
GeVS Keten Dossier Afspraken & Procedures Suwi versie 12.0

Gebaseerd op de Keten SLA Suwinet versie 12.0

Inhoudsopgave

1.	Inleiding.....	3
1.1	Achtergrond en doel van het GeVS Keten DAP	3
1.2	Positie van de Keten DAP	3
1.3	Documentbeheer	3
1.4	Leeswijzer.....	3
2.	Dienstenniveau beheer	4
3.	Servicedesk	4
4.	Configuratiebeheer	5
5.	Incidentbeheer	5
6.	Incidentprocedure privacy- en beveiligingsincidenten	7
7.	Probleembeheer	10
8.	Wijzigings- en releasebeheer.....	11
9.	Continuïteit en uitwijk	11
10.	Autoriseren gebruikersbeheerder Suwinet-Inkijk	11
11.	Escalatieproces.....	12
12.	Aanvraagprocedures.....	14
	Bijlage I: verklarende woordenlijst.....	15
	Bijlage II: releasementen 2018.....	17
	Bijlage III: Uitzonderingen openstellingstijden.....	18

1. Inleiding

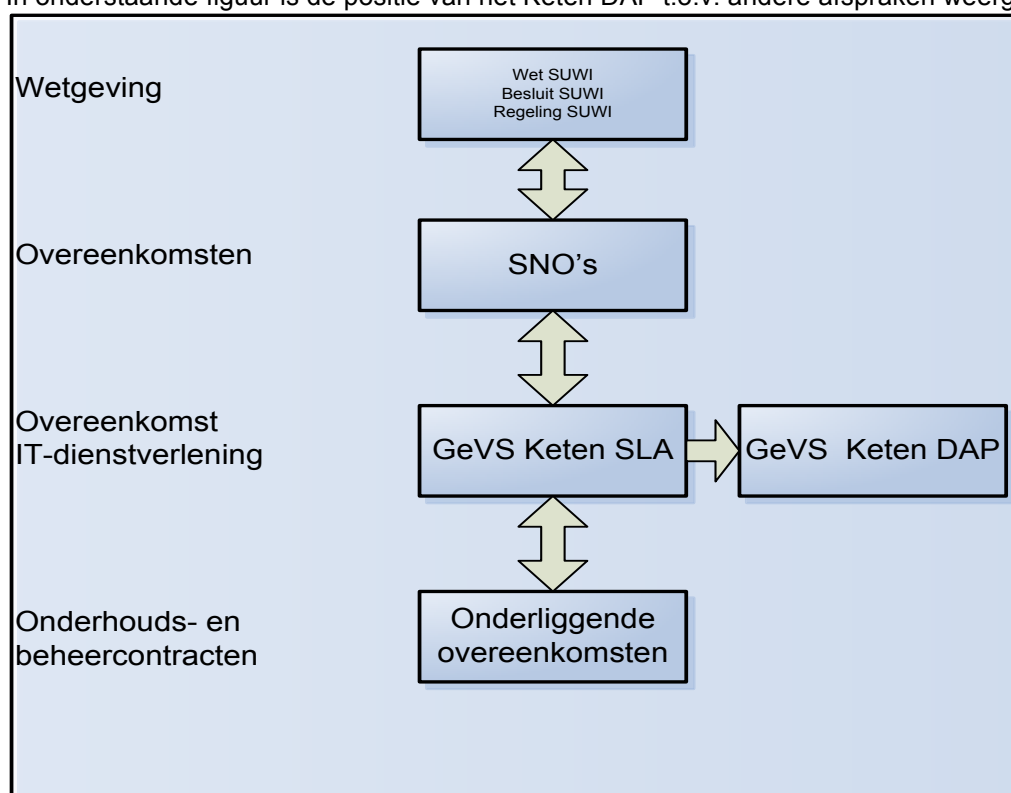
1.1 Achtergrond en doel van het GeVS Keten DAP

Het Gezamenlijke elektronische Voorzieningen Suwi Keten Dossier Afspraken en Procedures (verder genoemd Keten DAP) is een nadere uitwerking van de GeVS Keten SLA (verder te noemen Keten SLA) en bevat nadere afspraken en procedures met betrekking tot de ICT-beheerprocessen die van toepassing zijn op de dienstverlening door de (keten) partijen. Mochten de Keten SLA en het Keten DAP elkaar tegenspreken is de Keten SLA altijd leidend.

De partijen op wie de Keten SLA van toepassing is, zijn ook de partijen voor deze Keten DAP. Bij elke nieuwe versie van de Keten SLA wordt altijd een nieuwe versie van de Keten DAP gemaakt met daarin eventuele noodzakelijke aanpassingen. Deze twee documenten worden tezamen goedgekeurd door de Domeingroep ICT Beheer.

1.2 Positie van de Keten DAP

In onderstaande figuur is de positie van het Keten DAP t.o.v. andere afspraken weergegeven.



Afbeelding 1: Voor de keten geldende regels en afspraken

1.3 Documentbeheer

De Domeingroep ICT Beheer is beheerder van deze Keten DAP en borgt dat dit document in lijn blijft met de vigerende versie van de Keten SLA¹.

1.4 Leeswijzer

In de volgende hoofdstukken wordt per onderwerp weergegeven welke afspraken en procedures de partijen zijn overeengekomen. De hieraan gerelateerde prestatienormen zijn vastgelegd in de Keten SLA.

¹ De Keten SLA wordt jaarlijks geupdate en ondertekend door de partijen.

2. Dienstenniveau beheer

Openstellingstijden voor de productieomgeving en ondersteuning

- Uitzonderingen en aanvullingen op de openstellingstijden, voor zover vooraf bekend, zijn opgenomen in bijlage III.

Onderhoudstijden van de productieomgeving

- Gepland onderhoud, uitgevoerd door (één van) de partijen, aan (een onderdeel van) de diensten, vindt uitsluitend plaats buiten de beschreven openstellingstijden.
- Onderhoud moet vooraf worden gemeld aan de Suwidesk. De Suwidesk informeert de betrokken (keten)partijen.
- In de keten SLA zijn partij specifieke onderhoudsmomenten vastgelegd.

