GEMEENTEBLAD
Officiële uitgave van de gemeente Westland
Nr. 27350
23 januari
2023

Beveiligingsplan Suwinet

1. Inleiding

Suwinet is het systeem van informatie-uitwisseling in de keten van Werk en Inkomen. Suwinet is een uitvloeisel van de Wet Structuur Uitvoering Werk en Inkomen. Om de Participatiewet uit te kunnen voeren is Suwinet een belangrijke factor. Het is een belangrijk knooppunt om informatie uit te wisselen met de verschillende partijen in de keten van Werk en Inkomen (met name UWV, SVB en gemeenten). Deze informatie bevat veelal persoonsgegevens. De Algemene Verordening Gegevensbescherming, de Baseline Informatiebeveiliging Overheid en de regeling SUWI (29 november 2001) vereisen dat er veilig en zorgvuldig met deze gevoelige informatie wordt omgegaan. Conform de regeling SUWI zijn we verplicht een beveiligingsplan te hebben waarin invulling wordt gegeven aan het kader van de gezamenlijke elektronische voorzieningen SUWI (art. 6.4).

1.1 Herziening Suwinet beveiligingsplan

Het Suwinet beveiligingsplan wordt periodiek (minimaal eens per drie jaar) herzien. De reden hiervan is dat wet- en regelgeving doorlopend verandert. Dit geldt tevens voor dreigingen op het gebied van de beveiliging van informatie. Het is daarom van belang dat het Suwinet beveiligingsplan actueel blijft.
Dit Suwinet beveiligingsplan vervangt het vorige Suwinet beveiligingsplan d.d. 1 oktober 2018.
Dit nieuwe Suwinet beveiligingsplan gaat in per 31 december 2022. Dit Suwinet beveiligingsplan is herzien op basis van de actuele ontwikkelingen rondom Suwinet gebruik, met inachtneming van vereisten uit de Baseline Informatiebeveiliging Overheid en de Algemene Verordening Gegevensbescherming.
Daarnaast is bij vijf interne medewerkers de vraag gesteld welke ervaring zij hebben met het oude beveiligingsplan, wat zij hierin graag behouden zien, wat zij graag veranderd zien én wat zij graag aangevuld zien in het nieuwe beveiligingsplan. De medewerkers die hierover zijn gesproken betreffen:

- Security Officer Suwinet
- Functioneel Beheerder Suwinet
- Teammanager inkomen
- Audit Coördinator Gegevensbescherming / ENSIA-coördinator
- Privacy Officer

De belangrijkste opmerkingen ten aanzien van het beveiligingsplan betroffen:

- Zorg ervoor dat het beveiligingsplan een goed naslagwerk is;
- Maak het beveiligingsplan Suwinet goed toegankelijk voor iedere medewerker (niet iedere medewerker weet het Suwinet beveiligingsplan te vinden);
- Verplicht nieuwe Suwinet gebruikers het Suwinet beveiligingsplan door te nemen;
- Neem in het Suwinet beveiligingsplan op dat alle handelingen binnen Suwinet worden gelogd én gecontroleerd;
- Neem in het Suwinet beveiligingsplan op waarvoor Suwinet wel en niet mag worden geraadpleegd.

1.2 Verantwoordelijkheid

De verantwoordelijkheid voor het gebruik en de beveiliging van Suwinet ligt op bestuurlijk niveau bij het college van Burgemeester en Wethouders en op ambtelijk niveau bij de clusterdirecteur Dienstverlening. Het college van B&W stelt het Beveiligingsplan Suwinet vast.
De gemeenteraad ziet toe op de werking van het beleid. De controle op Suwinet voert zij uit onder de paraplu van het gemeentebrede Gegevensbeschermingsbeleid in de gemeentelijke planning & control cyclus.

1.3 Kader

Dit Beveiligingsplan Suwinet is aanvullend op het gemeentebrede Gegevensbeschermingsbeleid. Dit gemeentebrede beleid is opgesteld conform de Baseline Informatiebeveiliging Overheid. De baseline geeft een specifieke invulling aan de veiligheid en gebruik van informatie binnen gemeentelijke organisaties. Het vormt daarmee ook het normenkader dat de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatie(systemen) bevordert.

Voor Suwinet is een aanvullend normenkader opgesteld, de “Verantwoordingsrichtlijn GeVS 2022 v1.0”. De uitwerking daarvan is terug te vinden in dit Suwinet Beveiligingsplan.

1.4 Status
Het Beveiligingsplan dient jaarlijks beoordeeld te worden op actualiteit. Daarnaast wordt het Beveiligingsplan jaarlijks geëvalueerd. Indien nodig worden het plan en de procedures aangepast en opnieuw ter vaststelling aan het College van B&W aangeboden. Het Beveiligingsplan kent een maximale looptijd van drie jaar.

1.5 Lijnmanager Suwinet
De lijnmanager die verantwoordelijk is voor Suwinet is de Teamleider Inkomen. Hierbij gaat het om de verantwoordelijkheid voor Suwinet in brede zin, dus de lijnmanager die verantwoordelijk is voor het hebben én uitvoeren van het Suwinet Beveiligingsplan en aan wie de taak is gegeven overkoepelend toezicht te houden op het Suwinet gebruik.

2. Functionaliteiten en beveiligingsmaatregelen

Dit beveiligingsplan is enkel van toepassing op het gebruik van Suwinet. Alle andere applicaties vallen onder het gemeentebrede informatiebeveiligingsbeleid.

