Beveiligingsplan SUWINET

Afdeling Maatschappelijke Zaken
Gemeente Stadskanaal

Beveiligingsplan Suwinet afdeling Maatschappelijke zaken
Versie: 2
Status: Definitief
Bewerkt door: M. Westerhof
Datum: 1 maart 2016

Inhoudsopgave

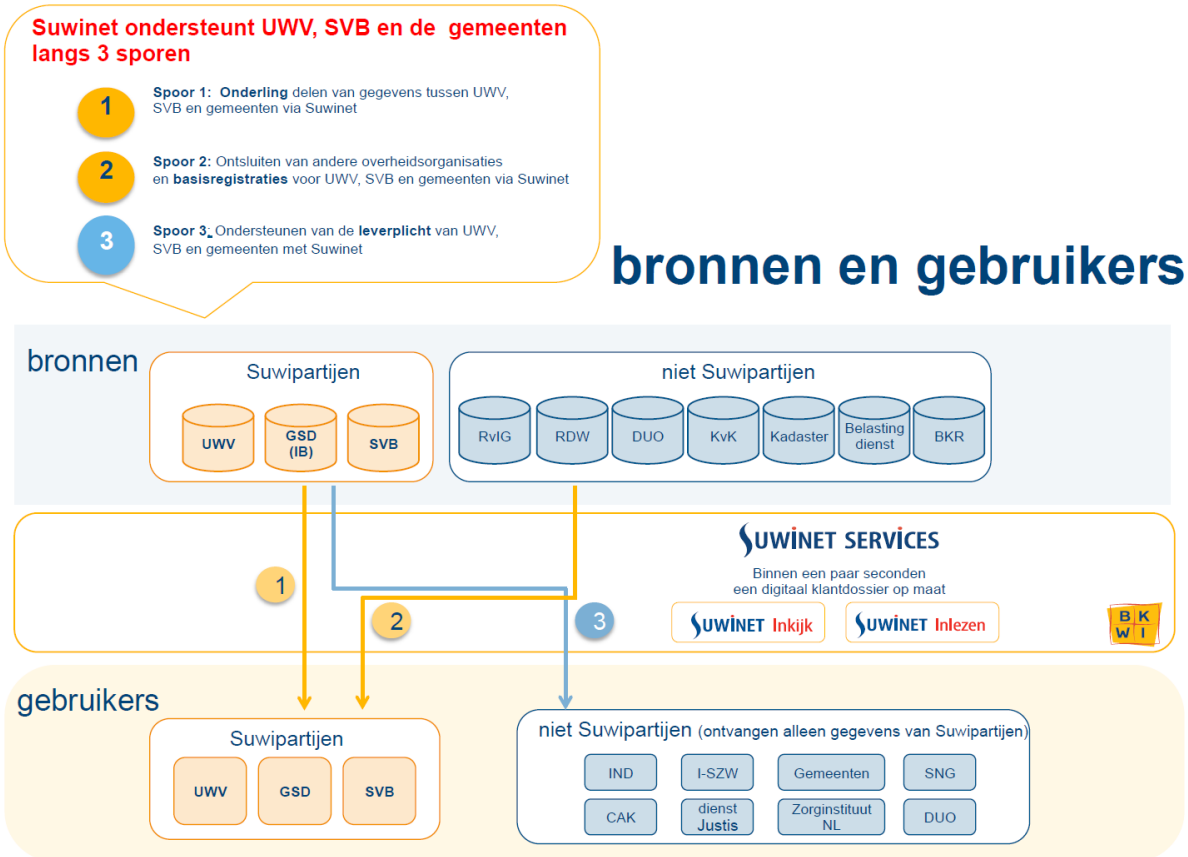
Hoofdstuk 1. Inleiding

1.1. Wat is Suwinet?

De organisaties van de keten Werk en Inkomen (UWV, GSD's en de SVB) wisselen onderling gegevens uit op basis van artikel 62 van de Wet structuur uitvoeringsorganisatie werk en inkomen (wet SUWI). Deze gegevens wisselen zij uit middels de gezamenlijke elektronische voorzieningen Suwi (Suwinet/Digitaal Klantdossier). Met de faciliteit Suwinet-Inkijk worden gegevens op basis van het burgerservicenummer toegankelijk gemaakt voor bevoegde medewerkers. Het gaat over privacygevoelige gegevens over o.a. 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.