Extra openstellingstijden van de productieomgeving

- Wanneer een partij extra openstelling van de Suwinet-Services wenst, stuurt deze per e-mail een aanvraag naar de Suwidesk.
Dit verzoek moet minimaal de volgende elementen bevatten:
 - de partij die de aanvraag doet;
 - de contactpersoon/contactpersonen van de aanvragende partij (zowel voor de aanvraag als gedurende de extra openstelling);
 - de gewenste functionaliteit(en);
 - de reden waarom de extra openstelling is gewenst;
 - de datum waarop extra openstelling wordt gewenst, inclusief tijd (van .. tot ..).
- Een aanvraag voor extra openstellingstijd moet tenminste twee weken voorafgaand aan de datum waarop de extra openstelling gewenst is bij het BKWI binnen zijn.
- Het BKWI registreert de aanvraag als service request onder een uniek referentienummer. De Suwidesk stuurt de aanvraag onder vermelding van het registratienummer binnen één werkdag na ontvangst door naar de contactpersonen van de betreffende partijen waarvan extra beschikbaarheid gewenst wordt.
- De partijen die de aanvraag hebben ontvangen, beoordelen het verzoek en geven aan of het mogelijk is op de aangegeven datum aan het verzoek te voldoen.
- Als aan het extra openstellen kosten zijn verbonden, dan is het uitgangspunt dat de kosten worden gedragen door de partij die de openstelling verleent.
- De partijen sturen het resultaat van de beoordeling uiterlijk binnen vijf werkdagen na ontvangst van de aanvraag aan de Suwidesk. De Suwidesk verzamelt de verschillende beoordelingen en stuurt dit totaalbeeld binnen 1 werkdag naar de aanvrager.
- Voor ondersteuning tijdens extra openstellingstijd kunnen partijen kosten in rekening brengen bij de aanvrager. Tenzij anders afgesproken verleent BKWI tijdens extra openstellingstijden geen ondersteuning.

Gebruik Ketenbrede Test Omgeving

- Er is een Ketenintegratie Test omgeving (KIT) inclusief testdata voor Suwinet beschikbaar voor de partijen.
- De KIT is gekoppeld aan testsytemen van ketenpartijen, waar mogelijk/gewenst biedt BKWI standaard teststubs aan om testomgevingen van ketenpartijen te simuleren.
- De KIT staat standaard gereserveerd voor BKWI om producten te kunnen testen.
- Als een partij (een wijziging) wil testen dan reserveert hij/zij dit twee weken van tevoren bij het BKWI. Het BKWI zorgt ervoor dat de testomgeving beschikbaar is en naar gewenst naar een bronsysteem of teststub wijst.
- Bij gebruik van de testomgeving terwijl de testomgeving door een andere partij is gereserveerd zijn er geen garanties voor een juiste werking.
- Gebruik testomgeving zonder reservering is toegestaan als dit de test van de partij die gereserveerd heeft, niet in de weg kan zitten.
- BKWI registreert de reserveringen in de Suwinet agenda.

3. Servicedesk

- Partijen zijn niet verplicht om een servicedesk in te richten, wel moet elke partij zorgen voor een enkelvoudig communicatiekanaal (single point of contact) met de Suwidesk van BKWI.
- Deelnemende partijen zijn zelf verantwoordelijk voor gebruikersbeheer en de eerstelijns-ondersteuning van de eigen gebruikers en zelf bepalen zij op welke wijze zij deze eerstelijns-ondersteuning invullen.
- Communicatie over incidenten of onderbrekingen in de dienstverlening verlopen in beginsel via

de Suwidesk.

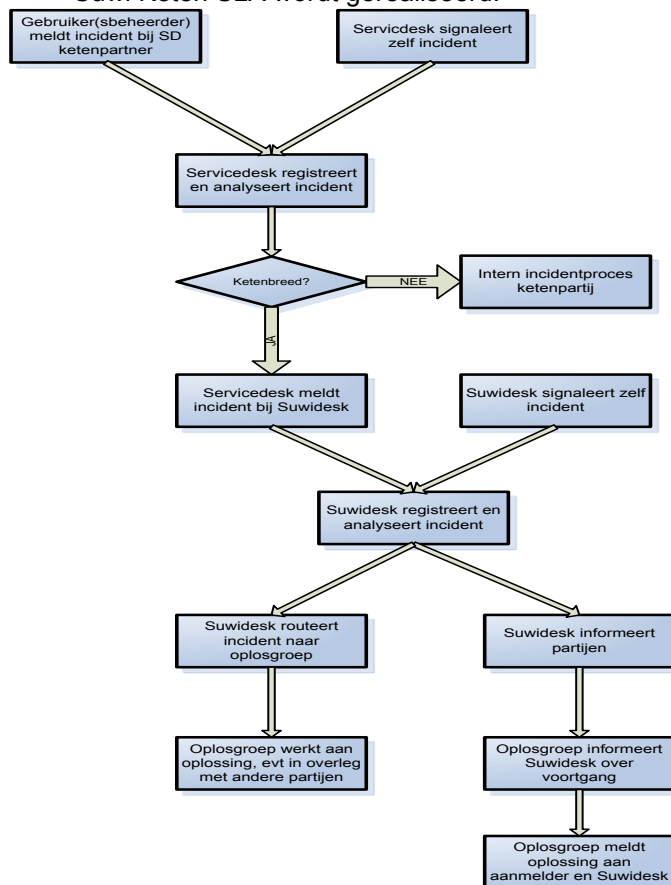
- Partijen informeren bij een incident eerst de eigen eerstelijnsondersteuning,
- De verschillende servicedesken (of degene die die rol heeft gekregen bij een ketenpartij) zijn aanmelder van incidenten en tevens oplosgroep voor ketenbrede incidenten.
- De Suwidesk vervult de rol van centrale regievoerder op het keten brede incidentbeheer en informeert de partijen over de status en voortgang van openstaande incidenten.
- De Suwidesk communiceert met de servicedesk van ketenpartijen of de door de ketenpartij aangedragen single point of contact.
- Iedere partij informeert zelf haar eigen gebruikers over de status en voortgang van incidenten en van tijdelijke onderbrekingen van de dienstverlening.
- In beperkte mate verleent de Suwidesk tweedelijns en derdelijns ondersteuning aan de partijen, zoals benoemd en afgesproken in de Keten SLA.

4. Configuratiebeheer

- De Suwidesk en BKWI TechSupport houden binnen het incidentregistratietool een overzicht bij van alle ketencomponenten, die een relatie hebben met de Suwiketen. Hier worden incidenten aan gerelateerd zodat inzichtelijk wordt welke componenten de meeste storingen kennen.
- Iedere partij heeft een eigen CMDB waarin partij specifieke componenten zijn opgenomen. Deze moeten actueel en volledig zijn. De status van een component moet bewaakt kunnen worden.
- De inhoud van de CMDB van de ketenpartijen wordt actueel gehouden, en minimaal jaarlijks gecontroleerd.

