Informatiebeveiligingsbeleid & Beveiligingsplan Suwinet

Werkplein Fivelingo

Namens de gemeenten Delfzijl, Appingedam en Loppersum

Datum : 22 mei 2017

Versie : 4.0

Versiebeheer

Versie	Datum	Wijzigingen	Afgestemd met	Vastgesteld
1.0	29-07-2008	**Informatiebeveiligingsbeleid ISD Noordoost** (versie BACIT)	MT, Directie, DB, AB	29-07-2008
2.0	10-10-2014	**Informatiebeveiligingsbeleid ISD Noordoost**	Security officer MT, Directie	10-10-2014
3.0	12-03-2015	**SUWI Informatiebeveiligingsbeleid ISD Noordoost** (Update conform SUWI-wetgeving)	MT, Directie, DB, AB	12-03-2015
4.0	22-05-2017	**Informatiebeveiligingsbeleid & Beveiligingsplan Suwinet Werkplein Fivelingo** (Aangepast aan de nieuwe organisatie en actuele wet- en regelgeving van dit moment)	Security officer, MT, Directie Dagelijks Bestuur	MT 30-05-17 DB 08-06-17

Referentie

Organisatie: Gemeenschappelijke Regeling Werkplein Fivelingo

Opdrachtgever: Egberdien ten Brink, Directeur Werkplein Fivelingo

Samenstelling: Mirjam Eefting-ter Maat, Bart Lensink

Datum: 22-05-2017

Versie: 4.0

Naam document: Werkplein Fivelingo - Informatiebeveiliging & Suwinet - versie 4.0 (22-05-17).docx

Inhoud

Leeswijzer

Het 'informatiebeveiligingsbeleid & beveiligingsplan Suwinet' is een samenvoeging van twee oorspronkelijke documenten. Het informatiebeveiligingsbeleid geeft een brede opzet en sluit aan op de Baseline Informatiebeveiliging Gemeenten (BIG).

Het beveiligingsplan Suwinet is daar later aan toegevoegd en is een verbijzondering van het informatiebeveiligingsbeleid op het gebied van de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI). Klantgegevens worden uitgewisseld voor het Digitaal Klant Dossier via het netwerk Suwinet. Als gevolg van de Regeling Suwi is elke gemeente verplicht te beschikken over een actueel informatiebeveiligingsplan. Hierin staat welke beveiligingsmaatregelen er worden getroffen.

Zowel het informatiebeveiligingsbeleid als beveiligingsplan Suwinet hebben een dynamisch karakter, en moeten jaarlijks worden geëvalueerd en zonodig geactualiseerd. Deze versie is de eerste versie voor Werkplein Fivelingo. Aan dit document is een evaluatie van de huidige stand van zaken met aanbevelingen/ voorstellen voor het managementteam van Werkplein Fivelingo toegevoegd.

Dit document kent de volgende opbouw:

Hoofstuk 1 geeft de aanleiding en doelstelling van dit document weer.

Hoofdstuk 2 gaat nader in op de onderhavige wet en regelgeving en de normstelling waaraan dit document moet voldoen. Het normenkader Gezamenlijke elektronische Voorzieningen Suwi (GeVS) hanteert zeven normen waaraan het huidige beleid in bijgaande evaluatie worden getoetst.

Hoofdstuk 3 is het geactualiseerde informatiebeveiligingsbeleid van Werkplein Fivelingo. Het gaat hier om de organisatie van informatiebeveiliging gericht op het voorkomen dat vertrouwelijke informatie in verkeerde handen komt of verloren gaat. Het gaat hierbij om technische voorzieningen en het gedrag van medewerkers.

Hoofdstuk 4 is het geactualiseerde beveiligingsplan Suwinet waaraan Werkplein Fivelingo zich conformeert. Het gaat hier met name om taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van (Suwinet)-gegevens.

In de bijlagen komen een aantal specifieke documenten terug die van belang zijn voor de organisatie van de informatiebeveiliging zoals de 'Tien gouden regels bij beveiliging van persoonsgegevens', rollen, taken en verantwoordelijkheden, de taakbeschrijving van de Security Officer, de 'Gedragscode internet en emailgebruik', de geheimhoudingsverklaring en het 'Protocol inzage in Suwinet door cliënt en/of gemachtigde'.

1 Inleiding

Aanleiding

Werkplein Fivelingo is een fusieorganisatie van de Intergemeentelijke Sociale Dienst (ISD) Noordoost en de sociale werkvoorziening Fivelingo. De organisatie heeft als doel het verstrekken van uitkeringen en het naar werk begeleiden van mensen die afhankelijk zijn van een uitkering. Dit betekent dat er persoonsgegevens verwerkt worden. De verwerking van persoonsgegevens brengt nieuwe verantwoordelijkheden met zich mee op het gebied van beveiliging.

Klanten van Werkplein Fivelingo leveren hun gegevens aan in het vertrouwen dat deze gegevens alleen beschikbaar zijn bij Werkplein Fivelingo. Het lekken van persoonlijke gegevens kan gevolgen hebben voor de belanghebbende. Als persoonlijke gegevens kunnen namen, adressen, contactgegevens en bankgegevens of combinaties hiervan aangemerkt worden. Werkplein Fivelingo is verantwoordelijk voor deze gegevens en zal moeten kunnen aantonen dat de beveiliging van gegevens voldoende is.

De directie van Werkplein Fivelingo geeft met dit beleidsdocument richting aan informatiebeveiliging in overeenstemming met bedrijfsmatige eisen en relevante wetten en voorschriften. Zij volgt hierin, naast SUWI-wet– en regelgeving, de normstelling van de Baseline Informatiebeveiliging Gemeenten (hierna BIG te noemen).

Dit beleidsdocument is geaccordeerd door het managementteam en de directie van Werkplein Fivelingo, en wordt met geplande tussenpozen beoordeeld om doeltreffendheid te waarborgen.

Doelstelling informatiebeveiligingsbeleid en informatiebeveiligingsplan SUWI

Definitie informatiebeveiliging

Onder informatiebeveiliging wordt verstaan: Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces. Betrouwbaarheid is de overkoepelende term voor beschikbaarheid (continuïteit, responstijd), integriteit (juistheid, volledigheid, tijdigheid, geoorloofdheid) en vertrouwelijkheid (exclusiviteit). Hiermee wordt aangegeven in welke mate de organisatie kan vertrouwen op een informatiesysteem voor haarinformatievoorziening. Dit betreft zowel de technische, de organisatorische, als de menselijke aspecten.

Werkplein Fivelingo biedt met haar Informatiebeveiligingsbeleid een juiste basis voor het verantwoord om gaan met de aan haar toevertrouwde gegevens, een veilige werkplek voor haar medewerkers en adequate waarborging voor de continuïteit van haar bedrijfsprocessen en dienstverlening.

Voor de realisatie van het Informatiebeveiligingsbeleid is Werkplein Fivelingo in veel gevallen afhankelijk van partners en derden. Zij neemt daarbij haar verantwoordelijkheid door het initiatief te nemen voor overleg en samenwerking. Verder voert zij regelmatige de noodzakelijke controles uit op de realisatie en uitvoering van maatregelen, zowel intern als extern bij derden.

2 Wettelijk kader

2.1 Inleiding

Door de (nieuwe) Europese wetgeving, de technische mogelijkheden en de decentralisaties wordt het veld rond privacy voor gemeenten steeds complexer. Privacy is niet langer een onderwerp waar alleen juristen mee bezig zijn; privacy raakt de hele gemeentelijke organisatie. Gemeenten zijn nu bezig om de brede privacy benadering te borgen in de organisatie. Bijvoorbeeld door het aanstellen van een Functionaris Gegevensbescherming of een privacy officier.

Dit alles speelt zich af in een periode waarin vanaf 1 januari 2016 de Wet Meldplicht Datalekken in werking is getreden die kan leiden tot bestuurlijke boetes oplopend tot ruim 8 ton. In 2016 werd in de gehele Europese Unie de Algemene Verordening Gegevensbescherming (AVG) aangenomen. Deze verordening vervangt de huidige Wet bescherming persoonsgegevens. Gemeenten hebben naar verwachting tot 2018 om hun gegevensbescherming in lijn te brengen met de nieuwe wet en regelgeving. Deze nieuwe wetgeving moet zorgen voor harmonisatie van de huidige privacyregelgeving in Europa en verbetering van de privacy(bescherming) van burgers. In dit hoofdstuk nemen we de voor Werkplein Fivelingo meest relevante wet- en regelgeving onder de loep.

2.2 Algemene Verordening Gegevensbescherming (AVG).

De Europese Commissie en het Europees Parlement hebben besloten dat de huidige wetgeving niet langer aansluit op de constante veranderingen in de digitale wereld. Om een Europese regelgeving te creëren voor de bescherming van persoonsgegevens is een nieuwe Europese privacy-verordening aangenomen: de Algemene Verordening Gegevensbescherming (AVG). De AVG is op 25 mei 2016 in werking getreden en zal naar verwachting op 25 mei 2018 van kracht worden.

De AVG heeft een grote impact op organisaties die persoonsgegevens beheren en verwerken. De overgangsperiode tot 2018 is bedoeld om organisaties de ruimte te geven zo goed mogelijk te voldoen aan alle onderdelen van de verordening. Voor een goede voorbereiding moet Werkplein Fivelingo zorgen voor een procedure voor datalekken zodat het duidelijk is welke stappen er genomen moeten worden door de organisatie bij het vermoeden van of kennisneming van een incident dat (mogelijk) aangemerkt kan worden als een ‘datalek’.

2.3 Wet Datalekken

Het ontstaan van een ‘datalek’ heeft gevolgen voor de personen waarvan gegevens worden gelekt en Werkplein Fivelingo, wanneer zij het lek veroorzaakt. Een datalek dient gemeld te worden bij de autoriteit persoonsgegevens. Werkplein Fivelingo riskeert een boete wanneer blijkt dat er niet voldoende maatregelen getroffen zijn om het ontstaan van een datlek te voorkomen. Om een datalek te voorkomen treft Werkplein Fivelingo maatregelen. Hierbij hanteert Werkplein Fivelingo de normstelling van de Baseline Informatiebeveiliging Gemeenten (hierna BIG te noemen). In deze rapportage wordt toegelicht welke maatregelen genomen worden om te voldoen aan de BIG.

2.4 Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)

Werkplein Fivelingo heeft als uitvoerder van diverse wetten en regelingen te maken met veel registraties. Om de efficiency en de effectiviteit te verbeteren worden de laatste jaren steeds meer van die registraties gekoppeld en is samenwerking binnen verschillende ketens noodzakelijk. Ketenpartners zijn het Bureau Keteninformatisering werk en inkomen (BKWI), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de stichting Inlichtingenbureau Gemeenten (IB) en gemeenten. Zij wisselen via een elektronische infrastructuur persoonsgegevens met elkaar uit. Dit is het Suwinet.

Suwinet is tevens het netwerk waarin we de klantgegevens uitwisselen ten behoeve van het Digitaal Klant Dossier. Belangrijk aspect hierbij is de Wet eenmalige gegevensuitvraag (WEU), in werking getreden op 1 januari 2008. Bij de start van de WEU is vastgelegd dat gegevens slechts 1 keer mogen worden opgevraagd. De klantgegevens die beschikbaar zijn via Suwinet moeten dus optimaal hergebruikt worden.