Suwinet-Inkijk bevat gegevens die afkomstig zijn van o.a. GSD's, UWV, BRP en de SVB. De Vis (Verificatie Informatie Systeem) is per 1 april 2016 niet meer te benaderen via Suwinet Inkijk omdat er te weinig gebruik van werd gemaakt. Het UWV Werkbedrijf levert bijvoorbeeld gegevens over inschrijvingen als werkzoekende en gegevens over beroepservaring en opleidingen die een persoon gevolgd heeft. De gegevens van GSD's hebben betrekking op uitkeringen en uitkeringsaanvragen in het kader van de WWB, IOAW, IOAZ etc. De gegevens van UWV hebben betrekking op arbeidsrelaties en uitkeringsverhoudingen. De SVB levert gegevens over uitkeringen AKW, AOW, WIA en ANW
Ook de gemeentelijke Basisadministratie levert gegevens, evenals de Rijksdienst voor het wegverkeer (RDW). In 2010 is ook de Dienst Uitvoering Onderwijs (DUO) aangesloten met gegevens over opleidingen en diploma's. Daarnaast biedt Suwinet-Inkijk aanvullende informatie over de status van identiteitsbewijzen (via VIS) en adresgegevens en contactpersonen van bedrijven (KvK en Marktselect).

Suwinet Inkijk overzicht bronnen 1 maart 2016



1.2. Wettelijke basis

Om de Suwiketen 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 voorgeschreven in de wet Suwi (artikel 62).

- *Wet SUWI*

In de Regeling SUWI van de Minister en de Staatssecretaris van Sociale Zaken en Werkgelegenheid houdende Regels op grond van de Wet structuur uitvoeringsorganisatie werk en inkomen en de Invoeringswet Wet structuur uitvoeringsorganisatie werk en inkomen staat:

Artikel 6.4. Beveiliging elektronische voorzieningen SUWI

1. Het UWV, de SVB, de colleges van burgemeester en wethouders, het IB en op de gezamenlijke elektronische voorzieningen SUWI aangesloten niet SUWI-partijen dragen zorg voor de beveiliging van de gegevensuitwisselingen die plaatsvinden in het kader van de gezamenlijke elektronische voorzieningen SUWI, tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid, overeenkomstig hetgeen over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I (‘Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI’).

2. Het UWV, de SVB, de colleges van burgemeester en wethouders, het IB en op de gezamenlijke elektronische voorzieningen SUWI aangesloten niet- SUWI- partijen geven ieder in een beveiligingsplan aan op welke wijze zij invulling geven aan het eerste lid.

3. Artikel 5.22 is van overeenkomstige toepassing op het gebruik en de inrichting van de gezamenlijke elektronische voorzieningen SUWI.

Lid 1 en lid 3 tezamen sluiten goed aan op de Wet Bescherming Persoonsgegevens (WBP). Artikel 5.22 (verantwoording gegevensverwerking) geldt ook voor de gemeente. Overigens (nog) niet de daarin genoemde rapportageplicht aan het ministerie van SZW. Dit heeft betrekking op UWV, SVB en IB. Deze organisaties dienen vóór 15 maart van elk jaar te rapporteren aan de minister van SZW over de opzet en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking. Die rapportage moet worden vergezeld van een oordeel en een rapport van bevindingen van een tot de Nederlandse Orde van Register EDP-Auditors toegelaten persoon.

- *Wet Bescherming Persoonsgegevens (WBP)*

Ook in de 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.