5. Incidentbeheer

- Het doel van de afspraken met betrekking tot het proces incidentbeheer is dat na het optreden van een incident zo snel mogelijk een herstelde dienstverlening conform de afspraken in de Suwi Keten SLA wordt gerealiseerd.



Afbeelding 2: Procedure schema incidentbeheer

Incident aanmelden en registreren

- Gebruikers van de Suwinet-Services melden de geconstateerde incidenten in eerste instantie

- binnen de eigen organisatie.
- Verstoringen binnen het eigen beheerdomein, zonder ketenimpact, zijn de verantwoordelijkheid van de eigen partij en vallen buiten de scope van het Ketenbreed Incidentbeheer.
- Een ketenbreed incident is een verstoring waarvoor geldt dat;
 - de oorzaak in het beheerdomein ligt van één van de Suwi-partijen en
 - één of meer partijen - anders dan de veroorzakende partij – gevolgen ondervindt van deze verstoring.
- Iedere partij meldt actief incidenten met ketenimpact aan de Suwidesk, inclusief eigen referentienummer.
- Bij incidenten waarbij de oorzaak van het incident ligt bij de ketenpartij zelf wordt tevens een inschatting gegeven van de te verwachten oplostermijn.
- De Suwidesk prioriteert een incident conform de afspraken uit de Keten SLA, registreert het incident en geeft het referentienummer van de Suwidesk aan de ‘aanmeldende’ servicedesk.
- Incidenten krijgen bij registratie een prioriteit met daaraan gekoppeld een indicatieve oplostijd (zie tabel incidentbeheer /prioriteiten in de Keten SLA). Vaak zal dat het geval zijn bij incidenten aangaande de kwaliteit van gegevens, omdat oplossing van deze incidenten vaak een langere doorlooptijd kennen.

Incident routeren en oplossen

- De Suwidesk informeert de partijen via mail over storingen met behulp van verzendlijsten, die naast servicedesken ook beheerders en andere belanghebbenden kan bevatten.
- De Suwidesk routeert ketenbrede incidenten binnen de vastgestelde reactietijd (zie Keten SLA) na ontvangst naar de oplosgroep voor het incident. Hierbij wordt het referentienummer (van de Suwidesk) van het incident vermeld.
- Indien nodig wordt een ketenbreed incident door een partij gerouteerd naar een leverancier van een ketenpartij. De Servicedesk van de ketenpartij blijft echter altijd de verantwoordelijke oplosgroep en het aanspreekpunt m.b.t. de voortgang. Zij dragen zorg voor communicatie over voortgang aan de Suwidesk. De Suwidesk verspreidt deze informatie via de geëigende route.
- Terugkoppeling van de voortgang aan de Suwidesk vindt altijd plaats onder vermelding van Suwidesk incidentnummer. Ook wordt - voor zover bekend - altijd de oorzaak van het incident teruggekoppeld.
- De oplosgroep zal de Suwidesk tijdig op de hoogte brengen van een dreigende overschrijding van de oplostijden. Aanmelder en oplossende partij overleggen of de overschrijding wordt geaccepteerd of dat de escalatieprocedure wordt gestart.
- De oplosgroep meldt opgeloste incidenten terug aan de Suwidesk. Suwidesk informeert de indiener van het incident over de oplossing.

6. Incidentprocedure privacy- en beveiligingsincidenten

Dit deel is een richtlijn over wanneer het kenmerk "Privacy en Beveiliging" (P&B) van toepassing is op een incident en hoe de ernst van een P&B incident wordt bepaald.

P&B is een aanvullend kenmerk dat een incident of calamiteit kan bezitten. Of bij een gemeld incident of calamiteit de eigenschap P&B wordt herkend, bepaalt (in eerste instantie) de medewerker van de servicedesk van de aanmeldende Suwinet-partij, die incidenten registreert en in behandeling neemt. Dit wordt afgestemd met de medewerker Service Support van de Suwidesk tijdens de kwalificatie van de call.

Definitie gebruikte termen

Privacy:	de mate waarin persoonsgegevens zijn beschermd tegen het in handen vallen van onbevoegden.
Beveiliging:	omvat de volgende deelgebieden:
<i>Beschikbaarheid:</i>	de mate waarin een faciliteit beschikbaar is op momenten dat dit voor een ketenproces is gewenst en/of is afgesproken
<i>Integriteit:</i>	de mate waarin de werking van processen en de gegevens zonder fouten zijn
<i>Vertrouwelijkheid:</i>	de mate waarin processen en gegevens slechts beschikbaar zijn voor diegenen die daar recht op hebben, ook wel exclusiviteit genoemd.

Onderscheid tussen de P&B-aspecten bij de behandeling van incidenten

De afhandeling van incidenten en calamiteiten die uitsluitend betrekking hebben op het aspect **Beschikbaarheid**, wordt verzorgd door de standaard incidentafhandelingsprocedure aanvullende eisen worden er niet gesteld. Registratie met een extra kenmerk 'P&B incident' blijft voor deze incidenten wel noodzakelijk vanwege rapportage en sturingsdoeleinden.

Deze procedure richt zich dus op het **P&B-incident** of **-calamiteit** waarmee inbreuk op de **vertrouwelijkheid, integriteit** en/of de **privacy** plaats vindt.

Voorbeelden van **vertrouwelijkheid-incidenten**:

Personen of applicaties kunnen/konden² toegang krijgen tot beschermde faciliteiten en/of gegevens³ zonder dat zij daar recht op hadden, bijvoorbeeld:

1. Aan een persoon of applicatie is een autorisatie en/of rol (toegangsrechten) gegeven zonder dat hiervoor toestemming is verleend door een bevoegd persoon;
2. Een reeds geopende beschermde faciliteit of gegevens is/zijn voor onbevoegden beschikbaar (bijvoorbeeld op een onbewaakte terminal).
3. De toegangsmiddelen⁴ (bijvoorbeeld username/password) worden gebruikt door een andere geautoriseerde⁵
4. Autorisatiemechanismen worden omzeild, bijvoorbeeld:
 - a. door het niet of onvoldoende functioneren van beveiligingsmechanismen;
 - b. doordat de werkende beveiligingsmechanismen onvoldoende bescherming bieden;
 - c. vanwege een succesvolle aanval door een hacker

² Hiervan is dus ook sprake wanneer van de ongeautoriseerde toegang geen gebruik is gemaakt.

³ Het betreft hier zowel gegevens die beschermd zijn door een applicatie als gegevens op een beveiligde informatiedrager.