Suwinet-inkijk is de applicatie die op Suwinet draait. Binnen deze applicatie worden gegevens op basis van onder andere het Burgerservicenummer (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Het gaat over privacygevoelige gegevens zoals; inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, uitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering. De organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.

Om de Suwi keten effectief te laten functioneren moeten partijen erop kunnen vertrouwen dat ‘hun’ gegevens door de partners in de Suwi-keten op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Dit betekent dat bevoegde gebruikers van Suwinet over nogal wat privacygevoelige informatie van cliënten beschikken. Daarnaast neemt het aantal bronnen waarvan Suwinet gebruik kan maken alleen maar toe. Naast de Rijksdienst voor het Wegverkeer (RDW), Sociale Verzekeringsbank (SVB), UWV en de Dienst Uitvoering Onderwijs (DUO) is ook de Belastingdienst aangesloten op Suwinet.

Als gevolg van de Regeling Suwi is elke gemeente verplicht te beschikken over een actueel informatiebeveiligingsplan. In de Wet Bescherming Persoonsgegevens (WBP) is uitgebreid geregeld hoe met persoonsgegevens moet worden omgegaan. Ook staat hierin welke beveiligingsmaatregelen er moeten worden getroffen. Er zijn dus genoeg redenen om met regelmaat het Beveiligingsplan Suwinet te actualiseren.

2.5 GeVS en BIG

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is gebaseerd op de ISO 27001, de ISO 27002 en op de Baseline Informatiebeveiliging Rijksdienst (BIR). Het normenkader Gezamenlijke elektronische Voorzieningen Suwi (GeVS) hanteert zeven normen. Deze normen zijn te vertalen naar de normen uit de BIG. Een voordeel van deze vertaling is, dat de inspanning die nodig is om deze zeven normen te implementeren, een gedeelde inspanning kan zijn. Als een gemeente bezig is met de implementatie van de BIG, bestaat immers de mogelijkheid dat de zeven normen al op enige manier binnen de gemeente uitgewerkt zijn. Beide normenkaders zijn van toepassing op (een deel van) de gemeentelijke informatievoorziening. Voor beide normenkaders zijn de eisen, die gelden voor de risicobeheersing ten aanzien van de informatiehuishouding, ontleend aan de code voor Informatiebeveiliging ISO 27002. Het doel van de normenkaders voor gemeenten is, dat gemeenten op een verantwoorde manier omgaan met de aan hen toevertrouwde (persoons)gegevens.

Voldoen aan het normenkader is een wettelijke verplichting. Onderstaand wordt de vergelijking, op basis van de zeven normen uit het Normenkader GeVS nader uitgewerkt:

1. Norm 1.3

Het informatiebeveiligingsbeleid en -plan (Suwinet) zijn formeel goedgekeurd/vastgesteld door het management en/of de directie en/of het college van burgemeester en wethouders (College B&W).

Dat betekent dat:

a) Er is een specifiek op Suwinet gericht informatiebeveiligingsbeleid of veiligheidsplan aanwezig of er is een Suwi-specifieke passage in een algemeen plan aanwezig.
b) Dit beleid, dit plan of deze passage heeft specifiek betrekking op de gemeenten van Werkplein Fivelingo.
c) De goedkeuring is formeel vastgelegd. Het beleid, het plan of de passage is ondertekend of van de goedkeuring is expliciet melding gemaakt in het verslag van de betreffende vergadering.

2. Norm 1.4

Het informatiebeveiligingsbeleid en -plan (Suwinet) wordt (op reguliere basis) door de gemeente uitgedragen binnen de organisatie.

Dat betekent dat:

a) Het informatiebeveiligingsbeleid is centraal voor alle gebruikers centraal beschikbaar (het is bijvoorbeeld aan iedereen gemaild of staat op intranet).
b) Er is het afgelopen jaar minimaal 2x een actie geweest om de gebruikers (opnieuw) te attenderen op het bestaan van het veiligheidsbeleid, -plan of -passage.
c) Bijvoorbeeld door hernieuwd te wijzen op intranet, te agenderen voor een afdelingsoverleg of te bespreken in functioneringsgesprekken. Wanneer alleen nieuwe gebruikers wordt gevraagd om een geheimhoudingsverklaring te tekenen is dat een goede actie, maar niet voldoende.

3. Norm 1.5

Het informatiebeveiligingsbeleid en -plan (Suwinet) wordt op reguliere basis (bijvoorbeeld jaarlijks) door de gemeente geëvalueerd en indien noodzakelijk geactualiseerd.

Dat betekent dat:

a) De laatste evaluatie is minder dan een jaar oud.
b) De laatste evaluatie is vastgesteld door management en/ of directie en/ of college van B&W.
c) De evaluatie is een concrete actie van alle directbetrokkenen geweest, schriftelijk vastgelegd en leidt zo nodig tot aanpassen van het informatiebeveiligingsbeleid, het veiligheidsplan of de beveiligingspassage.

4. Norm 2.2

De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van (Suwinet)-gegevens, -applicaties, -processen en infrastructuur dienen te zijn beschreven, en duidelijk en afhankelijk van de schaalomvang van de organisatie, gescheiden te zijn belegd (functiescheiding).

Bij de functiescheiding is het belangrijk dat bij verschillende personen is belegd:

a) Uitvoering van taken (het gebruik van Suwinet).

b) Het beheer van autorisaties (toegang verlenen tot Suwinet).
c) Kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet).
d) Management (beslissen over bevoegdheden van functiegroepen, en/of individuele medewerkers, uitdragen.

5. Norm 2.2

De Security Officer beheert en beheerst de beveiligingsprocedures en -maatregelen in het kader van Suwinet. Zodanig dat de beveiliging van Suwinet overeenkomstig met de wettelijke eisen is geïmplementeerd.

Dat betekent dat:
a) Er is een medewerker verantwoordelijk gemaakt om periodiek – ten minste twee keer per jaar - naar de beveiliging van Suwinet kijken.
b) Deze medewerker rapporteert en adviseert periodiek rechtstreeks aan het management en/ of de directie en/ of het college van B&W.
c) Dat is vastgelegd in zijn/ haar functieomschrijving inclusief takenoverzicht.

6. Norm 13.1

De organisatie autoriseert en registreert de toegang die gebruikers hebben tot (Suwinet)-applicaties, op basis van formele procedures.

Dat betekent dat:
a) Elke gebruiker van Suwinet moet geautoriseerd worden.
b) Er is een formeel vastgelegde autorisatieprocedure waarin functies aan autorisaties en in het verlengde daarvan aan rollen worden gekoppeld.
c) Het accountbestand wordt meerdere keren per jaar gecontroleerd en aansluitend worden inactieve accounts verwijderd.
d) Er is geen toegang verstrekt buiten de sociale dienst, de gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coördinatiefunctie bij voortijdig schoolverlaten. Voor het gebruik door gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coördinatiefunctie bij voortijdig schoolverlaten is een apart contract afgesloten. Het is op dit moment niet geoorloofd om WMO- medewerkers, medewerkers Parkeerbeheer of andere hierboven niet benoemde medewerkers toegang te verstrekken tot Suwinet.

7. Norm 13.5

De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.

Dat betekent dat:
a) Een medewerker van Werkplein Fivelingo vraagt ten minste meerdere keren per jaar bij BKWI een rapportage over het gebruik van Suwinet-inkijk op.
b) De beoordeling van deze rapportage (door wie en langs welke criteria) is centraal belegd.
c) Deze beoordelaar maakt hiervan een schriftelijk verslag.
d) Als uit dit verslag blijkt dat nadere beoordeling gewenst is, wordt vervolgens bij BKWI een specifieke rapportage opgevraagd die vervolgens wordt beoordeeld.
e) Bij geconstateerd oneigenlijk gebruik c.q. misbruik wordt er ook opgetreden c.q. gesanctioneerd.

2.6 Eenduidige Normatiek Single Information Audit (ENSIA)

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

Uitgangspunt van ENSIA is de single information audit. Dit betekent dat we maar één keer per jaar de zelfevaluatielijst hoeven in te vullen. De informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad.

Als een gemeente de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) implementeert en binnen het gemeentelijke informatiebeveiligingsbeleid en het informatiebeveiligingsplan, de verschillende normen (SUWI, BPR, BAG, reisdocumenten, DigiD) nadrukkelijk een plaats geeft, dan kan de auditlast afnemen als gevolg van het sneller kunnen doorlopen van de verschillende audits. Het kernpunt hierbij is dossiervorming en bewijsvoering.

3 Informatiebeveiligingsbeleid

3.1 Inleiding

In dit beleid is rekening gehouden met alle actuele wet- en regelgeving en richtlijnen zoals deze zijn opgelegd. De inhoud van dit informatiebeveiligingsbeleid wordt sterk bepaald door de betreffende wetten en regels.

Vanuit de VNG en KING is in 2013 de Baseline Informatiebeveiliging Nederlandse Gemeenten vastgesteld (BIG). Deze baseline biedt een basisniveau van informatiebeveiliging voor Nederlandse Gemeenten en haar afnemers en toeleveranciers. Een onderdeel van het basisniveau, en ook een wettelijke vereiste vanuit diverse wet en regelgeving, is het beschikken over een actueel informatiebeveiligingsbeleid. Werkplein heeft, als gemeenschappelijke Regeling namens Delfzijl, Appingedam en Loppersum ook te maken met deze regelgeving.

Het management heeft hierbij de bijzondere verantwoordelijkheid om te voorzien in middelen en het beleggen van de juiste taken betreffende informatiebeveiliging. De taak en verantwoordelijkheid om Werkplein Fivelingo te voorzien van de juiste maatregelen, te adviseren over informatieveiligheid en het toezicht op maatregelen is belegd bij de ‘security officer’. Het beleid is geschreven voor een periode van 3 jaar maar wordt jaarlijks geëvalueerd en daar waar nodig geactualiseerd.

3.2 Organisatie van informatiebeveiliging

1. Interne organisatie

Werkplein Fivelingo beheert en belegt de Informatiebeveiliging op de volgende manier binnen haar organisatie:

- Actieve betrokkenheid van de directie bij informatiebeveiliging, zoals het geven van goede voorbeelden en ondersteuning van de bij informatiebeveiliging betrokken functionaris(sen).
- Betrokkenheid en coördinatie vanuit alle delen van de organisatie.
- Door het toewijzen van verantwoordelijkheden en bevoegdheden voor Informatiebeveiliging door de aanstelling van een functionaris Informatiebeveiliging.
- De geheimhoudingsverklaring vormt een weerslag van de eisen voor vertrouwelijkheid binnen de organisatie en wordt door alle medewerkers (intern en extern) gekend en ondertekend.
- Contacten met overheidsinstanties op het gebied van (informatie)beveiliging zoals KING.
- Onafhankelijke toetsing en beoordeling van de Informatiebeveiliging op een regelmatige basis bevordert de kwaliteit en geeft een onafhankelijk advies voor mogelijke verbeteringen.

2. Partners en externe partijen

Partners en derde partijen kunnen toegang hebben (fysiek en/of elektronisch) tot informatie en IT–voorzieningen van Werkplein Fivelingo. Elke toegang tot de IT–voorzieningen en het verwerken en communiceren van informatie door externe partijen wordt beheerst. Ook voorkomt Werkplein Fivelingo dat medewerkers van derde partijen onbevoegde inzage hebben in gegevens. Communicatie

en afstemming van het informatiebeveiligingsbeleid met GemCC en andere partijen zijn belangrijke onderdelen van het beleid.