2.1 Functionaliteiten Suwinet
Het BKWI levert onder de naam Suwinet verschillende producten in de vorm van applicaties die specifieke functionaliteiten bieden. Gemeente Westland maakt gebruik van de volgende producten:
- Suwinet-Inkijk voor GSD;
- Suwinet-Mail;
- Suwinet-Rapportages;
- Suwinet-Inkijk voor Burgerzaken;
- Suwinet-Inkijk voor RMC.
- Suwinet-Inkijk voor WGS
- DKD-inlezen

2.2 Suwinet-Inkijk voor GSD
Het team Inkomen van het cluster Dienstverlening maakt gebruik van Suwinet-Inkijk voor GSD. Suwinet-Inkijk is door middel van rollen toegankelijk gemaakt voor het raadplegen van klantgegevens en -informatie. Dit op basis van die taken waarvoor wettelijke grondslag is en doelbinding van gegevensgebruik is vastgesteld. Als Suwinet om andere redenen wordt gebruikt dan is er in principe sprake van ongeoorloofd gebruik.

Beveiliging:
In Suwinet-Inkijk zijn zeer privacygevoelige gegevens te raadplegen. De toegangsverlening tot Suwinet is geregeld in het hoofdstuk Toegangsrechten en autorisatiebeheer en in bijlage 1 “Procedure autorisaties”.

2.3 Suwinet-Mail
Met Suwinet-Mail kunnen partijen die gebruik maken van Suwinet, vertrouwelijke informatie sturen via een besloten netwerk. Naast het feit dat Suwinet-Mail eenvoudig in gebruik is, worden risico’s die zijn verbonden aan het mailen van klantgegevens aanzienlijk verkleind doordat het via een besloten netwerk plaats vindt.

Beveiliging
De gemeente is als organisatie aangesloten op Suwinet-Mail. Alle medewerkers met een mail-account van de gemeente kunnen gebruik maken van Suwinet-Mail. E-mail verkeer verloopt dan via een besloten netwerk.

2.4 Suwinet-Rapportages
Binnen de Suwiketen dient elke aangesloten organisatie in control te zijn aangaande de beveiliging van de eigen delen van Suwinet. Dit impliceert dat de organisatie ook een controleproces heeft ingericht om eventueel ongeoorloofd gebruik vast te kunnen stellen. Hiervoor is de rapportage-module beschikbaar gesteld. De Security Officers van Suwinet hebben toegang tot deze module. Binnen de module worden twee soorten rapportages onderscheiden: generieke en specifieke gebruiksrapportages.
Generieke rapportages worden iedere maand verstrekt. Deze geanonimiseerde rapportages zijn bedoeld om het management te ondersteunen bij het beoordelen van het gebruik van Suwinet.

Specifieke rapportages worden opgevraagd om inzicht te krijgen in de specifieke raadplegingen die zijn uitgevoerd door de medewerkers. Hierbij worden ook de persoonsgegevens van klanten versterkt.

Beveiliging
De interne controle, en daarmee de autorisatie op de rapportage-module, is uitsluitend belegd bij de Security Officers van Suwinet. De uitvoering van de controle is beschreven in het hoofdstuk "Controle".

2.5 Suwinet-Inkijk voor Burgerzaken
De gegevens die voor Burgerzaken beschikbaar zijn, betreffen de adresgegevens van iedereen die werkt of een uitkering ontvangt. Deze komen uit de loonaangifte die werkgevers en uitkeringsinstanties periodiek doen naar de Belastingdienst. Deze adresgegevens mogen alleen gebruikt worden voor het bijhouden van adresgegevens in de Basisregistratie Personen (BRP).

Beveiliging
Medewerkers van Burgerzaken loggen in op een 'eigen' pagina van Suwinet. Hier kunnen zij uitsluitend adresgegevens inzien van de klanten.

2.6 Suwinet-Inkijk voor RMC
Het raadplegen van gegevens voor de RMC-functie is regiogebonden. Gemeente Westland is aangesloten op het Regionale Meld en Coordinatiepunt (RMC) van de gemeente Den Haag. Medewerkers van gemeente Westland krijgen dan ook een Suwinet-account via de Gemeente Den Haag. Met dit account loggen ze in op een aparte VSV-pagina in Suwinet-Inkijk. Hier zijn gegevens te raadplegen als uitkeringsaanvragen, uitkeringsverhoudingen, bijzondere bijstand en re-integratie.

Beveiliging
De controle op de raadplegingen wordt uitgevoerd door de Security Officer van het RMC. Bij ongeoorloofde raadplegingen zal deze contact opnemen met de Security Officer van de gemeente West-land.

2.7 Suwinet-Inkijk voor WGS
De gegevens die voor WGS beschikbaar zijn, betreffen de gegevens over inkomen en vermogen die medewerkers van het team Schuldhulpverlening van het cluster Dienstverlening mogen raadplegen via Suwinet voor het verlenen van toegang tot schuldhulp en het opstellen van een plan van aanpak.

Beveiliging
De controle op de raadplegingen wordt uitgevoerd door de Security Officer van Suwinet.

2.8 DKD-inlezen
Het Inlichtingenbureau biedt gemeenten de mogelijkheid om DKD-klantgegevens digitaal in te lezen in de eigen, gemeentelijke applicatie.
Daarnaast is het mogelijk om elektronische aanvraagformulieren gedeeltelijk, automatisch in te laten vullen, bijvoorbeeld bij het aanvragen van een bijstandsuitkering.
Hiermee maakt DKD-Inlezen eenmalige gegevensuitvragen en het hergebruik van gegevens mogelijk.
De gegevens mogen alleen gebruikt worden voor de uitvoering van de participatiewet taken.

Beveiliging
DKD-inlezen valt onder de ENSIA-verantwoording. De applicatie die gebruik zal gaan maken van DKD-inlezen is de Suite voor het Sociaal Domein (SSD).
Voor deze applicatie is een controlemethodiek nodig waarmee de logbestanden en autorisaties gecontroleerd kunnen worden. Centric, de leverancier van de Suite, beschrijft een aantal "triggers" welke signalerend kunnen zijn voor een risicovolle handeling binnen SSD. Een raadpleging om 02:00 's nachts kan een reden zijn om de rechtmatigheid van deze raadpleging nader te onderzoeken.