⁴ verkregen al dan niet met de medewerking van een andere geautoriseerde

⁵ Dit geldt ook wanneer de overtreder dezelfde autorisatie bezit.

Voorbeelden van **privacy-incidenten**:

Persoonsgegevens zijn of waren⁶ beschikbaar voor personen voor wie deze niet zijn bedoeld, bijvoorbeeld vanwege:

1. het verwerken van persoonsgegevens zonder dat daar een dossier aan ten grondslag ligt;
2. de zichtbaarheid voor onbevoegden van persoonsgegevens op een beeldscherm of document op een onvoldoende bewaakte⁷ werkplek;
3. het opbergen van documenten of onbeschermden gegevensdragers met persoonsgegevens in een onvoldoend bewaakte of afgesloten kast of lade;
4. het opslaan van elektronische persoonsgegevens op een onvoldoend beschermd of bewaakt medium;
5. het afdrukken van persoonsgegevens op een onvoldoend bewaakte printer of kopieerapparaat;
6. het transport van documenten of onbeschermden gegevensdragers met persoonsgegevens op een onvoldoend beschermd wijze.

Verantwoordelijkheid voor beoordeling en afhandeling

Bij het beoordelen en het proces van afhandelen van beveiligingsincidenten hebben de security en privacy functionarissen van de betrokken organisaties een prominente rol. En zijn verantwoordelijk voor de coördinatie en afhandeling van incidenten.

⁶ *Hiervan is sprake, wanneer van deze beschikbaarheid geen gebruik is gemaakt.*

⁷ *De eisen aan de kwaliteit van de afsluiting, bescherming of bewaking hangt af van de gevoeligheid van de informatie; deze eisen moeten zijn vermeld in een ter plaatse geldend en bekend gemaakt document, bijvoorbeeld over documentclassificatie.*

Beoordeling P&B-Ernst

De ernst van het aspect P&B wordt beoordeeld op basis van de onderstaande tabel.

Ernst	Omschrijving per aspect
Licht	<p>De schending blijft binnen de hieronder omschreven criteria: <i>Een schending van de privacy en/of de exclusiviteit was/is beperkt van omvang en kon/kan worden gecorrigeerd zonder dat de privacy van de betreffende personen hiervan schade ondervinden of hebben ondervonden</i>⁸.</p> <p>Een dergelijk incident heeft, vergeleken met niet-P&B incidenten, een afwijkende afhandeling nodig, gericht op het:</p> <ul style="list-style-type: none">* zo nodig opheffen van oorzaak van de gebeurtenis;* zo nodig herstellen van de schade;* starten van een wijziging ter voorkoming van een herhaling van de gebeurtenis <p>De laatste actie mag pas worden overgeslagen als het risico⁹ van een herhaling gering is en de kosten en inspanning daarmee onevenredig hoog zijn.</p>
Hoog	<p>De schending blijft binnen de omschreven criteria: <i>Een schending van de privacy en/of de exclusiviteit was/is van aanzienlijke omvang en kon/kan niet worden gecorrigeerd zonder dat de privacy van de betreffende personen hiervan schade ondervinden of hebben ondervonden of hiervoor een reëel risico lopen of liepen</i>¹⁰.</p> <p>Een dergelijk incident heeft, vergeleken met niet-P&B incidenten, een afwijkende afhandeling nodig, gericht op het zo spoedig mogelijk:</p> <ul style="list-style-type: none">* opheffen van de oorzaak van de gebeurtenis;* zonodig informeren van de betrokkenen;* herstellen van de schade;* starten van een wijziging ter voorkoming van een herhaling van de gebeurtenis
Zeer Hoog =Calamiteit	<p>De schending voldoet aan de volgende criteria: Een schending van de privacy en/of beveiliging was/is van omvang zodanig dat deze de bedrijfsvoering van één of meerdere Suwi-partijen raakt, het ministerie raakt, of een publieke zaak wordt. Een dergelijk incident escaleert naar de verantwoordelijke vergtegenwoordiger(s) van betrokken partijen. Als is aangetoond dat de schadelijke werking van een P&B-calamiteit kan worden opgeheven door het uitschakelen van (een deel) van Suwinet, dan zal de Security Officer van het BKWI, in overleg met de betrokken Security Officers van de ketenpartijen en mogelijk met technisch deskundigen, hiertoe opdracht geven aan de Suwidesk.</p>

De meldplicht datalekken geldt al sinds 2016. Onder de nieuwe Europese privacywet die sinds 25 mei 2018 geldt, de Algemene verordening gegevensbescherming (AVG), blijft de meldplicht datalekken bestaan. De Autoriteit Persoonsgegevens kan hoge boetes opleggen als organisaties zich niet houden aan de Wet Bescherming persoonsgegevens, waaronder het niet (tijdig) melden van datalekken.

De meldplicht en boetedreiging dwingt organisaties om naar de AP en naar de getroffen personen transparant te zijn over datalekken en om datalekken zo snel mogelijk te dichten.
Datalekken

⁸ Als een persoon wiens privacy het betreft een klacht heeft ingediend die verband houdt met dit incident, dan is de ernst "Hoog".

⁹ Risico is het product van de kans dat het incident zich herhaalt en de schade die daarvan het gevolg kan zijn.

¹⁰ Als een persoon wiens privacy het betreft een klacht heeft ingediend die verband houdt met dit incident, dan is de ernst minimaal "Hoog".

Een datalek gaat altijd over persoonsgegevens en niet over (gevoelige) bedrijfsinformatie. Bij een datalek is sprake van een 'inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking'. Onder een datalek valt dus niet alleen het vrijkomen (lekkens) van persoonsgegevens, maar ook vernietiging daarvan en andere vormen van onrechtmatige verwerking.

Ook een vermoeden van datalek dient gemeld te worden aan de Autoriteit Persoonsgegevens. Als het vermoeden vals alarm blijkt te zijn kan de melding weer ingetrokken worden.

Procesgang

Als er een (vermoeden van een) datalek is, wordt dit als een prio 1 incident gemeld bij de Suwidesk. Bij een vermoeden van datalek wordt het partij eigen proces gevolgd en daarnaast de Suwidesk geïnformeerd. Dit dient zowel schriftelijk (per mail aan Suwidesk@bkwi.nl) en daarnaast ook verplicht telefonisch gemeld te worden. Dit in verband met de 72 uur termijn die staat voor de melding aan de Autoriteit Persoonsgegevens.