3.3 Beheer van bedrijfsmiddelen

Werkplein Fivelingo maakt gebruik van middelen bij de uitvoering van haar bedrijfsprocessen. Onder bedrijfsmiddelen verstaat men in de breedste zin alle middelen die daarvoor worden gebruikt. Betreffende IT–voorzieningen vallen daaronder niet alleen apparatuur, maar ook applicaties, bijbehorende licenties en de informatie. Van een deel van de bedrijfsmiddelen is Werkplein Fivelingo 'afnemer' van middelen beschikbaar gesteld door GemCC. Alle bedrijfsmiddelen zijn door Werkplein Fivelingo adequaat vastgelegd.

3.4 Beveiliging van personeel

Werkplein Fivelingo gaat op juiste en verantwoorde manier om met personeel, zowel werknemers, ingehuurd personeel, betrokken medewerkers van partners als externe gebruikers. Vanwege de gevoelige informatie waarmee Werkplein Fivelingo omgaat, is veiligheid daarvan een belangrijk onderdeel. Deze verantwoordelijkheid beperkt zich niet tot de periode van het dienstverband, maar ook voorafgaand, bij veranderingen en de beëindiging.

Onderstaand de **kernpunten** van de verschillende stadia:

1. Voorafgaand aan het dienstverband:

- Vastleggen van rollen en verantwoordelijkheden van personeel ten aanzien van veiligheid en informatiebeveiliging, dit duidelijk communiceren.
- Vastleggen van verplichtingen in de arbeidsovereenkomst.
- Vaststellen en vastleggen welke sancties mogelijk zijn.
- Laten ondertekenen dat personeel bovenstaande informatie heeft gelezen.
- Nagaan van personalia, antecedenten en cv's, door screening in die mate als vereist voor de beoogde functie.

2. Tijdens het dienstverband:

- Verbeteren van bewustzijn aangaande informatiebeveiliging en het beleid bij personeel.
- Participeren door directie en management door het stellen van eisen en het geven van goede voorbeelden.
- Geven van training en voorlichting over Informatiebeveiliging en het beleid.
- Navolgen van sancties en disciplinaire maatregelen, afhankelijk van gesteld beleid en inbreuk door personeel.

3. Wijziging en beëindiging van het dienstverband:

- Vastleggen van procedures en beleggen in de organisatie, zodat bij wijziging of beëindiging van het dienstverband dit ordelijk kan verlopen.
- Beëindigen van verantwoordelijkheden, zorg dragen voor juiste overdracht.
- Innemen en retourneren van bedrijfsmiddelen (registratie is noodzakelijk).
- Blokkeren van toegangsrechten, Werkplein Fivelingo geeft dit door aan GemCC; bij ontslag op staande voet worden toegangsrechten direct geblokkeerd.

3.5 Fysieke beveiliging en beveiliging van de omgeving

Werkplein Fivelingo beschermt haar medewerkers, partners en bedrijfsmiddelen op de volgende wijze:

1. Beveiligde ruimten

Door het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het gebouw en de informatie van de organisatie:

- Fysieke beveiliging van het gebouw en de ruimten, specifiek daar waar zich informatie en IT–voorzieningen bevinden.
- Bescherming door toepassing van geschikte toegangsbeveiliging voor kantoren, ruimten en faciliteiten; toegang alleen voor geautoriseerd personeel, inhoudend zowel eigen medewerkers, die van partners als ingehuurd personeel.
- Bescherming van bedreigingen van buiten, zoals schade door brand, overstroming, explosies, aanslagen en andere calamiteiten.
- Werkplein Fivelingo geeft speciale aandacht aan de fysieke bescherming en richtlijnen voor werken in speciale ruimten, zoals spreekkamers; te denken valt aan mogelijk agressief gedrag van cliënten.

2. Beveiliging van apparatuur

Door het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en daardoor onderbreking van de bedrijfsactiviteiten. Apparatuur is beschermd tegen fysieke bedreigingen en gevaren van buitenaf. Werkplein Fivelingo is hierbij voor een belangrijk deel afhankelijk van Gemeente Delfzijl en GemCC, samen met deze dienstverleners bereikt ze dit door onderstaande punten:

- Daar waar mogelijk wordt apparatuur zodanig geplaatst en beschermd dat risico's worden verminderd.
- Er is speciale aandacht voor apparatuur buiten het gebouw van Werkplein Fivelingo, zoals laptop, PDA's, USB–sticks en dergelijke.
- Zonder toestemming vooraf, mag men geen apparatuur, informatie en programmatuur van Werkplein Fivelingo van de locatie meenemen.

3.6 Beheer van communicatie– en bedieningsprocessen

Binnen de bedrijfsprocessen zijn de informatiesystemen voor Werkplein Fivelingo van essentieel belang. Een juist en adequaat beheer van dit onderdeel van de processen is van groot belang. Daar waar mogelijk neemt zij haar verantwoordelijkheid op de volgende wijze:

1. Bedieningsprocedures en verantwoordelijkheden

Door het waarborgen van een correcte en veilige bediening van IT–voorzieningen om zodoende het risico van nalatigheid of opzettelijk misbruik van het systeem te verminderen.

Kernpunt:

- Het scheiden van taken en verantwoordelijkheidsgebieden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen in de organisatie te verminderen.

2. Beheer van de dienstverlening door een derde partij

De dienstverlening door een derde partij dient in lijn te zijn met het informatiebeveiligingsbeleid van Werkplein Fivelingo en wordt verwoord en in een overeenkomst voor dienstverlening met die derde partij.

Kernpunten:

- Beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij, worden geïmplementeerd, uitgevoerd en bijgehouden door die derde partij; dit inclusief geheimhoudingsverklaring.
- De diensten, rapporten en registraties die door de derde partij worden geleverd, worden regelmatig gecontroleerd.
- Toegang (fysiek en elektronisch) van medewerkers van derde partijen is tijdelijk en op afspraak, met alleen benodigde autorisaties.

3. Bescherming tegen virussen en “mobile code”

Voor de realisatie en toepassing van “anti–malware” is Werkplein Fivelingo afhankelijk van GemCC. Indien apparatuur in eigen beheer is, bijvoorbeeld laptops, ligt hiervoor de verantwoordelijkheid bij Werkplein Fivelingo.

4. Back–up

Voor Werkplein Fivelingo is de handhaving van de integriteit en beschikbaarheid van informatie en IT–voorzieningen van essentieel belang. Het maken van back–ups van gegevens is hierbij belangrijk om tijdig herstel bij verstoringen en calamiteiten te realiseren. Werkplein Fivelingo heeft de uitvoering hiervan bij GemCC belegd.

5. Beheer van netwerkbeveiliging

De bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur is belegd bij GemCC en Suwinet. Vanwege het belang voor de bedrijfsprocessen controleert Werkplein Fivelingo regelmatig of de juiste maatregelen zijn genomen voor veiligheid en beveiliging.

6. Behandeling van media

Media als gegevensdragers zijn fysiek beschermd om onbevoegde openbaarmaking, modificatie, verwijdering en vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten te voorkomen.

7. Uitwisseling van informatie

Veel van de gegevens, waarmee Werkplein Fivelingo werkt en die zij beheert, betreffen gevoelige informatie. Verantwoorde en veilige uitwisseling is daarom van groot belang. Voor wat betreft de uitwisseling via Suwinet zijn getroffen maatregelen onderhevig aan wet– en regelgeving. Andere uitwisseling zijn in lijn met normen, wet– en regelgeving.

8. Diensten voor e–commerce

Te denken valt aan aspecten van het “Digitale Klanten Dossier” (DKD) en toekomstige inzage van burgers in persoonsgegevens van de overheid. Werkplein Fivelingo stelt zich ten doel deze aspecten

en ontwikkelingen te volgen, indien nodig het beleid aan te scherpen en adequate maatregelen te nemen. Dit om frauduleuze activiteiten, onbevoegde toegang, onbevoegde openbaarmaking en onterechte modificatie van door haar beheerde informatie te voorkomen.

9. Controle

Om met redelijke zekerheid mogelijk inbreuken op informatiebeveiliging te kennen controleert Werkplein Fivelingo het volgende.

- Dat alleen geautoriseerd personeel gebruik kan maken van de IT–voorzieningen.
- Welke verwerkingsactiviteiten en gebeurtenissen er op het gebied van informatiebeveiliging, bijvoorbeeld in audit–logbestanden plaatsvindt.
- Of de juiste bescherming van bovengenoemde bestanden bewerkstelligd wordt in overleg en samenwerking met GemCC.

3.7 Toegangsbeveiliging

Werkplein Fivelingo onderkent dat de mens bij toegangsbeveiliging een zwakke schakel in de keten is.

1. Bedrijfseisen ten aanzien van toegangsbeheersing

Als beleid stelt Werkplein Fivelingo dat alleen die medewerkers toegang tot bepaalde informatie hebben als dit voor hun functie en rol noodzakelijk is. Dit geldt ook voor direct betrokken ingehuurde derden zoals b.v. ZZP'ers.

2. Beheer van toegangsrechten van gebruikers

Werkplein Fivelingo wil onbevoegde toegang tot informatiesystemen voorkomen door alleen bevoegde gebruikers toegang te verlenen. Vastlegging en beheer van toegangsrechten van gebruikers tot informatie, regelmatige controle en verificatie is essentieel. Kernpunten:

- Registreren van bevoegde gebruikers met functie en rol en de daarbij behorende reguliere toegangsrechten.
- Vaststellen, documenteren en handhaven van formele procedures voor registreren en afmelden van gebruikers, en voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten.
- Speciale bevoegdheden zijn tot een minimum te beperkt, bovendien mogen deze alleen van tijdelijke aard zijn en (indien mogelijk) automatisch komen te vervallen.
- Toewijzing van wachtwoorden gebeurt gecontroleerd, alleen tijdelijke wachtwoorden kunnen worden verstrekt, de gebruiker dient zelf het uiteindelijke wachtwoord te bepalen en in te geven. Dit is ook verwoord in de “10 gouden regels” (zie bijlage 1).
- De toegangsrechten van gebruikers worden regelmatig beoordeeld in een formeel proces.

3. Verantwoordelijkheden van gebruikers

Gebruikers van de informatiesystemen bij Werkplein Fivelingo werken mee aan een doeltreffende beveiliging, om daarmee onbevoegde toegang door gebruikers, en beschadiging of diefstal van informatie en IT–voorzieningen te voorkomen.

Gebruikers worden op de hoogte gebracht van hun verantwoordelijkheid voor het handhaven van doeltreffende toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur. Dit is verwoord in de “10 gouden regels”.

Kernpunten:

- Gebruikers nemen goede beveiligingsgewoontes in acht bij het kiezen en gebruiken van wachtwoorden.
- Gebruikers bewerkstelligen dat onbeheerde apparatuur passend is beschermd om onbevoegde inzage van gegevens te voorkomen.
- Waar mogelijk streeft Werkplein Fivelingo een “clear desk”–beleid voor papier en verwijderbare opslagmedia na en een “clear screen”–beleid voor IT–voorzieningen.

4. Toegangsbeheersing voor netwerken

Evenals inzage van informatie voorkomt Werkplein Fivelingo de onbevoegde toegang tot netwerkdiensten waarvan ze gebruik maakt, zowel intern als extern. Voor Werkplein Fivelingo heeft dat in het bijzonder betrekking op Internet en Suwinet. Kernpunten:

- Gebruikers hebben alleen toegang tot diensten waarvoor ze specifiek bevoegd zijn; dit geldt met name voor toegang tot Suwinet en daaraan gerelateerde onderzoeksystemen.
- Bescherming van netwerkpoorten is afdoende.