Hierdoor is er een lijst van "triggers" opgesteld waarbij er bij een raadpleging eventueel nader onderzoek nodig is.
1. **Raadplegingen (ver) buiten kantoortijd**: indien een raadpleging tussen 22:00 en 07:00 plaatsvindt, moet er worden nagegaan of deze raadpleging rechtmatig was.
2. **Raadplegingen per dag**: het aantal raadplegingen dat een medewerker per dag verwerkt kan signalerend zijn voor risicovol gedrag, indien deze ver boven de door de gemeente vastgestelde waarde uitschiet. Hierbij kan de gemeente Westland zelf een waarde bepalen en zodra een medewerker hierboven komt, ontvangt de Security Officer een signaal en kan deze beslissen om de logbestanden te controleren.
3. **Raadplegingen door meerdere medewerkers**: Indien de persoonsgegevens van een burger door een hoger aantal medewerkers geraadpleegd wordt dan een vooraf bepaalde waarde, kan er reden zijn om de logbestanden te beoordelen. In het verleden kwam het bij bekende Nederlanders (BN'ers) regelmatig voor dat medewerkers van gemeentes de gegevens van BN'ers onrechtmatig opzochten indien zij (negatief) in het nieuws kwamen. Door van tevoren een waarde vast te leggen van het hoogste aantal medewerkers dat doorgaans één burger raadpleegt, kan er een signaal

worden afgegeven indien één burger ineens door twee keer zoveel medewerkers wordt geraadpleegd als de vooraf vastgelegde waarde.

Aanvullend kan worden gecontroleerd op de:

4. **Doelmatigheid van de raadpleging**: Indien een medewerker een burger raadpleegt, dan dient er een actieve klantrelatie te zijn. Dat wil zeggen dat de burger op dat moment een dienst afneemt bij de gemeente Westland of als terugbetaler staat geregistreerd. Indien dit niet het geval is, dan zal er nader onderzoek gedaan dienen te worden naar de reden van de opvraging.

Indien gebruik gemaakt wordt van DKD-inlezen binnen de Suite, kan de gemeente deze signalen gebruiken om de logbestanden van SSD te controleren. Hierbij wordt aangeraden de controle maandelijks uit te voeren. De reden hiervan is dat medewerkers over een langere periode vaak moeilijker kunnen terughalen waarom zij een bepaalde raadpleging gedaan hebben.

2.9 Whitelist

In een whitelist staan alle burgerservicenummers van burgers waar een gemeente een dienstverleningsrelatie mee heeft (gehad). Wanneer een gebruiker een burgerservicenummer van een burger opvraagt toetst Suwinet-Inkijk eerst automatisch of dit op de whitelist van de desbetreffende organisatie voorkomt. Wanneer een Burgerservicenummer niet op de whitelist van deze organisatie voorkomt, worden de bijbehorende gegevens niet getoond.

De gemeente Westland kiest er bewust voor om geen gebruik te maken van een whitelist. Ook bij het gebruik van een whitelist moet de security officer de controles op raadplegingen buiten het klantenbestand controleren met de raadplegende medewerker. Dit is noodzakelijk omdat de security officer inzicht nodig heeft in welk werkproces ten grondslag lag voor de raadpleging. Feitelijk verlicht een whitelist de controlelast van de security officer niet, terwijl de consulenten wel extra acties moeten voltooien om hun werk uit te kunnen voeren. Daarom werkt de gemeente Westland niet met een whitelist.

3. Beveiligingseisen medewerkers

3.1 Vast personeel

Binnen de opgaven wordt met persoonsgegevens gewerkt. Conform de Ambtenarenwet, de Algemene Verordening Gegevensbescherming en de wet SUWI zijn medewerkers gebonden aan geheim-houdingsbepalingen. Alle nieuwe medewerkers moeten een Verklaring omtrent Gedrag overleggen en leggen de eed/gelofte af. Nieuwe medewerkers die gebruik gaan maken van Suwinet, krijgen het Beveiligingsplan Suwinet zo spoedig mogelijk na het toekennen van de autorisaties voor Suwinet-Inkijk uitgereikt.

3.2 Extern personeel

Extern personeel ondertekent bij aanvang van de werkzaamheden in de gemeente Westland een geheimhoudingsverklaring. Deze verklaring wordt uiterlijk op de eerste werkdag ondertekend.

3.3 Bewustwording medewerkers

Aan alle medewerkers die gebruik maken van de Suwinet functionaliteiten wordt het Beveiligingsplan Suwinet uitgereikt. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld (logging). Van deze loggegevens worden geanonimiseerde rapporten opgesteld door het BKWI. Aan de hand van deze rapporten controleren de Ketenpartners of er onjuist gebruik of misbruik is gemaakt van Suwinet-Inkijk. Als er een vermoeden van ongeoorloofd gebruik bestaat kan specifieke informatie bij het BKWI worden opgevraagd.

Met het oog hierop is de navolgende informatie verstrekt aan de medewerkers die (gaan) werken met Suwinet-Inkijk:

- Het bestaan van logging en het doel hiervan;
- De (aard van de) gegevens die worden verzameld;
- Het gebruik van de gelogde gegevens; deze worden niet voor andere doeleinden gebruikt dan waarvoor ze zijn vastgelegd;
- Wanneer er sprake is van onrechtmatig of doel overschrijdend gebruik en de acties die hieruit leiden.

3.4 Geoorloofd / ongeoorloofd gebruik

Als de geautoriseerde medewerkers Suwinet doelmatig gebruiken dan is er sprake van geoorloofd gebruik. Als Suwinet wordt gebruikt in het kader van de Participatiewet, de Wet Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ) of de Wet inkomensvoorziening

oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW), is er sprake van doelmatig Suwinet gebruik.
Wordt Suwinet om andere redenen gebruikt dan is er in principe sprake van ongeoorloofd gebruik. Dit ongeoorloofd gebruik wordt onderzocht door de Security Officer en gemeld aan de eindverantwoordelijke manager.