Bij de melding aan de Suwidesk wordt in elk geval het volgende aangegeven:

- of er sprake is van een datalek
- zo ja, of het een meldenswaardig datalek is
- Van hoeveel personen is de data gelekt?
- Welke persoonsgegevens zijn gelekt?
- Wat is de oorzaak van het lek?
- Is het lek onder controle?
- Welke maatregelen zijn er (al) getroffen?

Verder volgt dit datalek het proces van incidentbeheer prio 1 met als enige verschil de mogelijke melding bij de Autoriteit Persoonsgegevens. Elke partij heeft zijn eigen verantwoordelijkheid bij het melden van een Datalek bij de Autoriteit Persoonsgegevens. Als bij BKWI een datalek geconstateerd door BKWI vindt deze melding plaats via UWV.

7. Probleembeheer

- Het doel van probleembeheer is het vinden van oplossingen voor veelvoorkomende incidenten, waarmee uiteindelijk incidenten voorkomen (kunnen) worden.
- Er is sprake van een probleem wanneer (en/of):
 - sprake is van herhaling van een incident;
 - het incident niet nog een keer op mag treden;
 - de service levels onder druk komen te staan;
 - analyse van de infrastructuur de kans van incidenten aantoonbaar maakt.

Probleem registreren

- Elke ketenpartij registreert problemen die zij zelf constateren (als van toepassing inclusief referentienummers van de bijbehorende incidenten) en meldt deze centraal aan de Suwidesk. De coördinator Suwidesk analyseert en beslist of het een probleem betreft. De coördinator Suwidesk registreert het Problem en meldt het probleem terug aan de meldende partij inclusief het Suwidesk referentienummer. De coördinator Suwidesk beslist of de overige ketenpartners ingelicht dienen te worden. Het KIPO wordt altijd ingelicht. Terug koppeling moet binnen één werkdag geschieden.
- Als het geen ketenprobleem is, maar een Problem bij/met slechts één van de ketenpartners, dan zal de coördinator Suwidesk in contact treden met de Problem coördinator van de meldende partij om gezamenlijk het Problem af te handelen.

Oplostermijnen problemen

- Het KIPO wordt bij problemen met hoge prioriteit bij elkaar geroepen. Het KIPO beoordeelt het probleem en koppelt een oplostermijn aan het probleem. Oplostermijnen voor problemen kunnen in tegenstelling tot incidenten niet vooraf gedefinieerd worden, maar is afhankelijk van het onderzoek, gekozen oplossing en hierbij horende doorlooptijd.
- Partijen streven ernaar om binnen twee weken het onderzoek naar de oorzaak af te ronden. Bij de conclusies van het onderzoek moet ook een oplossing voorstel en termijn genoemd worden.

8. Wijzigings- en releasebeheer¹¹

- Het doel van wijzigings- en releasebeheer is het gestructureerd en gecontroleerd doorvoeren van ketenbrede wijzigingen en releases, waarmee de risico's op verstoringen geminimaliseerd zijn.
- De afspraken omtrent wijzigingsbeheer zijn beschreven in het document "Uitvoeringsafspraken Ketenbrede wijzigingen en releases". Een samenvatting van de afspraken is hier opgenomen.
- Ketenwijzigingen zijn alle wijzigingen die mogelijk een impact op één of meerdere ketenpartijen hebben of mogelijk een impact hebben op één of meerdere ketencomponenten.
- Alle wijzigingen die invloed kunnen hebben op de werking van de GeVS worden aan het CMK gemeld.
- Partijen zijn verantwoordelijk voor het melden van ketenwijzigingen aan de andere Suwipartijen. Wijzigingen dienen door de wijzigingscoördinator (1 of 2 per partij) te worden gemeld via het CMK.
- De wijziging wordt ontworpen, uitgewerkt, getest, gepland en beschikbaar gesteld voor gebruik. Daarbij worden resultaten getoetst aan de ketenstandaarden middels afstemming met de beheerders van de standaarden, de domeingroepen.
- De wijzigingsverantwoordelijke meldt de implementatie van de wijziging bij het CMK. Het CMK verifieert bij de aanmelder (wijzigingscoördinator business of ICT) van de wijziging of de wijziging gesloten kan worden.
- Het CMK is verantwoordelijk voor het registreren, publiceren en routeren van de ketenwijzigingen. Ook coördineert het CMK het ketenbrede wijzigingsbeheer.
- Jaarlijks wordt voorzien dat er 11 releases doorgevoerd worden (zie bijlage II). De releasedata worden in het Keten CAB opgesteld en geaccordeerd. Bij uitzondering mag afgeweken worden van de vastgestelde releasedata of een extra ingepland worden. Dit kan alleen met goedkeuring van het Keten CAB.
- De releasementen worden door BKWI gepubliceerd in dit document op bkwi.nl.
- BKWI zal nadat één of meer nieuwe ketenpartners via Suwinet-Mail worden ontsloten, deze domeinnaamswijzigingen via een mail doorgeven aan de betrokken ketenpartners. Deze zullen de nieuwe domeinnamen kunnen ophalen via www.bkwi.nl, en de wijzigingen doorvoeren in de eigen mailomgeving, waarna deze nieuwe ketenpartner voor de desbetreffende partijen bereikbaar is via Suwinet-Mail.

9. Continuïteit en uitwijk

- Voor de centrale omgeving werkt BKWI met een active-active opstelling over twee fysiek gescheiden locaties. Dit houdt in dat er voor de centrale omgeving geen uitwijk voorziening meer nodig is omdat de beschikbaarheid gegarandeerd is.
- Ketenpartijen dragen zelf zorg voor de inrichting van het continuïteitsbeheer /uitwijk en zijn vrij hier zelf invulling aan te geven, als zij maar kunnen garanderen binnen een acceptabele termijn de dienstverlening kunnen herstellen. De acceptabele termijn is ter beslissing van het MT van de verschillende organisaties.
- **Demo omgeving Suwinet Inkijk hier ?**

10. Autoriseren gebruikersbeheerder Suwinet-Inkijk

Aan wie worden beheerrechten toegekend

- Niemand kan autorisatie(s) voor zichzelf aanvragen; altijd vraagt een binnen de organisatie gemandateerde medewerker - voor zover deze hiertoe gerechtigd is - voor eigen personeelsleden de benodigde autorisaties aan.
- Elke aangesloten partij autoriseert zelf haar personeel en stelt hiervoor gebruikersbeheerders aan.
- Op verzoek gemandateerde medewerker van de aangesloten partij kent BKWI aan betreffende gebruikersbeheerders de rechten toe, welke passen bij deze partij. Hiertoe geeft betreffende partij voor zowel een nieuwe situatie¹² als bij wijziging van bestaande situatie formeel aan BKWI

¹¹ Uitgebreide beschrijving van het keten brede wijziging beheerproces is te vinden in de Uitvoeringsafspraken Keten breed Wijzigingsbeheer en Releases.