5. Toegangsbeveiliging voor besturingssystemen

De primaire toegangsbeveiliging bij Werkplein Fivelingo vindt plaats vanuit het besturingssysteem of direct daaraan gelieerde programmatuur. Beheer hiervan berust bij GemCC. Het huidige systeem gaat uit van een gebruikersnaam en een wachtwoord.

6. Draagbare computers en telewerken

Draagbare computers (notebooks, laptops, PDA’s en smartphones) en computers die medewerkers gebruiken voor thuiswerken vormen speciale risicogroepen. Draagbare computers zijn gevoelig voor diefstal, in die situaties mag informatie binnen redelijke termen niet raadpleegbaar zijn.

Kernpunten:

- Opgeslagen informatie, ook van tijdelijke aard, is niet leesbaar voor onbevoegden; toepassing van encryptie is een vereiste.
- Waar mogelijk en reëel is adequate anti–malware te worden toegepast en regelmatig vernieuwd.
- Werkplein Fivelingo controleert of beveiliging van computers door telewerkers voldoende is; en gaat na of technische maatregelen gewenst en mogelijk zijn.
- Werkplein Fivelingo maakt afspraken met medewerkers over het uitwisselen van persoonsgegevens via draagbare gegevensverwerkers met betrokken cliënten.

3.8 Verwerving, ontwikkeling en onderhoud van informatiesystemen

GemCC voert het technische beheer uit voor Werkplein Fivelingo, daar berust voor een belangrijk deel de uitvoering van verwerving en onderhoud van informatiesystemen. Werkplein Fivelingo ontwikkelt zelf geen informatiesystemen, behalve toepassing van bepaalde hulpmiddelen ter ondersteuning van bedrijfsprocessen.

1. Beveiligingseisen voor informatiesystemen

Beveiliging maakt integraal deel uit van informatiesystemen. Werkplein Fivelingo oefent in dit kader alleen invloed uit bij de keuze van haar informatiesystemen en bij uitbreiding daarvan.

2. Correcte verwerking in toepassingen

Zowel de invoer, verwerking, uitvoer als het berichtenverkeer zijn voldoende gewaarborgd om de juistheid, volledigheid en integriteit van de gegevens voldoende te waarborgen. Hiermee fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen voorkomen.

- Valideren van invoergegevens voor informatiesystemen om zeker te stellen dat ze juist, geschikt en compleet zijn.
- De verwerking van gegevens bevat voldoende waarborgen en controles om corrumperen door fouten of opzettelijke handelingen te ontdekken, indien mogelijk te voorkomen.

3. Beveiliging bij ontwikkelings– en ondersteuningsprocessen

Processen voor ontwikkeling en ondersteuning zijn voldoende beveiligd. Werkplein Fivelingo werkt samen met GemCC om de beveiliging van toepassingsprogrammatuur en –informatie te handhaven.

3.9 Beheer van informatiebeveiligingsincidenten

1. Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Zwakheden aangaande informatiebeveiliging worden gemeld zodat dit kenbaar is en men daarop adequate maatregelen kan treffen.

Kernpunten:

- Rapportage van gebeurtenissen over informatiebeveiliging:
- Alle medewerkers van en bij Werkplein Fivelingo melden zwakke plekken in de beveiliging in informatiesystemen en diensten aan de Security officer.
- De Security officer rapporteert aan de directie van Werkplein Fivelingo.

2. Beheer van informatiebeveiligingsincidenten en –verbeteringen

Naast de melding is een adequate registratie en beheer nodig van incidenten aangaande informatiebeveiliging. Hierbij draagt Werkplein Fivelingo een (gedeelde) verantwoordelijkheid. Verzamelde bewijzen dienen aan bepaalde voorwaarden te voldoen en stellen ook eisen aan de betrokken functionarissen, sterke betrokkenheid van Justitie en Politie is dan ook essentieel.
Kernpunten:

- Adequate reactie op incidenten afhankelijk van het type incident.
- Evaluatie van maatregelen en procedures om lering te trekken van informatiebeveiligingsincidenten zodat continue verbetering kan worden gerealiseerd.
- Werkplein Fivelingo dient mogelijk bewijzen overleggen. Het verzamelen van bewijslast is dan ook van groot belang; de betrokkenheid van justitiële en opsporingsambtenaren is sterk gewenst.

3.10 Bedrijfscontinuïteitsbeheer

Ernstige storingen en calamiteiten kunnen de bedrijfsprocessen ernstig stagneren. GemCC heeft een kader (raamwerk) opgesteld voor Bedrijfscontinuïteit van het gebied wat zij beheert. Werkplein Fivelingo haakt daarop in en neemt zo haar verantwoordelijkheid op dit gebied.

1. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

De gevolgen van ernstige storingen en calamiteiten kunnen voor Werkplein Fivelingo leiden tot uitval van kritische bedrijfsprocessen en verlies van informatie. Ook kunnen bij calamiteiten gegevens openbaar komen. Werkplein Fivelingo gaat onderbreking van bedrijfsactiviteiten tegen en beschermt kritische bedrijfsprocessen tegen gevolgen van dergelijke storingen en calamiteiten.

Kernpunten:

- Mogelijke risico's van de bedrijfscontinuïteit zijn bekend, ingeschat en beoordeeld, inclusief de gevolgen voor de informatiebeveiliging.

3.11 Naleving

1. Naleving van de wettelijke voorschriften

Als onderdeel van de overheid is schending van enige wetgeving, wettelijke of contractuele verplichtingen niet toelaatbaar. Wat betreft de Archiefwet heeft Werkplein Fivelingo dit belegd bij Gemeente Delfzijl, en controleert regelmatig op de juiste naleving ervan.

Kernpunten:

- Identificeren van toepasbare wetgeving, zoals:
  - WBP – Wet Bescherming Persoonsgegevens.
  - SUWI – Wet Structuur Uitvoeringsorganisatie Werk en Inkomen, met richtlijnen van BKWI.
  - Archiefwet, aangevuld met richtlijnen over bewaarperiodes.
  - Wet Computercriminaliteit.
- Nagaan welke (types) bedrijfsdocumenten buiten klanten– en persoonsgegevens bescherming nodig hebben.
- Bescherming en geheimhouding van persoonsgegevens vormt een belangrijk aspect binnen de bedrijfsprocessen van Werkplein Fivelingo.
- Voorkomen van misbruik van IT–voorzieningen door vaststellen van procedures, regels en richtlijnen, kenbaar maken en handhaven.

2. Naleving van beveiligingsbeleid en –normen en technische naleving

De naleving van beleid, maatregelen, regels en richtlijnen door medewerkers worden gecontroleerd, beoordeeld en gewaarborgd door:

- De naleving van het beveiligingsbeleid en de –normen (dit beleid dus).
- Het controleren van de informatiesystemen op technische naleving van beleid en normen.
- Werkplein Fivelingo wil door audits de doeltreffendheid van het informatiesysteem maximaliseren en verstoring als gevolg van audits minimaliseren. In principe laat Werkplein Fivelingo audits uitvoeren door een ander (of andere partij) dan de uitvoerende personen of organisatie.

4 Beveiligingsplan Suwinet

4.1 Inleiding

Het Bureau Keteninformatisering werk en inkomen (BKWI), het Werkbedrijf, de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Belastingdienst, de Informatie Beheer Groep (IBG), de RDW (Rijksdienst voor het wegverkeer) en gemeenten wisselen persoonsgegevens met elkaar uit via Suwinet, een elektronische infrastructuur.

Met de faciliteit Suwinet-Inkijk worden gegevens op basis van Burger Service Nummers (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Het gaat om privacygevoelige gegevens over arbeidsverleden, loon, uitkeringen en opleiding van burgers. De organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.

Dit betekent dat bevoegde gebruikers van Suwinet over nogal wat privacygevoelige informatie van cliënten kunnen beschikken. Daarnaast is de verwachting dat het aantal bronnen waarvan Suwinet gebruik kan maken (gevoed door het Inlichtingenbureau) in de toekomst alleen maar zal toenemen (bijvoorbeeld kentekenregistraties, koppeling huursubsidie etc.).

Om de Suwi-keten effectief te laten functioneren moeten partijen er op kunnen vertrouwen dat "hun" gegevens door de partners in de Suwi-keten op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is.

Gemeenten dienen zich te verantwoorden over het feit of de gemeente voldoet aan de beveiligingseisen die als Suwinet partij aan de gemeente worden gesteld en of er een beveiligingsplan is. Ook in de Wet Bescherming Persoonsgegevens (WBP) is uitgebreid geregeld hoe met persoonsgegevens moet worden omgegaan; voor welke doeleinden ze mogen worden verzameld, op welke wijze ze mogen worden verwerkt en welke beveiligingsmaatregelen moeten worden getroffen.

Dit Beveiligingsplan is een dynamisch document; het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisatie en de omgeving van Werkplein Fivelingo zijn voortdurende in ontwikkeling, onder andere door wijzigende of vernieuwende inzichten en wetgeving of aanpassingen in de informatiesystemen. Dit betekent dat dit plan periodiek moet worden beoordeeld op actualiteit en dus mogelijk constante aanpassing behoeft.

Het niet voldoen aan de normen uit het Suwi-normenkader kan leiden tot tijdelijke afsluiting van Suwinet. Hiertoe heeft de staatssecretaris van Sociale Zaken en Werkgelegenheid in 2015 een afsluitprotocol vastgesteld. Afsluiting van Suwinet betekent dat we meer informatie bij de cliënt op moeten vragen, dit leidt aan beide zijden tot administratieve lastenverzwaring en langere behandeltijden van bijstandsaanvragen. Afsluitingen worden in de Staatscourant gepubliceerd, dit kan leiden tot imagoschade.

4.2 Gebruik Suwinet

1. Wie mag Suwinet gebruiken?

De volgende geautoriseerde medewerkers van Werkplein Fivelingo die belast zijn met de uitvoering van de wettelijke taken die vallen onder de P-wet, IOAW en IOAZ mogen gebruik maken van Suwinet-inkijk:

- Functioneel beheer verzorgt autorisatie voor Suwinet;
- Medewerker interne controle/ security officer vraagt logging gegevens op;
- Klantmanagers Werk en Inkomen mogen raadplegen;
- Administratief medewerkers mogen opvragen/ raadplegen voor een globale check op het recht op een uitkering;
- Juridisch kwaliteitsmedewerkers mogen raadplegen;
- Sociale recherche;
- RMC's (Regionale Meld- en Coördinatiepunten) voor hulp aan voortijdig schoolverlaters.

Dit geldt tevens voor ingehuurde externe capaciteit, bijvoorbeeld een medewerker die wordt ingehuurd via een uitzendbureau. De medewerker werkt dan op het kantoor en onder gezag en toezicht van de desbetreffende gemeente.

2. Wie mag Suwinet niet gebruiken?

Suwinet mag bij uitbesteding van taken niet worden gebruikt door medewerkers van de partij waaraan is uitbesteed.

- Personen onder gezag van een commerciële dienstverlener mogen niet geautoriseerd worden. Let op: uitbesteden en toegang tot Suwinet gaan niet samen.
- Gemeentelijke medewerkers die andere taken uitvoeren dan de P-wet of IOAW en IOAZ en niet behoren tot één van de hierboven genoemde niet Suwi-partijen.