3.5 Maatregelen bij onrechtmatig gebruik
Bij geconstateerd onrechtmatig gebruik van Suwinet zal de gemeente conform het 'Privacyreglement gebruik Suwinet'(zie bijlage 3) maatregelen opleggen.

3.6 Wachtwoord
Suwinet-Inkijk vraagt zelf om een periodieke wijziging van het wachtwoord. Het herstellen van een wachtwoord verloopt via Applicatiebeheer. Zij geven een tijdelijk wachtwoord uit dat veertien dagen geldig is.

3.7 Kennisnemen van het beveiligingsplan Suwinet
Dit beveiligingsplan Suwinet is van toepassing op alle gebruikers van Suwinet-Inkijk binnen de gemeente Westland. Het plan wordt op Schulinck (Grip op) gepubliceerd en is voor iedereen toegankelijk in het document management systeem (Corsa). Alle gebruikers worden minimaal twee maal per jaar in een periodiek werkoverleg door hun manager geattendeerd op de inhoud van dit plan. Nieuwe medewerkers worden onder verantwoordelijkheid van de manager geattendeerd op de inhoud van dit plan met de opdracht er kennis van te nemen. Hierdoor weten de medewerkers welk gedrag de organisatie van hen verwacht en weten ze dat er gegevens worden bewaard waarmee hun gedrag gecontroleerd kan worden. De controle op de logbestanden mag alleen indien hier redelijkerwijs aanleiding toe is.

3.8 Bewaarperiode logbestanden
De logbestanden worden eenmaal per jaar vernietigd gedurende de eerste twee weken van januari. Op dat moment worden de logbestanden verwijderd van het jaar voorafgaand aan het afgesloten jaar. Bijvoorbeeld: in de eerste twee weken van januari 2023 worden alle logbestanden verwijderd uit 2021. Dat wil zeggen dat er een maximale bewaarperiode bestaat van 2 jaar. Hier is voor gekozen omdat het risico op het langer bewaren van de logbestanden kan leiden tot oneigenlijk gebruik van deze bestanden. Het korter bewaren van deze bestanden zou ertoe kunnen leiden dat eventuele vragen op de bevindingen uit de controles, onvoldoende kunnen worden beantwoord. Op basis van deze risico afweging wordt dan ook geconcludeerd dat de gestelde bewaarperiode (minimaal 1 jaar en maximaal 2 jaar) voldoende waarborgen biedt voor zowel de integriteit als de betrouwbaarheid van de logbestanden en de daaruit voort gevloeide bevindingen.

4. Toegangsrechten en autorisatiebeheer

4.1 Beleid ten aanzien van autorisaties
De autorisaties voor Suwinet worden per medewerker toegekend aan de hand van de autorisatiematrix. De manager van de medewerker geeft aan welke autorisaties een medewerker nodig heeft voor het uitvoeren van zijn taken. De wijze waarop de autorisaties worden toegekend, gewijzigd of ingetrokken staat onderaan dit hoofdstuk nader beschreven.

4.2 Autorisatieplan medewerkers
In de bijlage 5 "Verantwoordelijkheden en rollen Suwinet" zijn de rollen en het daarbij behorende toegestane gebruik van dit medium beschreven.

4.3 Autorisatiematrix
Er is een autorisatiematrix opgesteld om helder weer te geven welke rechten aan de verschillende rollen worden toegekend. Deze rechten zijn vooraf, in deze matrix, vastgesteld. Applicatiebeheer kan op basis van deze matrix snel de juiste rechten aan een medewerker toekennen. In de bijlage 4 wordt de autorisatiematrix gepresenteerd.

4.4 BKWI autorisaties en conflicterende rollen
Het BKWI heeft uiteengezet welke autorisaties conflicterend kunnen zijn en derhalve risico's met zich meebrengen indien deze gelijktijdig worden toegewezen aan één medewerker.
De gemeente Westland vindt het belangrijk dat er maatregelen zijn getroffen om onbedoelde of ongeautoriseerde wijzigingen of misbruik van bedrijfsmiddelen te voorkomen,

Hierom conformeert de gemeente zich aan de beschrijving van de autorisaties zoals aangegeven in dit overzicht van het BKWI: Overzicht autorisaties op Suwinet-Inkijk voor GSD (v20201015). Derhalve implementeert de gemeente Westland functiescheiding binnen Suwinet zoals benoemd in het voorgaande overzicht van het BKWI.

4.5 SSD autorisaties en conflicterende rollen

Centric, de leverancier van de Suite voor het Sociaal Domein, onderschrijft dat zij gemeenten de mogelijkheid biedt om te voorkomen dat conflicterende rollen aan één medewerker toegewezen kunnen worden. Met conflicterend wordt wederom verwezen naar rollen die risico's met zich meebrengen indien deze gelijktijdig worden toegewezen aan één medewerker. Het is de verantwoordelijkheid van de gemeente om zelf te bepalen bij welke rollen deze functiescheiding wordt toegepast.

Bijlage 1 Procedure autorisaties

Inleiding

De procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor Suwinet-Inkijk en de controle hierop.

De procedure bestaat uit twee afzonderlijke deelprocedures die apart worden uitgevoerd:
- Autorisaties tot Suwinet-Inkijk;
- Periodieke controle autorisaties;

Met een autorisatie wordt bedoeld het door het bevoegd gezag verstrekken van een gelegitimeerde toegang tot een of meerdere informatiesystemen van de gemeente.