Hoofdstuk 2 Beveiligingsmaatregelen

De aandachtsgebieden voor informatiebeveiliging en het juist omgaan met vertrouwelijke gegevens kunnen worden onderscheiden in tien categorieën. Om een beeld te geven worden ze hieronder allen genoemd.

Tabel 1: Beveiligingscategorieën

Beveiligingscategorieën	***Trefwoorden***
1. Beveiligingsbeleid	Doelstellingen voor informatiebeveiliging vastleggen in beleidsdocument. Goedkeuring en uitdraging beleid door management.
2. Beveiligingsorganisatie	Beveiligingsfuncties, taken en verantwoordelijkheden, coördinatie, samenhang en rapportagelijnen. Verantwoordelijkheid over afspraken met derden.
3. Classificatie en beheer van bedrijfsmiddelen	Overzicht van bedrijfsmiddelen en hun verantwoordelijke 'eigenaar'. Gebruik van classificatieschema's voor informatie.
4. Beveiligingseisen ten aanzien van personeel	Training, beveiligingsbewustwording, veilig gedrag, aanname beleid en functioneringsbeoordeling. Reageren op meldingen en incidenten.
5. Fysieke beveiliging en beveiliging van de omgeving	Beveiliging van de infrastructuur. Toegangscontrole bij de poort, fysieke beveiliging van computerruimten en decentrale computers. Clean desk policy, stroomvoorziening, koeling, bescherming van diskettes, tapes en documentatie.
6. Beheer van communicatie en bedieningsprocessen	Bedieningsprocedures, beheer van de technische beveiliging en verantwoordelijkheden van dit beheer. Antivirusmaatregelen, incidentafhandeling en –rapportage, beveiliging bij uitwisseling, e-mail, ofwel veilige systemen ook veilig houden.
7. Toegangsbeveiliging	Toegangsbeheersing en –autorisatie voor informatiesystemen.
8. Ontwikkeling en onderhoud van systemen	Aandacht voor de nodige beveiligingsfunctionaliteit en veilige ontwikkel- en onderhoudsmethoden leiden 'zeker' tot veilige systemen, die ook veilig blijven.
9. Continuïteitsmanagement	Calamiteitenopvang, rampenplannen, uitwijk.
10. Toezicht	Naleving van wettelijke en contractuele voorschriften, beveiligingscontroles op IT-systemen, IT-audit, interne controle

2.1. Risico analyse

De Autoriteit Persoonsgegevens hanteert vier risicoklassen:

0. publiek niveau;
1. basis niveau;
2. verhoogd niveau;
3. hoog risico.

De gegevensuitwisseling via Suwinet valt onder de risicoklassen 2 en 3.

Bij een risicoanalyse spelen twee factoren een cruciale rol:
- de kans dat een gebeurtenis zich voordoet;
- de schade die door zo'n gebeurtenis wordt toegebracht.

Een inschatting van de risico's bij het gebruik van Suwinet levert het volgende beeld op.

Tabel 2: Risico analyse

	Kans	***Schade***
Organisatorische inbedding beveiligingsbeleid	Redelijk groot	Zeer groot
Bedreiging van binnenuit (misbruik van autorisatie)	Klein	Zeer groot
Bedreigingen van buitenaf (gebouw, werkplekken)	Klein	Groot
Bedreigingen van buitenaf (virusaanvallen hackers)	Redelijk groot	Groot

De fysieke beveiligings- en technische beveiligingsaspecten (Tabel 1: punten 3, 5, 6, 7, 8, 9, en 10) worden in dit plan benoemd voorzover deze nodig zijn. Voor deze beveiligingsmaatregelen wordt verwezen naar het informatiebeveiligingsplan BRP. Dit kan, omdat deze zaken gemeentebreed opgepakt worden.

Een bedreiging van het systeem, waarin privacy gevoelige informatie is opgeslagen, kan van buitenaf of van binnenuit komen. Bij bedreigingen van buitenaf kan een onderscheid gemaakt worden in fysieke bedreigingen (het weer, stroomuitval, inbraak) en logische bedreigingen (ongewenste gasten, hackers).