3. Waar mag ik Suwinet voor gebruiken?

Een gemeente heeft gegevens nodig van andere partijen voor de uitvoering van de Participatiewet, IOAW of IOAZ. Daarmee ontstaat een wettelijke grondslag tot het raadplegen van gegevens (art. 64 P-wet, 44/45 IOAW/ IOAZ). Partijen wisselen deze gegevens met elkaar uit via Suwinet (art. 62 Wet SUWI).

Daarnaast zijn er in de Wet bescherming persoonsgegevens (Wbp) algemene regels over de verwerking van persoonsgegevens. Een belangrijke regel is dat gebruik van persoonsgegevens beperkt moet blijven tot de relevante gegevens (art. 11 Wbp).

Bij de beoordeling of Suwinet gebruikt mag worden staan 3 vragen centraal:

1. Valt deze taak onder de uitvoering van de P-wet/IOAW/IOAZ?
2. Zo ja, staat deze taak/beoordeling expliciet beschreven in P-wet/IOAW/IOAZ?
3. Zo ja, zijn de gewenste gegevens noodzakelijk voor de uitvoering van de uit te voeren taak uit de P-wet/ IOAW/IOAZ?

Als het antwoord op alle vragen 'ja', is raadpleging van Suwinet toegestaan. Dit geldt voor taken als (niet uitputtend):

- Vaststellen van de rechtmatigheid van de uitkering (art.17 lid 1 PW en art.53a lid 1 en 6 PW, art.14 IOAW/IOAZ)

- Vaststellen definitieve einddatum van de uitkering na opschorting (art.17 lid 1 PW en art.53a lid 1 en 6 PW, art.14 IOAW/IOAZ)
- Re-integratie werkzaamheden, ook voor ex-gedetineerden mits het de doelgroep van de P-wet betreft (art. 7 lid 1 PW)
- Bijzondere bijstand (art. 35, 36, 36b PW)
- Taken rondom Bbz, Besluit bijstandsverlening zelfstandigen (art. 78f, 78g PW)
- Terugvordering en Verhaal, bijv. het raadplegen van de ex-partner voor vaststelling onderhoudsplicht (art. 58-62i P-wet, art. 25-33 IOAW/IOAZ)

Soms wordt er op basis van de derde vraag een beperking aangegeven.

Voor het vaststellen van kostendeling (art. 22a) mag van de medebewoners (niet zijnde de partner van de klant of inwonende kinderen onder 18 jaar) alleen de pagina kostendelerstoets worden geraadpleegd. Het is niet toegestaan om van de medebewoner andere gegevens te raadplegen zoals uitkerings- of inkomensgegevens.

Voor de Wet Inburgering mag het Inburgeringsportaal via Suwinet gebruikt worden. De overige pagina's van Suwinet mogen voor pure inburgeringstaken niet gebruikt worden tenzij het een duaal traject betreft (inburgeraar volgt tevens re-integratie).

4. Waar mag ik Suwinet niet voor gebruiken?

Suwinet mag niet gebruikt worden:

- Voor de uitvoering van gemeentelijke regelingen zoals de stadspas of onderdelen van armoedebeleid. Gemeentelijke regelingen mogen alleen in Suwinet worden geraadpleegd als deze regeling is gebaseerd op de P-wet, IOAW of IOAZ (art. 8, 8a, 8b P-wet). Of dit zo is, is zichtbaar in de aanhef van de gemeentelijke regeling: Gelet op artikel xx van de XXX-wet...
- Voor de interne controle op juistheid van de beslissingen van de medewerker. Het controleren van de juistheid van de beslissing van een medewerker valt niet onder de uitvoering van de P-wet, IOAW of IOAZ, maar onder interne controle. Daarvoor mag Suwinet niet worden geraadpleegd.
- Voor de controle op de naleving van Social Return. Gemeenten nemen in contracten met leveranciers/dienst- verleners passages op over het inzetten van werkzoekenden of bijstandsgerechtigden (Social Return). Het controleren of de leverancier/dienstverlener hieraan voldoet, valt niet onder de P-wet, IOAW of IOAZ.

Daarom mag Suwinet hiervoor niet worden geraadpleegd:

- Voor onderzoek naar de effectiviteit van de uitvoering van wetten.
- Voor de uitvoering van andere wetten zoals WMO, wet op de lijkbezorging, (bestaande) WSW, wet gemeentelijke schuldhulpverlening etc.
- De Wet gemeentelijke schuldhulpverlening is een Suwi taak. Het is echter nog niet mogelijk om Suwinet voor dit doel te raadplegen omdat een AMvB op grond van de Wet gemeentelijke schuldhulpverlening ontbreekt.
- Voor de uitvoering van gemeentelijke incasso. Alleen voor de gemeentelijke belastingdeurwaarders geldt dat zij een overeenkomst hebben op grond van art. 5.23 van het Besluit Suwi en conform het Aansluitprotocol (Bijlage III Regeling Suwi). Daarmee hebben zij een eigen aansluiting op Suwinet.

Tenslotte, de verzamelde gegevens die via Suwinet zijn ingenomen en daarmee aan Werkplein Fivelingo zijn overgedragen, mogen niet worden hergebruikt of doorgeleverd voor andere doelen dan

waarvoor de gegevens oorspronkelijk verzameld zijn. Dit is bepaald in de geheimhoudingsplicht van artikel 74 van de wet Suwi.

5. 'Whitelist'

Voor het gebruik van Suwinet-Inkijk dienen medewerkers te zijn geautoriseerd. Daarmee is de toegang tot gegevens beperkt tot personen die uitvoering geven aan bovengenoemde wettelijke taken. Nadat deze toegang is verleend, kunnen geautoriseerde medewerkers in principe gegevens opvragen van iedere in Nederland woonachtige burger. Dat betreft dan ook burgers waar geen dienstverleningsrelatie mee is op basis van de gemeentelijke wettelijke taken. De gegevensraadpleging is dus niet begrensd tot de 'eigen' burgers. Dit is onwenselijk omdat dit kan leiden tot het raadplegen van gegevens van burgers waar geen dienstverleningsrelatie mee is.

Om dit tegen te gaan en om het raadplegen van gegevens te begrenzen tot die 'eigen' burgers, is het mogelijk om binnen Suwinet-Inkijk gebruik te maken van een filtermechanisme. Dit filtermechanisme is vormgegeven als een zogenaamde '*White list*'. Een whitelist is een lijst die de BSN's bevat van alleen die burgers waar de gemeente/organisatie een dienstverleningsrelatie mee heeft of mee heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde 'escapefunctie'. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van burgers.

Werkplein Fivelingo krijgt maandelijks een overzicht van bevragingen van BSN's die niet op de whitelist staan.

Enkele bronhouders gaan het gebruik van een whitelist door de gemeente als voorwaarde stellen aan de gegevenslevering. De Belastingdienst gaat waarschijnlijk vanaf het tweede kwartaal van 2017 alleen nog gegevens beschikbaar stellen aan een gemeente als die gebruik maakt van whitelisting. Dat betekent dat gemeenten die hier niet aan voldoen die betreffende gegevens niet meer geleverd krijgen. Voor de Belastingdienst gaat het om gegevens over vermogen, toeslagen en heffingskortingen.

6. Suwinet-Mail

Vanwege de regels rondom privacy en beveiliging is het in het algemeen niet toegestaan om informatie over cliënten per e-mail uit te wisselen met andere instanties. Suwinet-Mail is in het leven geroepen om dit op een veilige manier alsnog te kunnen. Het zorgt er namelijk voor dat u kunt garanderen dat uw mailbericht niet over openbare netwerken reist, maar via het besloten netwerk van Suwinet zijn bestemming bereikt.

Suwinet-Mail mag gebruikt worden door medewerkers van organisaties op het gebied van Werk en Inkomen voor het onderling uitwisselen van e-mail met potentieel gevoelige informatie over burgers en andere vertrouwelijke informatie voor de uitvoering van wettelijke taken.

4.3 Verdeling verantwoordelijkheden medewerkers Werkplein Fivelingo

1. Algemeen

Er zijn verschillende functies waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van cliëntgegevens/informatie. In het onderstaand overzicht volgt per functie in welke gevallen Suwinet-

inkijk gebruikt mag worden. De directeur van Werkplein Fivelingo is overigens eindverantwoordelijke voor het gebruik en de beveiliging van Suwinet Inkijk.

2. Functies en afspraken over gebruik Suwinet-Inkijk

Er zijn verschillende functies waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van cliëntgegevens/informatie. In het onderstaand overzicht volgt per functie in welke gevallen Suwinet-inkijk gebruikt mag worden. We spreken in die gevallen van geoorloofd gebruik. Wordt Suwinet om andere redenen gebruikt dan zoals hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik.

De volgende functies binnen Werkplein Fivelingo zijn geautoriseerd om gebruik te maken van Suwinet-Inkijk:

- Applicatiebeheerder
- Klantmanager inkomen
- Klantmanager werk
- Sociale recherche
- Uitkeringsadministratie

In het onderstaand overzicht volgen per functie de rechten met betrekking tot het gebruik van Suwinet-Inkijk en de verantwoordelijkheidsverdeling.

Functie	Afspraken over gebruik Suwinet-Inkijk
Werk en Inkomen	
Medewerker uitkeringsadministratie	- Afhandeling van de maandelijkse signalen Inlichtingen Bureau (IB) - Controle van opgave van inkomsten bij uitkeringsverwerking - Controle van de ingevulde gegevens op het wijzigingsformulier. - Beheer van het debiteurenbestand - Overige beoordelingen om het werk goed uit te kunnen voeren. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in een rapportage
Inkomensconsulent, werkconsulent, uitkeringsadministratie en Juridisch medewerker	- Aanvragen PW, IOAW, IOAZ, Bijzondere Bijstand en Bbz-uitkering - Heronderzoeken (zowel rechtmatigheids- als doelmatigheidsonderzoeken) - Debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen en/of werkgever - Overige beoordelingen die via een mutatieformulier binnenkomen. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage
Applicatiebeheerder	- Beheren van het toepassingsbereik (tot welk niveau kan de autorisatie verleend worden) van de Suwinet webapplicatie - Verlenen van aanmeldaccounts volgens de richtlijnen en verwijderd de accounts bij vervallen van de functie - Melden beveiligingsincidenten - Verzorgt de maandelijkse upload van data aan het systeem (gemeente als dataleverancier) - Ondersteuning bij gebruikersvragen.
Security-officer	- Rapporteert aan het managementteam over de log-ins - Rapporteert aan het managementteam over het gebruik. - Attendeert de medewerkers op zorgvuldig gebruik Suwinet. - Vraagt detail rapportages op, indien er vermoeden bestaat van onrechtmatig gebruik.

3. Verantwoordelijkheden

Voor Suwinet hebben de volgende functies de volgende verantwoordelijkheden:

Suwinet-gebruikers:	Zorgvuldig gebruik voor het uitvoeren van wettelijke taken
Applicatiebeheerder:	Beheer van autorisaties
Security officer:	Kwaliteitszorg en borging van rechtmatig gebruik
Management:	Optreden bij oneigenlijk gebruik of misbruik van Suwinet
	Uitdragen van zorgvuldig gebruik

4. Autorisatie

Bij het autoriseren van toegang tot Suwinet gelden de volgende uitgangspunten:

1. De toegang wordt verleend op basis van de functie waarin de medewerker is benoemd. Naast de standaardautorisatie op basis van de autorisatiematrix (zie bijlage 2) worden geen autorisaties voor andere functionaliteiten verleend.
2. Bij functiewijziging of vertrek wordt de autorisatie direct aangepast. De teamleider is verantwoordelijk voor een tijdige aanpassing.
3. Suwinet-accounts zijn persoonsgebonden. Inloggegevens worden niet aan andere personen ter beschikking gesteld. Er bestaan geen groepsaccounts.
4. Applicatiebeheerders hebben een beheeraccount. Zij hebben geen toegang tot persoonsgegevens.
5. De Security officer heeft eveneens geen toegang tot persoonsgegevens. Hij/ zij beschikt alleen over een autorisatie voor het opvragen van specifieke rapportages ten behoeve van kwaliteitscontrole.