Om toegang te krijgen tot de gegevens is naast de specifieke autorisatie in de desbetreffende applicatie tevens een bevoegdheid nodig op het netwerken en/of het systeemniveau. Deze laatstgenoemde bevoegdheden worden beheerd door de systeembeheerder. De bevoegdheden binnen de applicatie Suwinet-Inkijk worden beheerd door de functioneel beheerder van Suwinet.

Verantwoordelijkheid
De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het College van B&W, en namens dit college de clusterdirecteur Dienstverlening.

De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij Suwinet-Inkijk berust bij de clusterdirecteur Dienstverlening. De uitvoering hiervan en het up-to-date houden van de procedure ligt bij de Security Officer van Dienstverlening.

Uitvoering

Autorisatie tot Suwinet -Inkijk
- Per medewerker wordt één of meerdere rollen toegekend.;
- De medewerker vraagt via Topdesk de autorisatie aan. Hierbij wordt gelijk ook de benodigde rol aangegeven. De Teammanager keurt de aanvraag. Na goedkeuring verzorgt de functioneel beheerder de toegang tot Suwinet;
- De medewerker geeft tussentijdse wijzigingen in taak/functie die gevolgen hebben voor de autorisatie door, via Topdesk. De Teammanager keurt de wijzigingen goed.
- Bij vertrek van de medewerker worden de hem/haar toegekende autorisaties direct beëindigd;
- Suwinet-Inkijk is voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes;
- De wachtwoorden voor Suwinet-Inkijk zijn maximaal 90 dagen geldig.
- Als een gebruiker gedurende 90 dagen achtereen niet heeft ingelogd wordt het wachtwoord automatisch geblokkeerd;
- Na driemaal foutief inloggen wordt het account automatisch geblokkeerd. Alleen de applicatiebeheerder kan het account weer vrijgeven;

Periodieke controle autorisaties
De Securtiy Officer controleert maandelijks de actualiteit en rechtmatigheid van de uitgegeven autorisaties. De wijze van controleren is als volgt:

- De applicatiebeheerder draait een lijst van gebruikers, gebruikersgroepen en ingevoerde autorisaties voor Suwinet-Inkijk uit;
- De security officer maakt een inventarisatie van de gebruikers, gebruikersgroepen en de toegekende autorisaties;
- Vervolgens verzoekt de security officer de betrokken teammanagers de autorisaties van hun medewerkers te controleren op actualiteit en juistheid;
- Voor zover nodig actualiseert de security officer het gebruikersoverzicht en de gebruikers-groepen.

Bijlage 2 Protocol Inzage Suwinet-Inkijk door Cliënt

De cliënt verzoekt om inzage, hetzij schriftelijk, hetzij mondeling in diens gegevens

- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs;
- Vraag om het BSN van de cliënt;
- Stel vast dat het BSN is ontleend aan een officieel document;
- Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm;
- Berg uitdraai onmiddellijk op in het cliëntendossier of vernietig eventueel uitgedraaid exemplaar;
- Beëindig inkijksessie.

Het is mogelijk dat een cliënt telefonisch vraagt om een uitdraai van zijn/haar gegevens. In dat geval dient de cliënt verwezen te worden naar het de balie of moet een schriftelijk verzoek ingediend worden. Dit verzoek moet binnen de wettelijke verplichte termijn afgehandeld worden.

Indien de cliënt inzage wil in al zijn/haar gegevens die bij een ketenpartner zijn geregistreerd, dient de cliënt te worden verwezen naar de betreffende ketenpartner.

Bijlage 3 Privacyreglement gebruik Suwinet

HOOFDSTUK 1 DEFINITIES, REIKWIJDTE EN DOELEINDEN

Artikel 1 Definities

In dit privacyreglement wordt verstaan onder:

a. AVG: Algemene Verordening Gegevensbescherming;
b. Autoriteit Persoonsgegevens (AP): de toezichthoudende autoriteit als bedoeld in artikel 51 AVG;
c. gemeente: de gemeente Westland;
d. betrokkene: gebruiker van de applicatie Suwinet op wie een persoonsgegeven betrekking heeft en die aan te merken is als:
    1. medewerker in dienst van de gemeente;
    2. persoon die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verricht, anders dan in ambtelijk dienstverband;

e. Suwinet: de door of namens de gemeente aan betrokkenen ter beschikking gestelde applicatie. Daar waar in dit reglement applicatie geschreven staat wordt de applicatie Suwinet bedoeld. Suwinet biedt overheidsorganisaties de mogelijkheid om persoonsgegevens van burgers, die bij verschillende organisaties of basisregistraties zijn opgeslagen, te raadplegen in één webtoepassing;
f. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de AVG;
g. verwerken van persoonsgegevens: elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
h. monitoren: het inhoudelijk en op individueel niveau volgen van het gebruik;
i. bestand: elk, al dan niet geautomatiseerd, gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
j. verantwoordelijke: het college van burgemeester en wethouders, zijnde het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
k. onrechtmatig gebruik dan wel misbruik van de applicatie Suwinet: een doen of nalaten in strijd met dit privacyreglement of andere wet- en regelgeving of een inbreuk op een recht.

Artikel 2 Reikwijdte

1. Dit beveiligingsplan is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van de applicatie Suwinet.
2. Dit beveiligingsplan geldt voor medewerkers in dienst van de gemeente en personen die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband.

Artikel 3 Doeleinden

1. De verwerking van persoonsgegevens van medewerkers inzake het gebruik van de applicatie Suwinet heeft de volgende doeleinden:
    a. het verkrijgen van inzicht in de mate van gebruik van de applicatie;
    b. het voorkomen van onrechtmatig gebruik dan wel misbruik van de applicatie;
    c. Het behulpzaam zijn in het aantonen van mogelijk misbruik.

2. De omvang van de controle ter voorkoming van onrechtmatig gebruik, dan wel misbruik van de applicatie als bedoeld in het eerste lid sub b, wordt zo beperkt mogelijk gehouden, in die zin dat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend.