Voor de fysieke bedreigingen zijn voldoende maatregelen getroffen, het gebouw is beveiligd en de apparatuur waarop Suwinet draait, bevindt zich in werkruimten waar ongeautoriseerde derden geen toegang hebben, hierdoor is het risico op een beveiligingsincident laag. De programmatuur is voldoende beveiligd tegen hackers, hoewel deze dreiging natuurlijk nooit helemaal uit te sluiten is.

Bedreigingen van binnenuit kunnen ook van fysieke aard (brand, computeruitval, zwervende documenten) en van logische aard (misbruik van autorisatie) zijn.

Gebouw en systeem zijn onder verantwoordelijkheid van de Bouwkundig- en accommodatiemedewerker van de afdeling ROB en van de afdeling ICT adequaat beveiligd, dus ook hier een laag fysiek beveiligingsrisico.

2.2. Essentiele beveiligingsnormen

Aan de hand van zeven essentiële beveiligingsnormen uit het Normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS) is door de Inspectie SZW in 2015 getoetst of de beveiliging rondom Suwinet op orde is. Vier normen toetsen of de verantwoordelijkheden goed zijn verdeeld. Drie normen kijken of dat goed is geborgd in de organisatie.

1. Norm 1.3
   De gemeente heeft een formeel vastgesteld beveiligingsbeleid en -plan. Het Beveiligingsplan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door de inzet van mensen en middelen.
2. Norm 1.4
   De gemeente draagt op reguliere basis het beveiligingsbeleid en -plan uit.
3. Norm 1.5
   De gemeente evalueert op reguliere basis beveiligingsbeleid en -plan
4. Norm 2.2
   De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinetgegevens, -applicaties, -processen en -infrastructuur moeten zijn beschreven en duidelijk en afhankelijk van de schaalomvang van de organisatie gescheiden zijn belegd.

5. Norm 2.3
   De Security Officer beheert en beheerst beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. Richtinggevend hoe de norm ingevuld moet zijn:
   De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. De Security Officer rapporteert rechtstreeks aan de bestuurlijk verantwoordelijke.
6. Norm 13.1
   De organisatie autoriseert en registreert de toegang die gebruikers hebben tot de Suwinet applicaties op basis van een formele procedure.
7. Norm 13.5:
   De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats. Richtinggevend hoe de norm ingevuld moet zijn:
   - Interne controle op rechten en gebruik van Suwinet.
   - Analyseren van de van het BKWI verkregen informatie over het gebruik van Suwigegevens.

De maatregelen genoemd in dit plan waarborgen de kwaliteit van de beveiliging van Suwinet zodat aan alle gestelde normen wordt voldaan.

Hoofdstuk 3 Beveiligingsplan Suwinet

Het bestuur van de gemeente Stadskanaal draagt net als het UWV werkbedrijf verantwoordelijkheid voor de beveiliging van de gegevensuitwisseling binnen het Suwinet.

3.1. Doelstelling

De doelstelling van het beveiligingplan Suwinet is, dat de te nemen beveiligingsmaatregelen bekend zijn bij en gedragen worden door het management en de medewerkers die gebruik maken van Suwinet. Sturing, controle en het constant op de agenda houden van het voorgenomen beveiligingsbeleid is zo mogelijk.

3.2. Afbakening beveiligingsmaatregelen vanuit Sociale Zaken en Werkgelegenheid (SZW)

Bij de te kiezen beveiligingsmaatregelen speelt een rationele kosten-baten afweging een rol. Op alle fronten 100% beveiligen is onbetaalbaar.

Het moet duidelijk zijn dat de schade van een beveiligingsincident waarbij misbruik van de autorisatie wordt gemaakt, altijd groot is. Het beschermen van de privacy gevoelige informatie van cliënten is essentieel. Beveiligingsincidenten waarbij de integriteit van de betrokken medewerker in het geding is, vragen om een zorgvuldige aanpak. In die gevallen is er niet alleen een risico voor de gegevens van de cliënt, maar kan ook de betrokken medewerker ernstig geschaad worden.