5. Autorisatieprocedure

1. De teamleider dient bij de Security officer een autorisatieverzoek in. In dit verzoek vermeldt de teamleider de naam, functie, begindatum en indien van toepassing de einddatum van de periode waarvoor de autorisatie gevraagd wordt. Bij het verzoek moet een door de betreffende medewerker ondertekende Verklaring rechtmatig gebruik Suwinet gevoegd zijn als de betreffendemedewerker geen ambtseed of gelofte heeft afgelegd.
2. De Security officer beoordeelt het verzoek. Op basis van de functie wordt op basis van de autorisatiematrix (zie bijlage 2) een gebruiksrol toegekend.
3. De Security officer geeft de applicatiebeheerder opdracht het toegewezen account aan te maken. In geval van een einddatum wordt de einddatum in het gebruikersbeheer ingevoerd.
4. De applicatiebeheerder verstrekt per Suwi-mail de inloggegevens aan de medewerker.

6. Controle op autorisaties

Ten minste eenmaal per kalenderjaar controleert de Security officer zichtbaar of de personen die toegang hebben tot Suwinet:

1. (nog) werkzaam zijn binnen Werkplein Fivelingo;
2. een functie hebben waarvoor toegang tot Suwinet kan worden verleend;
3. daadwerkelijk gebruik maken van Suwinet. Als blijkt dat een persoon Suwinet langere tijd niet hebben gebruikt waar dit gezien de functie wel verwacht mag worden, dan gaat de CISO bij de teamleider na wat daarvan de reden(en) zijn. Dit kan duiden op gebruik van Suwinet op de autorisatie van een andere medewerker.

7. Kwaliteitsmedewerker

De kwaliteitsmedewerker controleert driemaandelijkse de logginggegevens van BKWI, op basis van specifieke rapportages en rapporteert hierover aan de Security officer.

Doel: controleren of het gebruik van de gegevens binnen Suwinet-Inkijk plaatsvindt binnen de wettelijke kaders en overeenkomstig de doelen die de organisatie hiertoe heeft geformuleerd.

- Jaarlijkse controle op actualiteit Beveiligingsplan controleren op actualiteit en volledigheid.
- Verantwoording afleggen over beveiliging. In het jaarlijkse document “verslag over de uitvoering” rapporteren over het beveiligingsplan

8. Applicatiebeheerder

- Gebruikers Suwinet-inkijk (functie raadplegen) autoriseren voor toegang;
- Operationeel houden van de applicatie.

Het doel is te borgen dat het gebruik van de gegevens binnen Suwinet-Inkijk plaatsvindt binnen de wettelijke kaders en overeenkomstig de doelen die de organisatie hiertoe heeft geformuleerd.

9. Procedure bij functiewijziging of einde dienstverband/opdracht

1. De teamleider is verantwoordelijk voor het doorgeven van de wijziging of het einde van het dienstverband aan de Security officer op een zodanig tijdstip dat oneigenlijk gebruik van Suwinet niet mogelijk is.
2. De Security officer geeft de applicatiebeheerder opdracht het gebruikersaccount aan te passen aan de gewijzigde functie, dan wel het gebruikersaccount in te trekken.

4.4 Logging rapportages

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft rapportages ontwikkeld over het gebruik van Suwinet-Inkijk en logt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet. Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van o.a. de gemeente kan worden nagegaan.

Het doel van deze logging is tweeledig:

1. Tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende verwerking (via specifieke rapportages.
2. Wetenschappelijke en/of statistische doeleinden (via generieke rapportages).

De gebruikers van Suwinet-Inkijk weten dat over hen gegevens worden verzameld en vastgelegd. Bij indiensttreding krijgen zij het protocol 'Suwinet-Inkijk' (bijlage 6) uitgereikt en tekenen zij de geheimhoudingsverklaring (bijlage 5). Dit is aanvullend op de afgelegde ambtseed resp. integriteits- en geheimhoudingsverklaring voor externe medewerkers een belangrijk onderdeel van de privacybescherming en informatiebeveiliging ten opzichte van deze medewerkers. Nu Suwinet hoogst privacygevoelige gegevens bevat, rechtvaardigt dit een specifieke verklaring van medewerkers die persoonsgegevens uit Suwinet raadplegen.

De medewerkers zijn op de hoogte van de volgende informatie:

- Het bestaan van de logging-gegevens;
- De (aard van de) gegevens die binnen deze applicatie worden gelogd.

Doelen van de logging;

- De gelogde gegevens worden niet voor andere doeleinden gebruikt dan waarvoor ze zijn vastgelegd.

Het vastleggen van de wijze en het moment waarop en door wie een onrechtmatig of doeloverschrijdend gebruik van het Suwinet-Inkijk wordt geconstateerd. Dat bij bovenstaande constatering dit door de teamleider wordt gecommuniceerd met de betreffende medewerker(s).

In het kader van de beveiliging wordt het beheer voor het gebruik van Suwinet neergelegd bij de functioneel beheerders van de afdeling Publieksservice. Zij zijn verantwoordelijk voor het beheren van accounts. De (logging)-gegevens over het gebruik van Suwinet-Inkijk worden regelmatig uitgevraagd door de medewerker interne controle/ security officer. De medewerker houdt regelmatig een steekproef of aan de gemaakte afspraken voldaan wordt. De resultaten van deze steekproef worden gerapporteerd aan de directeur van Werkplein Fivelingo.

De volgende gegevens worden gelogd:

- het tijdstip van iedere log-in en log-out en andere actie;
- de gebruikersnaam van degene die inlogt/uitlogt;
- elk BSN-nummer (of andere zoeksleutel) waarvan gegevens worden opgevraagd wordt als actie geregistreerd;
- elke actie, zoals de bekeken kolom- of overzichtspagina´s.

In het kader van de beveiliging wordt voorgesteld om de gegevens over het gebruik van Suwinet-Inkijk 1x per 3 maanden te laten uitvragen.

Suwinet-Rapportages

BKWI heeft twee soorten gebruiksrapportages: generieke en specifieke gebruiksrapportages.

Generieke gebruiksrapportages

BKWI verstrekt de aangesloten organisaties op reguliere basis generieke gebruiksrapportages over het gebruik van Suwinet. Deze geanonimiseerde rapportages zijn bedoeld om het management te ondersteunen bij het beoordelen van het gebruik van Suwinet. Generieke gebruiksrapportages worden elke maand automatisch klaargezet binnen Suwinet-Inkijk. Deze geven een globaal beeld van het gebruik en bevatten geen persoonsinformatie. De logginggegevens worden door de kwaliteitsmedewerker beoordeeld.

Specifieke gebruiksrapportages

Wanneer afwijkingen worden geconstateerd in de rapportages worden door de security officer hiervoor een specifieke rapportage aan te vragen ter ondersteuning van het interne controleproces. Deze rapportages bevatten gegevens over de handelingen van geautoriseerde gebruikers, onder andere persoonsgegevens van zowel gebruikers (gebruikersnamen) als geraadpleegde personen (burgerservicenummers). BKWI heeft in lijn met de Wet bescherming persoonsgegevens een zorgvuldig proces ingericht voor het opvragen van specifieke gebruiksrapportages door aangesloten organisaties.

5 Bijlagen

Bijlage 1: Tien gouden regels bij beveiliging van persoonsgegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Concreet kunnen deze regels als volgt worden vertaald:

1. Beheren van wachtwoorden

De gebruiker moet het door de administrator uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord iedere keer na x dagen. De gebruiker heeft dus het eigen beheer over het wachtwoord. Zodra een medewerker de gemeente verlaat, wordt het account verwijderd. Wanneer het account x weken niet wordt gebruikt, vervalt het account automatisch.

2. Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de applicatiebeheerder. Vervolgens wordt de afdeling Systeembeheer ingeschakeld om dat incident te onderzoeken. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht

Binnen Werkplein Fivelingo wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI en in de CAO zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is.

4. Gedragscode internet- en emailgebruik

De gemeente hanteert een protocol voor gebruik van email en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met email en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van externe email en internet wordt geobserveerd. Het protocol is voor alle medewerkers van de gemeente te raadplegen op het gemeentelijke Intranet.

5. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen Werkplein Fivelingo geldende informatiebeveiligingsbeleid (inclusief instructies en protocollen) is op iedereen binnen de afdeling van toepassing die gebruik maakt van Suwinet-Inkijk. Alle gebruikers hebben een exemplaar van de beveiligingsnota ontvangen en ook nieuwe medewerkers/gebruikers zullen via het afdelingshoofd een exemplaar ontvangen. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. In de beveiligingsnota is hier uitgebreid aandacht aan besteed. Jaarlijks, bij de evaluatie van het Beveiligingsnota, wordt dit onderwerp geagendeerd voor het werkoverleg.

6. Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Het voeren van telefoongesprekken brengt namelijk de risico's met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben. In principe

wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven indien afkomstig van een vaste contactpersoon.

7. 'Clean desk' en 'clear screen' policy

De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven. Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De kans is derhalve gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De screensaver is zodanig ingesteld dat na een x-aantal minuten de schermbeveiliging intreedt. Dit is door de afdeling Systeembeheer voor iedere medewerker standaard ingesteld.

8. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen Werkplein Fivelingo. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Daarom zijn er op iedere kamer speciale zakken geplaatst, waarin het te vernietigen materiaal verzameld wordt. De verzamelde vertrouwelijke gegevens worden regelmatig aangeleverd bij het vernietigingsbedrijf. Vertrouwelijke gegevens dienen niet terecht te komen in een prullenbak of een bak die bestemd is voor oud papier.

9. Aanspreken van onbekende personen

In het geval dat een medewerker van Werkplein Fivelingo een voor hem/haar onbekende persoon in de gang van de afdeling tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hun beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daarnaartoe te begeleiden.

10. De dagelijkse werkzaamheden vs. Informatiebeveiliging

Informatiebeveiliging is uitermate belangrijk voor het werk binnen Werkplein Fivelingo waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook cliënten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom middels het werkoverleg geregeld aandacht voor dit onderwerp besteed dient te worden.

