**Agendapunt 7 van MT 23-1-2007**

ISD Noordoost

# Beveiligingplan Suwinet

## 1. Inleiding

Het Bureau Keteninformatisering werk en inkomen (BKWI), het Centrum voor Werk en Inkomen (CWI), de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en gemeenten wisselen persoonsgegevens met elkaar uit via Suwinet, een electronische infrastructuur. Met de faciliteit Suwinet-Inkijk worden gegevens op basis van sofinummers toegankelijk gemaakt voor bevoegde medewerkers. Het gaat over privacygevoelige gegevens over 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 er op kunnen vertrouwen dat "hun" gegevens door de partners in de Suwiketen op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage XIV van de regeling Suwi.

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.).

Het IWI heeft in februari 2005 haar rapport "Beveiliging Suwinet bij gemeenten" uitgebracht. Het IWI concludeert enerzijds dat bij (bij de 50 onderzochte gemeenten) gemeenten "risico's (aanwezig) zijn voor de beveiliging van de met Suwinet uitgewisselde gegevens". Anderzijds gaven veel gemeenten aan er niet van op de hoogte te zijn dat zij een beveiligingsplan moeten opstellen.
Naar aanleiding van dit rapport is ook de VNG van mening dat beveiliging van het Suwinet bij gemeenten de komende tijd een punt van aandacht moet zijn.
Mogelijk zal het IWI nog dit jaar alle gemeenten onderzoeken middels een "beveiligings" audit.

Daarnaast dienen gemeenten zich in het Verslag over de uitvoering (VODU), conform artikel 77 van de WWB, 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.

Redenen genoeg om een Beveiligingsplan Suwinet voor ISD Noordoost vast te stellen.

Dit Beveiligingsplan is geen statisch document; het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisatie en de omgeving van de sociale dienst 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.

## 2. Verdeling verantwoordelijkheden medewerkers ISD Noordoost

Er zijn een viertal functies binnenISD Noordoost die geautoriseerd zijn om gebruik te maken van Suwinet-Inkijk. Het gaat om de volgende functies:

- applicatiebeheerder;
- medewerkers uitkeringsadministratie;
- consulenten werk en inkomen
- consulenten terugvordering en verhaal

De directeur van ISD Noordoost is overigens eindverantwoordelijke voor het gebruik en de beveiliging van Suwinet Inkijk.

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

Functie Taken/verantwoordelijkheden
Applicatiebeheerder ? Driemaandelijkse controle logginggegevens.
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 (zie hieronder bij punt 3).

- 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
  Medewerkers uitkeringsadministratie
  Consulenten werk en inkomen
  Consulenten terugvordering en verhaal Gebruikers Suwinet-Inkijk (raadplegen)

## 3. Gebruik Suwinet-Inkijk

Er zijn drie functies waarin Suwinet-Inkijk gebruikt wordt voor het raadplegen van cliëntgegevens/informatie.
In de onderstaande tabel volgt per functie in welke gevallen Suwinet-Inkijk gebruikt mag/kan 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.

Functie Afspraken over gebruik Suwinet-Inkijk
Medewerkers uitkeringsadministratie ? bij afhandeling maandelijkse signalen Inlichtingen Bureau (IB)
Consulenten werk en inkomen
Consulenten terugvordering en verhaal ? bij aanvragen WWB, Ioaw, Ioaz, Bbz uitkering

- bij heronderzoeken1 (zowel rechtmatigheids- als doelmatigheidsonderzoeken)
- bij debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen, werkgever
- in die gevallen ter beoordeling van de consulent. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage van de consulent

## 4. Logging rapportages

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft rapportages ontwikkeld omtrent de logging van het gebruik van Suwinet-Inkijk.
Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van o.a. de gemeente kan worden nagegaan.
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 sofi-nummer (of andere zoeksleutel) waarvan gegevens worden opgevraagd wordt als actie geregistreerd;
- elke actie, zoals de bekeken kolom- of overzichtspagina´s.

Het doel van deze logging is tweeledig:
1. tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende verwerking:
2. wetenschappelijke en/of statistische doeleinden.

De gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden verzameld en vastgelegd. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Met het oog hierop moet de navolgende informatie worden verstrekt aan de medewerkers die (gaan) werken met Suwinet-Inkijk.:

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

- Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- 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 directeur van ISD Noordoost wordt gecommuniceerd met de betreffende medewerker(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.
Het betreft dan de volgende gegevens:

1. Inkijkacties;
2. Opvragingen unieke sofinummers;
3. Geldige ten opzichte van ongeldige rollen;
4. Inlogpogingen;
5. Administrator accounts;
6. Accounts per status;
7. Opvragingen per pagina;
8. Geregistreerde ten opzichte van actieve accounts.

De logginggegevens worden door de applicatiebeheerder beoordeeld.

## 5. 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 ISD Noordoost 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 ISD Noordoost 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. Clear 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 ISD Noordoost. 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 ISD Noordoost 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 daar naar toe te begeleiden.

**10. De dagelijkse werkzaamheden vs. Informatiebeveiliging**
Informatiebeveiliging is uitermate belangrijk voor het werk binnen ISD Noordoost 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.

## 6. Protocol inzage in Suwinet door cliënt en/of gemachtigde

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.

**INZAGE**

***1. 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.

***2. 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.

***3. Een derde verzoekt om inzage, hetzij schriftelijk, hetzij mondeling in cliëntgegevens***

- Dit is niet mogelijk

**CORRECTIE**

***1. 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.

***2. 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

***3. Een derde verzoekt om correctie***

- Dit is niet mogelijk