations Centre - Capability Maturity Model
Triage binnen security	Triage is een kritisch reactieproces op incidenten waarmee beveiligingsteams een stortvloed aan waarschuwingen en potentiële bedreigingen kunnen doorzoeken om de meest urgente problemen te identificeren. Het omvat het onmiddellijk analyseren en prioriteren van

	beveiligingsgebeurtenissen op basis van ernst, zodat middelen dienovereenkomstig kunnen worden toegewezen. Het doel van cybersecurity-triage is het versnellen van de reactie op gedetecteerde of zich actief ontwikkelende IT-incidenten. Triage stelt beveiligingsanalisten in staat om meteen op de gevaarlijkste bedreigingen in te spelen voordat deze uit de hand lopen.
TTP	De term Tactiek, Technieken en Procedures (TTP) beschrijft het gedrag van een bedreigingsacteur en een gestructureerd raamwerk voor het uitvoeren van een cyberaanval. De actoren kunnen variëren van hacktivisten en hobbyistische hackers tot autonome cybercriminelen en door de staat gesponsorde tegenstanders. Door de tactieken, technieken en procedures te begrijpen die betrokken zijn bij een cyberaanval, kunnen bedrijven beveiligingsbedreigingen ontdekken, evalueren en erop reageren met een proactieve aanpak.
Use Case Framework (UCF) voor Use Case Management	Een UCF is een raamwerk en hulpmiddel voor use case management en administratie van use cases dat organisaties helpt hun strategie voor beveiligingsmonitoring te operationaliseren. Een UCF biedt de mogelijkheid om te bewijzen dat het SOC de controle heeft en de risico's in de onderneming adequaat beheert en vermindert. Dit omvat use case design, -test en -implementatie.