Bijlage 2: Rollen, taken en verantwoordelijkheden (autorisatiematrix)

	Naam	Pad	Kans op onzorgvuldig gebruik	Medew. rechtmatigheid	Terugvordering & Verhaal	Soc. recherche	Medew. re-integratie	Medew. Uitkeringen	Controle security officer	RMC	G.Buisman	Bolwijn	Appl.beheer
1	Bedrijvenregister	gsd/sbr		X		X	X						
2	Beheer: ww & blokkeren	gsd/useradmin-lite											X
3	Belastingdienst	gsd/belastingdienst		X	X	X		X					
4	Bijstandsregelingen	gsd/bijstandsregelingen		X	X		X	X		X			
5	Correctieservice	_CS/gsd		X	X								
6	Downloaden generieke rapportages	/report/reportfileserver											
7	Downloaden specifieke rapportages	/report/reportfileserver-privacy											
8	DUO gegevens	gsd/duo-gegevens		X		X	X	X					
9	Fraude scorekaart	gsd/fsc		X									
10	Fraude vorderingen	gsd/fraude-vorderingen			X								
11	GBA	gsd/gba											
12	GBA4	gsd/gba-isd4											
13	GBA Volledig	gsd/gba-volledig		X	X	X	X	X		X			
14	Gebruikersadministratie	gsd/useradmin											X
15	GSD voor IB-groep	https://ibgroep-prod.suwinet.nl:443/gsd/											
16	Inkomstenverhoudingen	gsd/inkomstenverhoudingen		X		X		X					
17	Kadaster	gsd/kadaster		X		X							
18	Klant algemeen	gsd/klant-algemeen											
19	Klant algemeen+	gsd/klant-algemeen-plus											
20	Klantbeeld	gsd/klantbeeld											
21	Kostendelerstoets	gsd/kostendelerstoets		X		X		X					
22	Onderhouden correctieservice	gsd/tipp-ex-admin											X
23	Onderhouden status wijzigingsverzoeken	gsd/tipp-ex											
24	Onderhouden werkvoorraad	gsd/werkvoorraad											X
25	Opvragen generieke gebruikersrapportages	gsd/documenten											X
26	Opvragen specifieke gebruikersrapportages	gsd/documenten-privacy							X				
27	RDW	gsd/rdw											
28	RDW+	gsd/rdw-plus											
29	RDW peildata	gsd/rdw-peildata		X		X							
30	Rechtmatigheid	gsd/rechtmatigheid								X		X	
31	Rechtmatigheid+	gsd/rechtmatigheid-plus		X		X							
32	Re-integratie	gsd/re-integratie					X			X			
33	SBR Query	gsd/sbrq					X						
34	SCI	https://ibgroep-prod.suwinet.nl:443/SCI/											
35	SVB gegevens	gsd/svb-gegevens		X		X		X					
36	Terugvordering en Verhaal	gsd/terugvordering			X								
37	UWV Uitkeringen	gsd/uwv-uitkeringen		X		X		X					
38	UWVWb	gsd/cwi		X		X	X						
39	Whitelist escape	http://special-resources/whitelist-escape/		X	X	X							
40	WIS-proxy Erow	https://wis-productie.suwinet.nl:443/		X							X		X
41	www.werk.nl	https://www.werk.nl:443/		X	X	X	X	X					
42	Zoek+ in GBA	gsd/zoek-in-gba-uitgebr				X							
43	Zoek in GBA	gsd/zoek-in-gba											
44	Zoek in Kadaster	gsd/zoek-in-kadaster				X							
45	Zoek in RDW	gsd/zoek-in-rdw											
46	Zoek in RDW+	gsd/zoek-in-rdw-plus				X							

Overzichtspagina's
Bronpagina's
Zoekpagina's
Overige (beheer)pagina's
Toegangsrechten voor andere applicaties

Bijlage 3: Taakbeschrijving Security Officer

Eisen die de Suwi-keten aan de Security Officer stelt.

- De Security Officer is het aanspreekpunt voor alle zaken aangaande de beveiliging van Suwinet. Het belangrijkste is hierbij de beveiliging van het netwerk, de gegevensuitwisseling en de bescherming van de privacy van de burger, waarvan de gegevens worden uitgewisseld.
- De functie van Security Officer is als staffunctie belegd binnen Werkplein Fivelingo, waarbij de Security Officer aan het hoogste gezagsorgaan binnen de organisatie rapporteert, bij Werkplein Fivelingo is dat de directeur.
- De Security Officer bevordert en adviseert op het gebied van (informatie-) beveiliging, controleert of en in hoeverre beveiligingsmaatregelen worden nageleefd, rapporteert over de status van de beveiliging, evalueert de uitkomsten van de beveiligingsonderzoeken en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging.

Taken van de Security Officer bij Werkplein Fivelingo

De Security Officer:

- Fungeert als centraal aanspreekpunt op het gebied van informatiebeveiliging;
- Voert periodieke controles uit op een rechtmatig gebruik van Suwinet;
- Beoordeelt, op basis van de visie op de betekenis van beveiliging voor de organisatie, de risico's en oplosrichtingen en hiervoor passende maatregelen.
- Stelt doelen voor de beveiliging in de vorm van een informatiebeveiligingsbeleid en vertaalt dit beleid naar een strategie om deze doelen te bereiken, via een beveiligingsplan en –activiteiten.
- Coördineert alle beveiliging gerelateerde activiteiten, in het bijzonder de afhandeling van beveiligingsincidenten.
- Toetst de uitvoering aan richtlijnen en beleid en het op relevantie voor beveiliging beoordelen van in- en externe rapportages.
- Adviseert gevraagd en ongevraagd het management aangaande de beveiliging.
- Bevordert het beveiligingsbewustzijn bij de medewerkers.
- Onderneemt actie voor de jaarlijkse evaluatie en het actueel houden van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan SUWI.

Nieuwe rol Functionaris Gegevensbescherming (FG) vanaf mei 2018

Onder de komende Europese privacyverordening (AVG), die in mei 2018 van kracht wordt, zijn alle overheidsorganisaties straks verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. De FG is verantwoordelijk voor het toezicht houden op de naleving van de privacywetten en -regels, het inventariseren en bijhouden van gegevensverwerkingen en het afhandelen van vragen en klachten van mensen binnen en buiten de organisatie. Daarnaast kan de FG ondersteunen bij het ontwikkelen van interne regelingen, het adviseren over privacy op maat én het leveren van input bij het opstellen of aanpassen van gedragscodes.

De FG is moet toezicht houden en indien nodig kunnen handhaven en is daarmee het verlengde van de Autoriteit Persoonsgegevens. De FG is een onafhankelijke staffunctie en ressorteert rechtstreeks onder de directeur maar kan direct aan het bestuur rapporteren. In de praktijk zal bij Werkplein Fivelingo de Security Officer de rol van FG overnemen.

Bijlage 4: Gedragscode internet en emailgebruik

Toelichting op de gedragscode Internet en e-mailgebruik

Het gebruik van Internet en e-mail is niet meer weg te denken in het maatschappelijke verkeer. Het heeft veel voordelen voor de productiviteit, de bereikbaarheid en de snelheid waarmee gegevens kunnen worden uitgewisseld. Werkplein Fivelingo heeft de plicht om toezicht te houden op de aard en de omvang van het gebruik van Internet en de e-mailfunctionaliteit binnen de eigen organisatie. Bij incidenten kan de code worden gebruikt om maatregelen te nemen.

In deze gedragscode Internet en e-mailgebruik zijn gedragsregels opgenomen voor een verantwoord Internet en e-mailgebruik en voor de manier waarop controle op het gebruik van de werkplek kan plaatsvinden. Er is naar gestreefd om een goede balans te vinden tussen de controlemogelijkheden enerzijds en de bescherming van de persoonlijke levenssfeer van de medewerker anderzijds.

In de gedragscode Internet en e-mailgebruik is het begrip medewerker ruim geformuleerd. Niet alleen de eigen werknemer, maar ook bijvoorbeeld de stagiaire, de uitzendkracht en de ingeleende arbeidskracht die op de werkplek gebruik maakt van Internet of e-mail valt onder de werking van de gedragscode. Tevens is het begrip werkplek zo geformuleerd dat het geen verschil maakt op welke fysieke plaats de medewerker gebruik maakt van de apparatuur. Dit betekent dat de gedragscode bijvoorbeeld ook van toepassing is op thuiswerkers.

In de gedragscode is onderscheid gemaakt tussen het zakelijk- en het privégebruik van de werkplek en voor beide vormen van gebruik zijn de grenzen aangegeven. Zo is weliswaar het privégebruik van Internet en e-mail toegestaan, maar alleen als dit de voortgang van de dagelijkse werkzaamheden niet belemmert. Bovendien is het niet toegestaan gebruik te maken van Internetpagina's die discriminerende, pornografische of daarmee vergelijkbare uitingen bevatten en is het verboden soortgelijke e-mail te verzenden of te ontvangen.

Met betrekking tot de omschrijving van het begrip verwerking van gegevens is in de gedragscode aansluiting gezocht bij de Wet bescherming persoonsgegevens (WBP). De gedragscode ziet op die verwerking van de gegevens over het gebruik van Internet en e-mailfunctionaliteit op de werkplek, die tot de individuele medewerker zijn te herleiden. Als de verkregen gegevens niet tot de individuele medewerker (kunnen) worden herleid, bijvoorbeeld als zij worden verwerkt ten behoeve van managementrapportage of gebruiksstatistiek, is verwerking zonder meer toegestaan. De verwerking zal zich in die gevallen meestal beperken tot getotaliseerde en geanonimiseerde verkeersgegevens over het gebruik van e-mail en Internet, zoals tijd, hoeveelheid en omvang van gebruik.

Werkplein Fivelingo mag slechts tot verwerking van gegevens overgaan als er sprake is van een vermoeden van een strafbaar feit, schending van bedrijfsgeheimen, bovenmatig gebruik of van gebruik waarbij de goede naam de gemeente c.q. Werkplein Fivelingo in geding is en in gevallen genoemd in artikel 5 en 7 tweede lid. De verwerking van gegevens moet behoorlijk en zorgvuldig plaatsvinden. Daarom is in de gedragscode bepaald dat vooraf schriftelijk moet vastleggen wat de aard is van het veronderstelde misbruik, de wijze en de duur van de verwerking en de waarborgen die zijn genomen ter bescherming van de privacy van de werknemer.

De behoefte om te controleren of gedragsregels door de medewerker worden nageleefd, rechtvaardigt overigens geen permanente controle op het gebruik. Dit zou een te vergaande inbreuk op de persoonlijke levenssfeer van de werknemer betekenen. Als een medewerker of een groep medewerkers ervan worden verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. Alleen e-mail berichten waartegen zwaarwegende bedenkingen bestaan mogen op inhoud worden gecontroleerd.

Als misbruik wordt geconstateerd is Werkplein Fivelingo bevoegd maatregelen te nemen tegen de medewerker. Het kan daarbij gaan om disciplinaire of arbeidsrechtelijke maatregelen, zoals berisping, overplaatsing, schorsing of beëindiging van de arbeidsovereenkomst. De aard van de te treffen maatregel hangt af van de aard en de omvang van overtreding en van de vraag of er al dan niet schade is ontstaan. De schade kan bijvoorbeeld bestaan uit feitelijke beschadigingen aan het systeem of een onderdeel daarvan - zoals het binnenhalen van een virus - of doordat de goede naam van de gemeente c.q. Werkplein Fivelingo in diskrediet is gebracht. Een opgelegde maatregel wordt gemotiveerd en in het personeelsdossier geregistreerd.

1. Definities

Artikel 1. Definities

In deze code wordt verstaan onder:

1. Medewerker: iedereen die werkzaamheden verricht voor Werkplein Fivelingo, ongeacht of hij in dienst is van Werkplein Fivelingo of is ingehuurd.
2. Werkplek: de door Werkplein Fivelingo ter beschikking gestelde apparatuur waarmee in beginsel gebruik kan worden gemaakt van het Internet en de e-mailfunctionaliteit, ongeacht de fysieke plaats waar de apparatuur wordt gebruikt.
3. Verwerking van gegevens: alle handelingen door Werkplein Fivelingo met betrekking tot gegevens over het gebruik van Internet en e-mail op de werkplek die tot een individuele medewerker kunnen worden herleid.