Hoewel gevallen van misbruik van autorisatie (gelukkig) zeldzaam voorkomen, neemt het risico op een dergelijke gebeurtenis toe, wanneer organisatorisch geen (structurele) controle acties worden uitgevoerd en als bij medewerkers niet regelmatig onder de aandacht gebracht wordt dat persoongegevens alleen mogen worden gebruikt in relatie tot de werkzaamheden die de functie met zich meebrengt.

De uitvoering van alle beveiligingsmaatregelen vindt gedeeltelijk plaats binnen de afdeling Maatschappelijke Zaken. Ze hebben vooral betrekking op de punten 1, 2 en 4 in Tabel 1 (de overige punten zijn omschreven in het informatiebeveiligingsplan BRP en waardedocumenten). In dit beveiligingsplan Suwinet gaat het er daarom om de optimalisering van:

1. Organisatorische inbedding van het beveiligingsbeleid;
2. Heldere procedures, bekend bij alle medewerkers.

Hoofdstuk 4 Personeel

4.1. Beperking aantal geautoriseerde gebruikers

Beveiliging wordt onder meer gerealiseerd door het aantal medewerkers die toegang hebben tot Suwinet te beperken tot een aantal dat echt nodig is. Afgesproken is, dat slechts medewerkers die werkzaam zijn in het primaire proces en de sociale recherche toegang krijgen tot Suwinet. Voor hen wordt een gebruikersaccount en wachtwoord aangemaakt. Naast inloggen op het gemeentelijk netwerk moet op Suwinet apart ingelogd worden.

Per functie danwel gebruiker wordt bepaald welke informatie benodigd is. Aan de hand daarvan worden de autorisaties voor de benodigde rollen beschikbaar gesteld.

Tabel 3: Toegangspoorten Suwinet (peildatum 1 maart 2016)
Bron: http://www.bkwi.nl/uploads/media/20150408_Handreiking_autorisatie_op_Suwinet-Inkijk_voor_GSD_01.pdf

Rol	Inhoud/proces
Bedrijvenregister (G024)	Het Suwi BedrijvenRegister bevat een deel van de gegevens van de KvK en een aanvulling van het bureau Graydon. De informatie is vooral bedoeld voor re-integratie activiteiten maar er kan ook gezocht worden naar eigen bedrijven en economische activiteiten van klanten op bijv. KvK nummer of naam van het bedrijf.
Belastingdienst (R1043)	Bevat de bij de Belastingdienst bekende rekeningnummers en eindsaldi per 31-12 van voorgaande jaar. Ook zijn de toeslagen en heffingskortingen zichtbaar. Gegevens zijn alleen zichtbaar als het BSN is aangemeld bij het Inlichtingenbureau voor samenloopsignalen.
Correctieservice (G031)	Bij gerede twijfel over de juistheid van een persoonsgegeven, kan de professional een terugmelding doen via Suwinet. Terugmelden naar het - GBA is zelfs een wettelijke verplichting.
Opvragen Gebruiksrapportages (R347)	Met deze link kan de gebruiksrapportage worden opgehaald. Deze rapportage geeft inzicht in het gebruik van Suwinet door uw gemeente over de afgelopen 6 maanden. De rapportage leent zich voor bespreking met het management en kan aanleiding zijn om nadere rapportage op te vragen.
Fraude Score Kaart (G004)	Fraudescorekaart: opstellen risicoprofielen.
Fraude vorderingen (R1272)	Toont informatie over bijstandsvorderingen betreffende fraude en/of recidive. Deze mag alleen gebruikt worden om recidive vast te kunnen stellen. Let op: Dit is een risicovolle autorisatie, advies: zeer beperkt toekennen aan bijvoorbeeld recidive beoordelaars. Algemene informatie over vorderingen voor fraude-alertheid is ook terug te vinden op de pagina Klant Algemeen.
BRP (G005)	Actuele informatie rondom persoonsgegevens, verblijfsgegevens, relatie (huidige partner) en overlijden (GBA). Dit is een beperkte gegevens set van de BRP gegevens.
BRP SHV	SHV = Schuldhulpverlening De gebruiker ziet actuele GBA gegevens en daarnaast de historie van adressen en relaties. Gegevens rondom ouders en kinderen.
BRP volledig	De gebruiker ziet actuele GBA gegevens en daarnaast de historie van adressen en relaties. Gegevens rondom ouders en kinderen.
GSD (G019)	De kolompagina GSD bevat alle informatie van GSD: persoonsgegevens, uitkeringsgegevens, aanvragen, vorderingen en re-integratie gegevens. Al deze informatie is ook opgenomen in de pagina Klant Algemeen+.
Handhaving	Een overzichtspagina met relevante procesgerichte informatie uit verschillende bronnen speciaal bedoeld voor sociaal rechercheurs en handhavers. Autorisatie mag niet i.c.m. Klant Algemeen+. Let op: Dit is een risicovolle autorisatie. Advies: zeer beperkt toekennen.
Kadaster*	De pagina bevat informatie over percelen en objecten in Nederland; het