HOOFDSTUK 2 VERANTWOORDELIJKHEDEN EN BEHEER

Artikel 4 Verantwoordelijkheden en beheer

1. Door de verantwoordelijke worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
2. Door de verantwoordelijke worden passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
3. Door de verantwoordelijke worden één of meerdere applicatiebeheerders aangewezen die belast zijn met het beheer van de applicatie. Deze applicatiebeheerders zijn, op grond van artikel 125a, derde lid, Ambtenarenwet, verplicht tot geheimhouding van de persoonsgegevens waarvan zij

kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

HOOFDSTUK 3 GEBRUIK APPLICATIE

Artikel 5 Gebruik applicatie

1. Betrokkenen gebruiken de applicatie voor het uitvoeren van de aan hen door de gemeente opgedragen taken.
2. Betrokkenen zullen bij het gebruik van de applicatie de nodige zorgvuldigheid (het zogenaamde 'goed huisvaderschap') betrachten en de integriteit en goede naam van de gemeente waarborgen.

Artikel 6 Voorkomen onrechtmatig gebruik dan wel misbruik

De gemeente neemt zo veel mogelijk maatregelen in technische en organisatorische zin ter voorkoming van onrechtmatig gebruik dan wel misbruik van de applicatie. Welke maatregelen dat zijn zal jaarlijks worden bepaald in een op te stellen informatie beveiligingsplan.

HOOFDSTUK 4 VASTLEGGING, BEWARING, VERWIJDERING EN VERSTREKKING PERSOONSGEGEVENS

Artikel 7 Vastlegging

1. Elektronisch vastleggen van persoonsgegevens geschiedt (automatisch) door de door de gemeente ingezette software.
2. De vastlegging, na toestemming burgemeester of gemeentesecretaris, beperkt zich tot de gegevens die noodzakelijk zijn voor de doeleinden van de verwerking als bedoeld in artikel 3, eerste lid.

Artikel 8 Persoonsgegevens

1. In de in artikel 7 genoemde vastlegging worden ten hoogste de volgende persoonsgegevens opgenomen:
   a. gebruikersidentificatie, naam, voornaam of voorletters van de betrokkene;
   b. naam en/of codering van de afdeling (of het team) waaronder de betrokkene valt;
   c. gegevens over de toegang tot Internet die door de gemeente is geboden aan de betrokkene, inclusief gebruikersnaam en Internet protocoladres;
   d. gegevens betreffende de datum en het tijdstip van het openen van de toegang tot Internet door de betrokkene;
   e. de inhoud van de door de betrokkene verzonden, dan wel ontvangen berichten;

2. Indien er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de applicatie door betrokkene, kan door de verantwoordelijke opdracht worden gegeven om nader onderzoek te verrichten.

Artikel 9 Bewaring en verwijdering

De in artikel 8, eerste lid, genoemde persoonsgegevens worden maximaal drie maanden bewaard. Gegevens die ouder zijn dan drie maanden worden automatisch verwijderd, tenzij er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de applicatie in die periode. In dat geval worden de gegevens uit die betreffende maand bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen ten opzichte van een betrokkene noodzakelijk is. Zo-dra een nader onderzoek is afgerond en dit niet leidt tot maatregelen tegen een betrokkene worden de gegevens verwijderd.

Artikel 10 Personen aan wie persoonsgegevens worden verstrekt

De vastgelegde persoonsgegevens kunnen worden verstrekt aan:

1. Alle bij Suwinet betrokken leidinggevenden, om inzicht te verkrijgen in de mate van gebruik.
2. De verantwoordelijke indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de applicatie. Het betreft hier dan de gegevens als bedoeld in artikel 8, eerste lid.
3. Degene(n) die in opdracht van de verantwoordelijke is (zijn) belast met of leiding geeft (geven) aan onderzoek naar onrechtmatig gebruik dan wel misbruik van de applicatie. Het betreft hier dan de gegevens als bedoeld in artikel 8, eerste lid.

HOOFDSTUK 5 RECHTEN VAN BETROKKENE: VERBETEREN, AANVULLEN, VERWIJDEREN OF AFSCHERMEN PERSOONSGEGEVENS

Artikel 11 Rechten van de betrokkene

1. Aan de betrokkene die daarom aan verantwoordelijke verzoekt, wordt een overzicht verschaft van de hem/haar betreffende persoonsgegevens die worden verwerkt. Indien een gewichtig belang van de verzoeker dit eist, voldoet de verantwoordelijke aan dit verzoek in een andere dan schriftelijke vorm, dat aan dat belang is aangepast.

2. Degene aan wie overeenkomstig het eerste lid kennis is gegeven van de hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.
3. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed. Een beslissing op een verzoek geldt als een besluit in de zin van artikel 1:3, Algemene wet bestuursrecht.
4. De verantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

HOOFDSTUK 6 SANCTIES, OPENBAARMAKING, INWERKINGTREDING EN SLOTBEPALING

Artikel 12 Sancties
1. Overtreding van dit beveiligingsplan kan voor medewerkers in dienst van de gemeente resulteren in disciplinaire maatregelen als bedoeld in de arbeidsvoorwaardenregeling van de gemeente.
2. Overtreding van dit beveiligingsplan kan voor personen die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband, resulteren in maatregelen waardoor deze personen, al dan niet tijdelijk, geen beschikking meer hebben over (een deel van) de applicatie.

Artikel 13 Onvoorziene omstandigheden
In gevallen waarin dit beveiligingsplan niet voorziet of bij twijfel over de toepassing van dit beveiligingsplan beslist het college van burgemeester en wethouders van de gemeente Westland.

Artikel 14 Openbaarmaking en inwerkingtreding
1. Dit beveiligingsplan wordt verstrekt of ter beschikking gesteld aan degenen die, direct of indirect, de beschikking krijgen over applicatie.
2. Dit beveiligingsplan treedt in werking op de eerste dag na publicatie.