¹² Vanuit het aansluitproces voor nieuwe partijen wordt vastgesteld welke persoon/personen het centrale gebruikersbeheer uitvoeren.

door wie zij het gebruikersbeheer wil laten uitvoeren. Dit formeel doorgeven bestaat uit een door directeur of gemeentesecretaris ondertekende brief, waarin de partij verzoekt beheerrechten toe te kennen aan met naam, functie en contactgegevens vermelde personen.

Welke rechten worden toegekend

- De rechten die worden toegekend zijn: het kunnen toekennen van die toegangsrechten, welke voor betreffende partij zijn vastgesteld.

Het delegeren van beheerrechten

- Wanneer een partij taken binnen de eigen organisatie uitbesteedt, dan kan de gebruikersbeheerder doorgeven welke persoon/personen vanuit welk organisatieonderdeel beheerrechten toegekend mogen krijgen en welke toegangsrechten deze beheerder mag toekennen.
- Wanneer een partij taken uitbesteedt aan een andere organisatie, dan moet betreffende partij dit formeel aanvragen bij het BKWI. De opdracht moet dus komen van de aangesloten organisatie.
- Dit formeel doorgeven bestaat uit een door directeur of gemeentesecretaris ondertekende brief, waarin de partij verzoekt de in de brief genoemde beheerrechten toe te kennen aan de met naam, functie en contactgegevens vermelde gebruikersbeheerder(s) van deze andere organisatie.

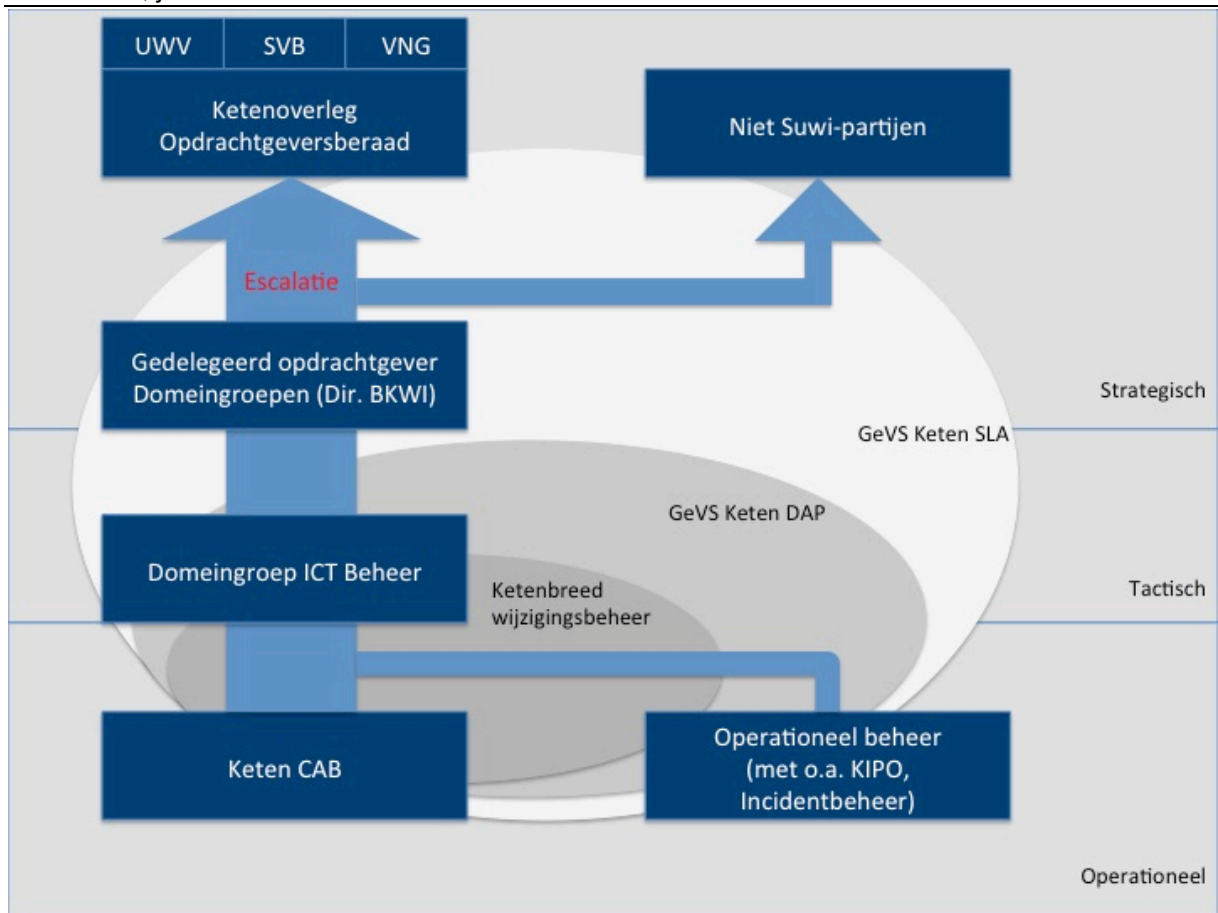
Welke gegevens moeten worden doorgegeven

1. naam van de organisatie en/of organisatieonderdeel
2. naam, functie en contactgegevens van de aanvrager
3. naam, functie en contactgegevens van de te autoriseren beheerder
4. toe te kennen beheerrechten; de toe te kennen autorisatie rollen volgen uit het aansluitproces.