2. Doel en algemene uitgangspunten

Artikel 2. Doel

Met de gedragscode wordt beoogd een verantwoord gebruik van het Internet en de e-mailfunctionaliteit op de werkplek door de medewerkers en bevat regels voor de verwerking van gegevens door Werkplein Fivelingo.

Artikel 3. Algemene uitgangspunten

1. Op de verwerking van gegevens is de Wet bescherming persoonsgegevens (WBP) van toepassing.
2. Verwerking van gegevens is toegestaan als Werkplein Fivelingo na zorgvuldige afweging van oordeel is dat het recht op privacy van de werknemer in verhouding tot het gerechtvaardigde bedrijfsbelang niet onevenredig wordt geschaad.
3. Verwerking van gegevens is toegestaan binnen de in deze gedragscode uitdrukkelijk omschreven doeleinden.

3. Gebruik van het Internet

Artikel 4. Internet

1. Werkplein Fivelingo stelt in beginsel voor elke werkplek de toegang tot het Internet beschikbaar.
2. Werkplein Fivelingo kan de toegang tot het Internet op de werkplek onthouden of beperken als zij van oordeel is dat de toegang voor een goed en volledig verrichten van de werkzaamheden niet noodzakelijk is.
3. De medewerker mag geen veranderingen aanbrengen in de hardware of de software van de werkplek.
4. De medewerker mag geen wijziging aanbrengen aan de door Werkplein Fivelingo beschikbaar gestelde toegang tot het Internet op de werkplek.
5. Op een verzoek van de medewerker om wijziging van de door Werkplein Fivelingo beschikbaar gestelde toegang tot het Internet op de werkplek beslist zijn directe leidinggevende.

Artikel 5. Privé-gebruik Internet

1. Een medewerker mag voor niet-zakelijke doeleinden beperkt gebruik maken van het Internet als dit de voortgang van de dagelijkse werkzaamheden niet belemmert.
2. Een medewerker mag geen gebruik maken van Internetpagina's die discriminerende, pornografische of daarmee vergelijkbare uitingen bevatten.
3. Werkplein Fivelingo kan het gebruik als bedoeld in het eerste lid te beperken.
4. Gebruik van de e-mailfunctionaliteit

Artikel 6. E-mail

1. Werkplein Fivelingo stelt in beginsel voor elke werkplek de e-mailfunctionaliteit beschikbaar.
2. Werkplein Fivelingo kan het gebruik van de e-mailfunctionaliteit op de werkplek onthouden of beperken als zij van oordeel is dat het gebruik voor een goed en volledig verrichten van de werkzaamheden niet noodzakelijk is.

Artikel 7. Privé-gebruik e-mail

1. Een medewerker mag voor niet-zakelijke doeleinden beperkt gebruik maken van de e-mailfunctionaliteit als dit de voortgang van de dagelijkse werkzaamheden niet belemmert.
2. Een medewerker mag geen gebruik maken van de e-mailfunctionaliteit om discriminerende, pornografische of daarmee vergelijkbare uitingen te verzenden of te ontvangen, waaronder tevens worden begrepen de verkondiging van politieke en religieuze standpunten.
3. Werkplein Fivelingo kan het gebruik als bedoeld in het eerste lid te beperken.

5. Verwerking van gegevens

Artikel 8. Verwerking van gegevens

1. Werkplein Fivelingo kan tot verwerking van gegevens besluiten als zij vermoedt dat sprake is van een strafbaar feit, schending van bedrijfsgeheimen, bovenmatig gebruik, gebruik waarbij de goede naam van de gemeente c.q. Werkplein Fivelingo in geding is of kan komen en in de gevallen bedoeld in Artikel 5 en 7 tweede lid.
2. Bevoegd tot het geven van een opdracht tot verwerking van gegevens in de gevallen genoemd in het eerste lid, is de leidinggevende manager.
3. Voordat Werkplein Fivelingo tot verwerking van gegevens overgaat legt zij schriftelijk vast, de aard van het veronderstelde misbruik, de wijze en tijdsduur van de verwerking en de waarborgen die zijn genomen ter bescherming van de privacy van de medewerker.
4. De leidinggevende manager die gebruik maakt van de bevoegdheid genoemd in het tweede lid, belast de systeembeheerder of een daartoe uitdrukkelijk aangewezen functionaris met de uitvoering.
5. De functionaris genoemd in het vierde lid is verplicht tot geheimhouding van hetgeen hem of haar bij de verwerking van gegevens is bekend geworden.
6. Van de inhoud van een e-mailbericht waartegen geen zwaarwichtige bedenkingen bestaan mag geen kennis worden genomen.
7. Werkplein Fivelingo stelt de medewerker wiens gegevens zijn verwerkt in kennis van de uitkomst van het onderzoek en van de inhoud van het document als bedoeld in het derde lid.
8. De verwerkte gegevens zullen na afloop van het onderzoek worden vernietigd, tenzij het vermoeden van misbruik door het onderzoek is bevestigd.

6. Rechten van de werknemer

Artikel 9. Rechten van de medewerker

1. De medewerker heeft het recht op inzage in de over hem verwerkte gegevens.

2. De medewerker heeft het recht te verzoeken feitelijk onjuiste gegevens te verbeteren, aan te vullen of te verwijderen.
3. De medewerker heeft het recht te verzoeken verwerkte gegevens die niet (langer) ter zake doen, hetzij in strijd zijn met deze gedragscode of een wettelijk voorschrift, te verwijderen en te vernietigen.
4. Op een verzoek als bedoeld in het tweede en derde lid beslist Werkplein Fivelingo binnen vier weken.
5. Als een verzoek als bedoeld in het tweede en derde lid wordt ingewilligd draagt Werkplein Fivelingo zorg dat daaraan terstond uitvoering wordt gegeven.

Artikel 10. Leden van de ondernemingsraad

1. Onverminderd het bepaalde in Artikel 8, is Werkplein Fivelingo niet bevoegd kennis te nemen van de inhoud van e-mailberichten die leden van de ondernemingsraad of van een commissie van die raad uit hoofde van hun lidmaatschap verzenden of ontvangen.

7. Sancties en Slotbepalingen

Artikel 11. Sancties

1. In geval van overtreding van de bepalingen van deze gedragscode kan Werkplein Fivelingo jegens de werknemer disciplinaire of arbeidsrechtelijke maatregelen treffen.
2. De aard van de te treffen maatregel is afhankelijk van de aard en de ernst van de overtreding en van de mogelijk toegebrachte materiële of immateriële schade.
3. Een opgelegde maatregel als bedoeld in het tweede lid wordt met redenen omkleed en in het personeelsdossier opgenomen.

Artikel 12. Toezicht

De leidinggevende manager is belast met het toezicht op de naleving van deze gedragscode.

Artikel 13. Citeertitel

Deze gedragscode wordt aangehaald als “Gedragscode Internet en e-mailgebruik”.

Artikel 14. Inwerkingtreding en bekendmaking

1. De gedragscode is voor instemming voorgelegd aan de ondernemingsraad.
2. De gedragscode treedt in werking nadat deze is ondertekend en op een voor iedere werknemer zichtbare, toegankelijke en bereikbare plaats is bekendgemaakt.

Ondertekening

Plaats : .....

Datum : .....

Handtekening : .....

Bijlage 5: Geheimhoudingsverklaring

Persoonsgegevens

Ondergetekende,

Naam : .....

Geboren : .....

Functie : .....

In (tijdelijke) dienst via : .....

Bij Werkplein Fivelingo vanaf : .....

Verklaart hierbij dat hij/zij alle zaken, waarvan hij/zij in het kader van zijn/haar werkzaamheden kennis draagt en die hem/haar als vertrouwelijk of geheim zijn toevertrouwd of te zijne/hare kennis zijn gekomen, niet zal openbaren aan anderen, dan aan hen, wie hij/zij volgens de wet of ambtshalve tot mededeling verplicht is. Zowel gedurende de periode waarin hij/zij bij de Werkplein Fivelingo werkzaam is als daarna.

Ondergetekende verklaart te hebben ontvangen:

1. Informatiebeveiligingsbeleid en informatiebeveiligingsplan SUWI van Werkplein Fivelingo;
2. 10 gouden regels voor een beveiligd gebruik van informatie, informatiesystemen en netwerken;
3. Gedragscode internet en emailgebruik.

Ondergetekende verklaart voorts bekend te zijn met hetgeen ten aanzien van de geheimhouding in de wet is bepaald te weten art. 272 WvSr en dat hij/zij tevens op de hoogte is van het feit dat schending van de geheimhoudingsplicht als ernstig plichtverzuim wordt aangemerkt en een onvrijwillig onmiddellijke beëindiging van het contract tot gevolg heeft.

Ondertekening

Plaats : .....

Datum : .....

Handtekening : .....

Bijlage 6: Protocol inzage in Suwinet door cliënt en/of gemachtigde

Inleiding

Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, in de hieronder beschreven gevallen, is gegevensinzage door derden mogelijk.

De via Suwinet-Inkijk opvraagbare gegevens zijn alleen in electronische vorm te zien. De gegevens moge niet lokaal worden opgeslagen (op de harde schijf of op diskette).

Hieronder volgt een handleiding voor een aantal situaties waar de Suwi-gebruiker mee te maken kan krijgen.

1. Inzage

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 (rijbewijs, paspoort, etc.);
- Vraag om het sofinummer van de cliënt;
- Stel vast dat het sofinummer is ontleend aan een officieel document (rijbewijs, paspoort etc.)
- Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm;
- Berg (mogelijk tweede) 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 de balie of moet een schriftelijk verzoek indienen, dat binnen de wettelijk verplichte termijn dient te worden afgehandeld. Indien de cliënt inzage wil in al zijn/haar gegevens die bij een ketenpartner zijn geregistreerd, dient de klant te worden verwezen naar de betreffende ketenpartner.

Gemachtigde verzoekt schriftelijk om inzage in cliëntgegevens

- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
- Vraag om het sofinummer van de cliënt;
- Stel vast dat het sofinummer is ontleend aan een officieel document (rijbewijs, paspoort etc.)
- Maak een uitdraai van de geraadpleegde gegevens of laat de gemachtigde meekijken op het scherm;
- Berg (mogelijk tweede) uitdraai onmiddellijk op in het cliëntendossier of vernietig eventueel uitgedraaid exemplaar;
- Beëindig inkijksessie.

Een derde verzoekt om inzage, hetzij schriftelijk, hetzij mondeling in cliëntgegevens

- Dit is niet mogelijk

2. Correctie

De cliënt verzoekt om correctie

- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
- Vraag om het sofinummer van de cliënt;
- Stel vast dat het sofinummer is ontleend aan een officieel document (rijbewijs, paspoort etc.);
- Informeer de cliënt dat hij/zij een officieel verzoek moet indienen via een standaardformulier;
- Maak twee kopieën van het verzoek;
- Verstrek een kopie aan de cliënt, archiveer de andere kopie.

Gemachtigde verzoekt om correctie

- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
- Vraag om het sofinummer van de cliënt;
- Stel vast dat het sofinummer is ontleend aan een officieel document (rijbewijs, paspoort etc.)
- Informeer de gemachtigde dat hij/zij een officieel verzoek moet indienen via een standaardformulier;
- Maak twee kopieën van het verzoek;
- Verstrek een kopie aan de gemachtigde, archiveer de andere kopie

Een derde verzoekt om correctie

- Dit is niet mogelijk