	koopsombedrag, de eigenaar van het perceel of object en de wijze van verkrijging namelijk hypotheek of contant.
Klant Algemeen (G042)	Op deze overzichtspagina combineren wij gegevens van GBA, GSD, UWV, (incl. UWVWb), SVB en DUO zoals: opleiding, arbeid, inkomen en uitkering.
Klant Algemeen+ (G043)	Deze overzichtspagina bevat dezelfde informatie als “Klant Algemeen” en extra informatie over evt. medebewoners.
Klantbeeld (G029)	Deze pagina toont dezelfde gegevens die de klant kan zien na inloggen met DigiD via www.mijnoverheid.nl en www.werk.nl.
Kostendelerstoets	Deze pagina toont medebewoners die mogelijk vallen onder de Kostendelersnorm. Met deze toets kunt u bepalen welke medebewoners uitgezonderd kunnen worden van de kostendelersnorm in verband met scholing, op grond van art. 22a Participatiewet, lid 4, sub d. DUO stelt hiervoor de relevante gegevens beschikbaar.
Langdurigheidstoeslag (G034)	Deze pagina bevat inkomsten en uitkeringsverhoudingen ter beoordeling van het recht op langdurigheidstoeslag.
Onderhouden correctieservice (G032)	Suwinet biedt bronhouders de mogelijkheid de kwaliteit van gegevens te verbeteren door deze open te stellen voor correctie (burger) of terugmelding (professional). Op deze pagina kunnen de instellingen van de correctieservice worden beheerd.
Onderhouden status wijzigingsverzoeken (G040)	Deze autorisatie is bedoeld voor de medewerker(s) die zorgt voor de afhandeling van de elektronische correctieverzoeken en terugmeldingen.
RDW (G020)	Deze pagina toont het actueel voertuigbezit. Er zijn gegevens opgenomen over het merk, het type, het jaar van toelating etc. Met deze gegevens kan de waarde van het voertuig bepaald worden.
RDW peildata (R454)	Deze pagina bevat dezelfde gegevens als de pagina RDW maar u kunt binnen een bepaalde periode in het verleden zoeken naar het voertuigbezit.
RDW+ (R1919)	Deze pagina bevat dezelfde gegevens als de pagina RDW, aangevuld met de verzekeringsgegevens.
SBR query	Op basis van zoekgegevens kunt u query’s maken op de gegevens in SBR voor specifieke doelgroepen. Let op: Deze pagina verschijnt niet in de navigatie aan de linkerkant, maar op de homepage onder “overzichten”.
Terugvordering en verhaal	Een overzichtspagina met relevante procesgerichte informatie uit verschillende bronnen speciaal bedoeld voor medewerkers met de taak terugvordering en verhaal. Autorisatie mag niet i.c.m. Klant Algemeen+. Let op: Dit is een risicovolle autorisatie. Advies: zeer beperkt toekennen.
UWVWb (G003)	Het kolomoverzicht UWVWb (voorheen CWI) bevat alle informatie van UWV Werkbedrijf zoals persoonsgegevens, inschrijfgegevens, arbeidsinformatie en dienstverlening.
werk.nl (G026)	Is een hyperlink naar de webpagina werk.nl.
Zoek in BRP (G18)	Door geboortedatum, postcode en huisnummer in te voeren, kunt u een persoon traceren in de GBA. Dit is een risicovolle autorisatie, advies: zeer beperkt toekennen.
Zoek in kadaster	Zoeken via kadastrale aanduidingen of via locatie (adres). Zoeken is mogelijk met meerdere zoeksleutels, bijvoorbeeld Perceelnummer of KvKnummer. Let op: Dit is een risicovolle autorisatie, advies: zeer beperkt toekennen.
Zoek in RDW	Via de zoeksleutels BSN, kenteken, naam, adresgegevens en KvK-nummer kan de gebruiker voertuigen uit heden en verleden opzoeken. De getoonde gegevens komen overeen met de pagina RDW. Let op: Dit is een risicovolle autorisatie, advies: zeer beperkt toekennen.
Zoek in RDW+	Via de zoeksleutels BSN, kenteken, naam, adresgegevens en KvK-nummer kan de gebruiker voertuigen uit heden en verleden opzoeken. De getoonde gegevens komen overeen met de pagina RDW+. Let op: Dit is een risicovolle autorisatie. Advies: zeer beperkt toekennen.