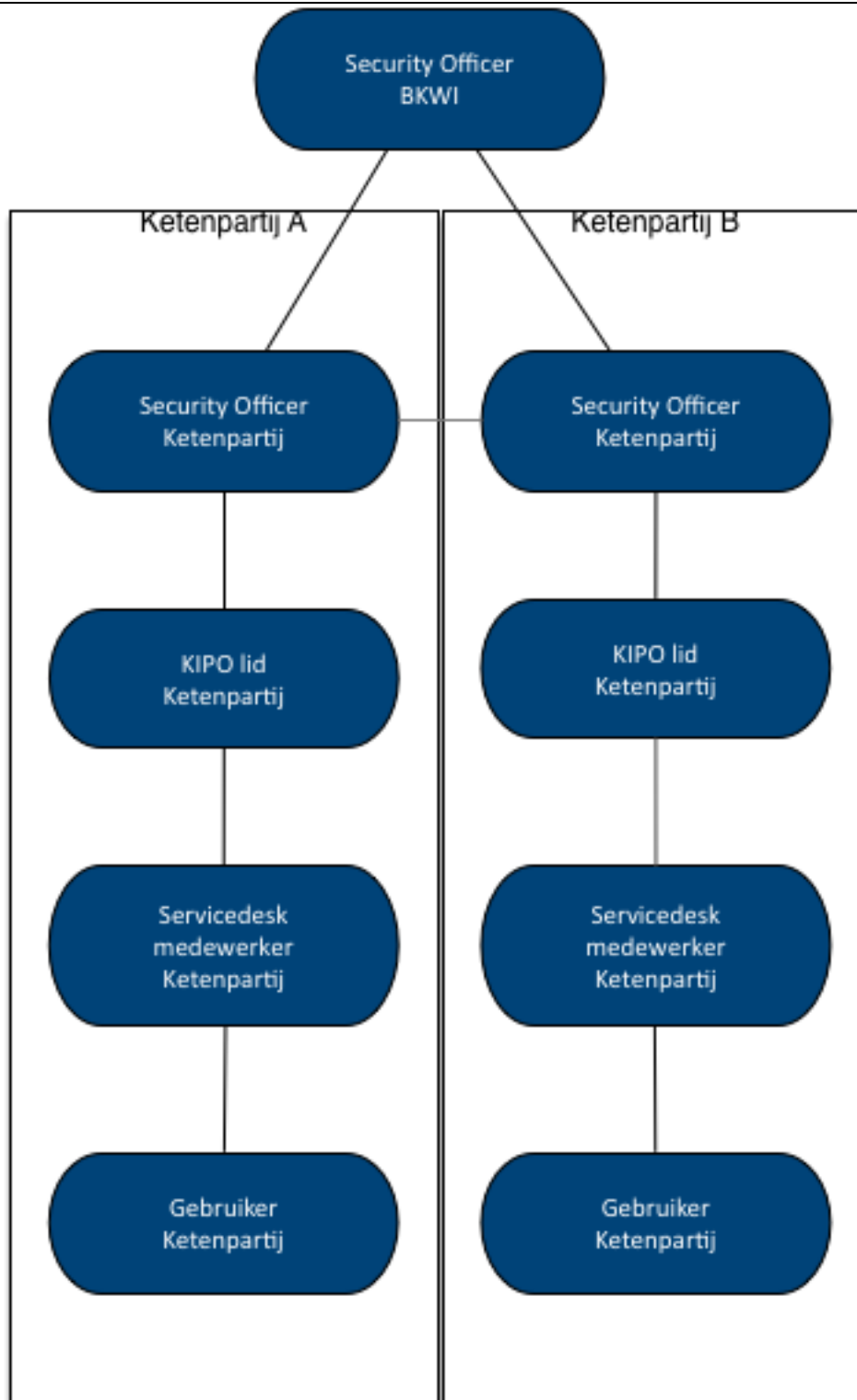
11. Escalatieproces

Escalaties kunnen om verscheidene redenen worden uitgevoerd, hierbij moet gedacht worden aan overschrijding van de oplostermijn van incidenten, wijzigingen die niet tijdig worden doorgevoerd, maar ook het niet nakomen van ketenbrede afspraken zoals gemaakt in de verschillende domeingroepen.

- Doel van de escalatieprocedure is het forceren van een doorbraak bij ongewenste situaties
- Als een overschrijding van de afgesproken oplostijd van een incident plaatsvindt of dreigt (bij prioriteit 1 of 2), wordt de Suwidesk uiterlijk een uur vóór het verlopen van de oplostijd op de hoogte gebracht van de nieuwe verwachte oplostijd. Als de oplostijd wordt overschreden, vindt escalatie volgens onderstaand schema plaats. Binnen een partij worden verticaal geescaleerd. Tussen organisaties ALTIJD horizontaal. Escalaties verlopen altijd via de voorzitter van de domeingroep voor zover het onderwerp past binnen deze domeingroep.
- Escalaties worden opgelost (lees; er wordt over besloten) door de gedelegeerd opdrachtgever van de Domeingroepen (lees; directeur BKWI). Hierbij enkel in de rol als onafhankelijk gedelegeerd opdrachtgever en dus niet als directeur BKWI (Afbeelding 3).
- In geval van (vermoeden van) een beveiligingsincident, vindt altijd escalatie plaats, volgens onderstaand schema (Afbeelding 4).



Afbeelding 3 Escalatieschema geschillen



Afbeelding 4: Escalatieladder bij beveiligings of privacy incidenten.

12. Aanvraagprocedures

Niet alle afnemers maken gebruik van alle beschikbare Suwinet producten. Voor alle producten die binnen het Suwi-domein beschikbaar zijn gelden specifieke aanvraagprocedures. Het moment van aansluiten bepaalt dat de procedure doorlopen moet worden.