Artikel 15 Slotbepaling
1. Onverminderd het bepaalde in dit beveiligingsplan, zal op het verwerken van persoonsgegevens de op 25 mei 2018 in werking getreden AVG van toepassing zijn.
2. Deze Regeling kan worden aangehaald als "Beveiligingsplan Suwinet ".

Bijlage 4 Autorisatiestructuur

Nr	Id	N.aam	Pad	Categorie	Kans op onrechtmatig gebruik	Poortwachter	Terugvordering en verhaal	Beheer	Boete ambtenaar	Uitkerings-administratie	Inburgering	BBZ	Security officer (fictief)	Gebruikers-beheerder (fictief)	Voor-administratie LO (fictief)
1	nvt	Bedrijfsmiddelen	gd/dzr	nvt	▲	v	v	v	v			v			
2	nvt	Beheer: ww & blokkeren	gd/uurcriadmin iis	nvt	▲▲	v	v	v	v			v			
3	nvt	Bels.stngdienst	gd/bels.stngdienst	nvt	▲▲	v	v	v	v			v			
4	nvt	Bijstandsregelingen	gd/bijstandsregelingen	nvt	▲▲▲	v	v	v	v			v			
5	nvt	Contactservice	C:\gpd	nvt											
6	nvt	Download de generieke rapportages	/report/reportfilescever	nvt											
7	nvt	Download de specifieke rapportages	/report/reportfilescever pr	nvt											
8	nvt	DUO gegevens	gd/duo gegevens	nvt	▲▲	v	v	v	v			v			
9	nvt	Fraude scorelijst	gd/fisc	nvt	▲▲	v	v					v			
10	nvt	Fraude verdachten	gd/fraude verdachten	nvt	▲▲	v	v	v	v			v			
11	nvt	GBA Volledig	gd/gba volledig	nvt	▲▲▲	v	v	v	v			v			
12	nvt	Gebruikersadministratie	gd/gbruiadmin	nvt										v	
13	nvt	GSD voor IB groep	https://bgroep prod.suwi	nvt											
14	nvt	Info matrix verhoudingen	gd/i nfo matrix verhoudi ng	nvt	▲▲										
15	nvt	Ka dster	gd/kadaster	nvt	▲▲▲	v	v	v	v	v		v			
16	nvt	Klant algemeen	gd/klant algemeen	nvt	▲▲▲										
17	nvt	Kontaktdirectiess	gd/kontaktdirectiess	nvt	▲▲▲	v			v			v			
18	nvt	Onderhouden contracte service	gd/tripp ox admin	nvt											
19	nvt	Onderhouden status wijzigingverzoeken	gd/tripp ox	nvt											
20	nvt	Onderhouden werkboomraad	gd/werkboomraad	nvt											
21	nvt	Openbare generieke gebruikersrapportages	gd/dbdocumenten	nvt	▲▲										
22	nvt	Openbare specifieke gebruikersrapportages	gd/dbdocumenten privacy	nvt	▲▲▲▲▲								v		
23	nvt	RDW	gd/rdw	nvt	▲▲	v	v	v	v			v			
24	nvt	RDW+	gd/rdw plus	nvt	▲▲	v	v	v	v			v			
25	nvt	RDW peildata	gd/rdw peildata	nvt	▲▲	v	v	v	v			v			
26	nvt	Rechtmatigheid+	gd/rechtmatigheid plus	nvt	▲▲▲	v	v	v	v			v			
27	nvt	Re integratie	gd/re integratie	nvt	▲▲	v	v	v	v		v				
28	nvt	SBR Query	gd/sbrq	nvt	▲▲	v	v	v	v						
29	nvt	SCI	https://bgroep prod.suwi	nvt	▲▲										
30	nvt	SVB gegevens	gd/svb gegevens	nvt	▲▲			v							
31	nvt	UWV Uitkeringen	gd/uwv uitkeringen	nvt	▲▲			v		v					
32	nvt	UWWB	gd/cwi	nvt	▲▲	v	v	v	v			v			
33	nvt	Whitelist scope	http://special resources/w	nvt	▲▲▲▲	v	v	v	v			v			
34	nvt	Wis proxy	https://wis productie.suwi	nvt		v	v								
35	nvt	www.werk.nl	https://www.werk.nl:443/	nvt											
36	nvt	Zoek in kadaster	gd/zoek in kadaster	nvt	▲▲▲▲▲										
37	nvt	Zoek in RDW	gd/zoek in rdw	nvt	▲▲▲▲▲										
38	nvt	Zoek in RDW+	gd/zoek in rdw plus	nvt	▲▲▲▲▲	v									