Bijlage I: verklarende woordenlijst

Beschikbaarheid	De mate waarin een informatiesysteem gebruiksgereed is op het moment dat de organisatie het nodig heeft. $\% \text{ beschikbaarheid} = \text{werkelijke beschikbare tijd} / \text{overeengekomen tijd} \times 100\%$.
Beveiligings-incident	Een beveiligingsincident is een gebeurtenis die ervoor heeft gezorgd, of ervoor had kunnen zorgen, dat bedrijfsmiddelen zijn beschadigd of verloren zijn geraakt. Een handeling die in strijd is met de beveiligingsprocedures van het bedrijf, is ook een beveiligingsincident.
CMK	Centraal Meldpunt Ketenwijzigingen. Het CMK registreert, publiceert, coördineert en routeert ketenwijzigingen en releases.
Centrale omgeving	De centrale omgeving van Suwinet bevat het Suwikoppelpunt, servers, routers, reverse proxy's en bijbehorende verbindingen ten behoeve van Suwinet-Inkijk, Suwinet-Mail en Suwinet-Meldingen.
Domeingroep ICT Beheer (DIB)	Een overleg dat wordt gevormd door de Service Level Managers van de betrokken partijen en wordt voorgezeten door het BKWI. Het overleg behandelt de inrichting en kwalitatieve groei van ketenbreed ICT Beheer.
Incident	Verstoring in de afgesproken dienstverlening of een vraag over de dienstverlening.
Incidentbeheer	Het registreren, prioriteren en (doen) verhelpen van gebeurtenissen die een onderbreking of vermindering van de kwaliteit van de dienstverlening veroorzaken.
Ketenbreed incident	Een ketenbreed incident is een verstoring waarvoor geldt dat (a) de oorzaak ligt in het beheerdomein van de Suwi-partijen, en (b) één of meer Suwi-partijen - naast de veroorzakende partij - ondervindt gevolgen van deze verstoring.
Ketencomponent	Kleinste gedefinieerde onderdeel van de Suwinet infrastructuur, vastgelegd in de CMDB van het CMK.
Keten Incidenten & Problemen Overleg (KIPO)	Keten Incidenten en Problemen Overleg, overleg waarin de incidentmanagers van de ketenpartijen ketenbrede incidenten en problemen bespreken en waar incidenten worden gepromoveerd tot problemen en worden toegewezen aan een oplosgroep.
Keten DAP	Keten Dossier Afspraken en Procedures Suwinet, het document waarin de afspraken van de Keten SLA nader zijn uitgewerkt.
Ketenbrede wijziging	Een ketenbrede wijziging is een wijziging in een ketencomponent waarvoor geldt dat (a) het initiatief ligt bij één van de Suwi-partijen, en (b) één of meer Suwi-partijen - naast de veroorzakende partij - ondervindt gevolgen van deze wijziging. Er wordt onderscheid gemaakt tussen voorgenomen veranderingen, ketenwijzigingen en ketencomponentwijzigingen.
Onderhoud	Het uitvoeren van preventieve of proactieve werkzaamheden aan Configuratie Items die van invloed zijn op de beschikbaarheid van de diensten.
Openstellingstijden	Afgesproken tijdstippen waarbinnen de diensten beschikbaar zijn.
Oplosgroep	Organisatie(onderdeel), verantwoordelijk voor het oplossen van een incident. Dit kan een Suwi-partij zijn, maar ook een leverancier van een Suwi-partij.
Oplostijd	De maximale tijd die is afgesproken voor het oplossen van een incident, op basis van de prioriteit van het incident.
Overzichtspagina	Een pagina waarmee gegevens, afkomstig van (soms meerdere) bronnen, op één pagina worden verzameld en getoond.
Prioriteit	Code waaraan een oplostijd is gekoppeld, afhankelijk van de urgentie en impact van een incident, probleem of wijziging.
Probleem	Onbekende onderliggende oorzaak van een of meerdere incidenten.
Probleembeheer	Het registreren, prioriteren en structureel (doen) verhelpen van gebeurtenissen die het functioneren van de IT-infrastructuur aantasten.
Reactietijd	De tijd die een opdrachtnemer heeft om statusmeldingen aan de opdrachtgever terug te melden.
Release	Een cluster van wijzigingen in één of meer ketencomponenten dat gelijktijdig wordt geïmplementeerd.

Responsetijd	De responsetijd van een applicatie of systeem geeft de tijd weer tussen het opvragen en de beschikbaarstelling van de applicatie of het systeem.
SLA	Service Level Agreement, het document waarin het afgesproken kwaliteitsniveau van de dienstverlening beschreven staat.
SNO	Service Niveau Overeenkomst; een overeenkomst waarin afspraken tussen partijen zijn vastgelegd omtrent bedrijfsprocessen, informatiestromen en gegevensuitwisseling.
Stelselontwerp	De beschrijving van de technische voorzieningen, de functionaliteiten en de specificaties die worden toegepast bij de inrichting en de werking van Suwinet. Zie voor de wettelijke omschrijving artikel 66 van de Wet structuur uitvoeringsorganisatie werk en inkomen.
Suwidesk	De tweedelijns helpdesk van BKWI-Exploitatie, waar ketenbrede incidenten, problemen en wijzigingen behandeld worden en waar de centrale technische voorzieningen van Suwinet beheerd worden.
Suwinet	Set van afspraken, regelgeving, overlegorganen en het fysieke netwerk dat de netwerken van Suwi-partijen koppelt, om zo een gestroomlijnde gegevensuitwisseling mogelijk te maken. Zie voor de wettelijke omschrijving van Suwinet artikel 1, onder p. jo. Artikel 62, tweede lid, van de Wet structuur uitvoeringsorganisatie werk en inkomen.
Suwinet-Inkijk	Het geheel van systemen dat medewerkers van Suwi-partijen online inzicht verschaft in relevante, door Suwi-partijen geregistreerde gegevens van hun cliënten.
Suwinet-Mail	Dienst met als doel dat 'secure mail' tussen partijen kan worden verzonden.
Suwinet-Meldingen	Gestandaardiseerde elektronische gegevensoverdracht tussen Suwi-partijen voor bijvoorbeeld een vooraankondiging WW of reïntegratiedvies. Ook wel elektronische ketenberichten genoemd.
Suwi-organisaties	De organisaties die deel uitmaken van de keten van werk en inkomen: UWV, GSD, Inlichtingenbureau, BKWI, SVB en Inspectie SzW. Ook wel ketenpartners genoemd.
Suwi-partijen	De Suwi-organisaties die partij zijn bij de Service Level Agreement.
Underpinning contracts	Overeenkomsten op het gebied van onderhoud en beheer, waarin afspraken zijn vastgelegd die deze SLA ondersteunen.
Wet Suwi	Wet structuur uitvoeringsorganisatie werk en inkomen. Via deze wet is de samenwerking tussen de partijen op het gebied van 'Werk en Inkomen' en de elektronische gegevensuitwisseling geregeld.
Wijzigingsbeheer	Het gecontroleerd doorvoeren van noodzakelijke wijzigingen en het voorkomen van verstoringen als gevolg van die wijzigingen.
XML-dienst	Het middel dat de gegevensbronnen van de verschillende partijen vertaalt naar gegevens op Suwinet-Inkijk.

Bijlage II: releasemomenten 2018

Release	Datum
19.01	17 januari 2019
19.02	28 februari 2019
19.03	28 maart 2019
19.04	25 april 2019
19.05	23 mei 2019
19.06	27 juni 2019
19.07	25 juli 2019
19.08	29 augustus 2019
19.09	26 september 2019
19.10	31 oktober 2019
19.11	28 november 2019
19.12	19 december 2019

Een ketenwijziging wordt pas ingepland in een release, zodra deze wijziging voorzien is van een impactbepaling. In het KetenCAB wordt vastgesteld in welke release de wijziging opgenomen wordt. In welke release de wijziging opgenomen wordt is afhankelijk van prioriteit, grootte, capaciteit, en afhankelijkheden met andere wijzigingen of projecten.

Bijlage III: Uitzonderingen openstellingstijden

Voor 2019 zijn er nog geen afwijkende openstellingstijden.