Eigen rollen Gemeente Westland

Vaste rollen Suwinet

Nr	Id	Naam	Afdeling	Categorie	Kans op onrechtmatig/ongeoorloofd gebruik	Poortwachter	Terugvordering en verhaal	Beheer	Bootte ambte naar	Uitkerings-administratie	Inburgering	BBZ	Security officer	Gebruikersbeheerder	Vooradministratie ID
8	R1135	EROW	/SUWI/gsd/westland	Vaste rollen buiten Suwinet		V									V
9	R1525	EROW beheer	/SUWI/gsd	Vaste rollen buiten Suwinet											
32	SC02	SC02 Raadpleging ISI op BSN	/SUWI/gsd	Vaste rollen buiten Suwinet											
33	SC03	SC03 Raadpleging ISI op BSN of adres	/SUWI/gsd	Vaste rollen buiten Suwinet											
34	SC05	SC05 Muteren ISI	/SUWI/gsd	Vaste rollen buiten Suwinet											
35	SC06	SC06 Alle bevoegdheden incl signalen	/SUWI/gsd	Vaste rollen buiten Suwinet							V				
36	R3841	SC07 Raadplegen PW gegevens	/SUWI/gsd	Vaste rollen buiten Suwinet											
3	R3130	Beheer ww & bbz rollen	/SUWI/gsd	Vaste beheerrollen											
15	SD03 2	SD03 2 Onderhouden correctieservice	/SUWI/gsd	Vaste beheerrollen											
18	GSD/MDM	Gebruikersbeheerder	/SUWI/gsd	Vaste beheerrollen										V	
22	R3846	Onderhouden werkvoorraad	/SUWI/gsd	Vaste beheerrollen											
23	R3347	Opvragen gemeentelijk gebruikersrapportage	/SUWI/gsd	Vaste beheerrollen									V		
24	RAPPORT_SPEC	Opvragen specifiek gebruikersrapportage	/SUWI/gsd	Vaste beheerrollen									V		
42	WE_GSD	Wijziging lijst escape	/SUWI	Vaste beheerrollen											
4	R1043	Beheer tijdelijk gebruikersbeheer	/SUWI/gsd	Vaste gebruikersrollen											
5	SD19	Bijstandsregelingen	/SUWI/gsd	Vaste gebruikersrollen											
7	R3724	BUIG gegevens	/SUWI/gsd	Vaste gebruikersrollen											
10	R1272	Fraude verdenkingen	/SUWI/gsd	Vaste gebruikersrollen											
11	SD03	SD03 UWWb	/SUWI/gsd	Vaste gebruikersrollen											
12	SD04	SD04 Fraude scorekaart	/SUWI/gsd	Vaste gebruikersrollen											
13	SD24	SD24 Bedrijvenregister	/SUWI/gsd	Vaste gebruikersrollen											
14	SD31	SD31 Correctieservice	/SUWI/gsd	Vaste gebruikersrollen											
16	SD40	SD40 Onderhouden status wijzigingsverzoeken	/SUWI/gsd	Vaste gebruikersrollen											
17	SD42	SD42 klant algemeen	/SUWI/gsd	Vaste gebruikersrollen											
20	R3726	Inkomstenverhoudingen	/SUWI/gsd	Vaste gebruikersrollen											
21	R2786	Kostendoelartikels	/SUWI/gsd	Vaste gebruikersrollen											
26	SD20	EROW	/SUWI/gsd	Vaste gebruikersrollen											
27	R1919	EROW +	/SUWI/gsd	Vaste gebruikersrollen											
28	R454	EROW gelddata	/SUWI/gsd	Vaste gebruikersrollen											
29	R3727	Rectificatiegheid	/SUWI/gsd	Vaste gebruikersrollen											
30	R3728	Rectificatiegheid +	/SUWI/gsd	Vaste gebruikersrollen											
31	R3725	Re integratie	/SUWI/gsd	Vaste gebruikersrollen											
38	R3722	SVB gegevens	/SUWI/gsd	Vaste gebruikersrollen											
41	R3723	UWV Uitkeringen	/SUWI/gsd	Vaste gebruikersrollen											
43	R2355	Zoek in ROW	/SUWI/gsd	Vaste gebruikersrollen											
44	R1920	Zoek in ROW +	/SUWI/gsd	Vaste gebruikersrollen											

Bijlage 5 Verantwoordelijkheden en rollen Suwinet

Er zijn verschillende profielen gedefinieerd om gebruik te maken van Suwinet:

- De Security Officer (opvragen generieke en specifieke rapportages)
- De Gebruikersbeheerder (gebruikersbeheer)
- BBZ (raadplegen)
- Inburgering (raadplegen en mutaties Wet Inburgering via Portal Inburgering)
- Uitkeringsadministratie (raadplegen)
- Boeteambtenaar (raadplegen)
- Beheer (raadplegen)
- Terugvordering en verhaal (raadplegen)
- Poortwachter (raadplegen)
- Sociale Recherche (handhaven)
- WGS (Raadplegen)

Security Officer
Deze functionaris is geautoriseerd voor het opvragen van algemene gebruikersrapportages bij het BKWI via Suwinet-Inkijk. Als daar aanleiding toe is kan deze functionaris ook specifieke rapportages opvragen.

Applicatiebeheerder
De applicatiebeheerder is geautoriseerd voor het verlenen van toegang tot Suwinet-Inkijk voor geautoriseerde gebruikers en het verwijderen van deze toegang.

Consulenten BBZ
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op het adviseren over de mogelijkheden en het verlenen van bijzondere bijstand aan ondernemers.

Consulent Inburgering
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op inburgeringswerkzaamheden.

Medewerkers Uitkeringsadministratie
Deze groep is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op Uitkeringsverwerking: debiteuren, (her)onderzoeken ter vaststelling van de actuele woonplaats, de draagkracht, de hoogte van het inkomen en de werkgever.

Boeteambtenaren
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op het verwerken van boetes van klanten die de inlichtingenplicht hebben geschonden.

Consulenten Beheer
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op het lopende klantenbestand. Het zijn de klantmanagers die het contact met de klanten onder handen nemen nadat de poortwachter heeft bepaald dat de klant uitkeringsgerechtigd is.

Consulent Terugvordering en Verhaal
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op het terugvorderen en invorderen van teveel ontvangen uitkeringen, het verhaal van verstrekte uitkeringen op derden en het onderzoek naar het opleggen van een boete op grond van de Participatie-wet, IOAW en IOAZ.

Poortwachters
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens om te beoordelen of een klant recht op uitkering hebben. Hierbij hebben ze ook de autorisatie op de zwaardere zoekfunctie "Zoeken op RDW+".

Sociale Recherche
De sociale recherche werkt signaal-gestuurd en gaat op mogelijk frauduleuze signalen af. Bij fraude met een uitkering of zorggelden is de Sociale Recherche de opsporingsinstantie.

Consulenten WGS
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op het verlenen van toegang tot schuldhulp en het opstellen van een plan van aanpak.