Zoek+ in BRP	Zoeken via meerdere zoeksleutels, zoals geboortedatum, postcode, huisnummer, achternaam en geslacht. Let op: Dit is een risicovolle autorisatie, advies: zeer beperkt toekennen.

4.2. Geoorloofd gebruik

Suwinet-Inkijk mag alleen gebruikt worden voor het raadplegen van cliëntgegevens/ informatie conform onderstaande. Wordt Suwinet om andere redenen gebruikt, dan is er in principe sprake van ongeoorloofd gebruik.

Suwinet gebruik is toegestaan bij:

a. aanvragen WWB, IOAW, IOAZ, Bbz;
b. tussentijdse onderzoeken (zowel rechtmatigheids- als doelmatigheidsonderzoeken);
c. debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen, werkgever;
d. afhandeling maandelijkse signalen Inlichtingen Bureau (IB);
e. raadplegen ten behoeve van arbeidsmarkttoeleiding c.q. re-integratie.
f. raadplegen van Suwinet in het kader van voortijdig schoolverlaten door RMC medewerkers uit het samenwerkingsverband Regio meld- en Coördinatiepunt Oost Groningen. Hiervoor is tussen het UWV en de gemeente Veendam op 15 december 2015 een aanvullend addendum op de reeds bestaande overeenkomst uit 2015 opgesteld.

4.3. Beveiligingseisen bij het aannemen van personeel

Dit beveiligingsplan is op iedereen binnen de gemeente van toepassing die gebruik maakt van Suwinet-Inkijk. Alle gebruikers, ook nieuwe medewerkers, krijgen de beveiligingsregels (= dit beveiligingsplan) via de leiding. De individuele gebruikers worden op de afdeling geïnstrueerd over de correcte omgang met Suwinet.

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 leidinggevende wordt gecommuniceerd met de betreffende medewerker(s).

4.4. Vast personeel

Vast personeel van de gemeente Stadskanaal legt bij of kort na indiensttreding een eed of belofte af. De ambtenaar die toegang krijgt tot Suwinet-inkijk tekent daarnaast bij indiensttreding een "Formulier Autorisatie SUWI " (bijlage 1). Dit houdt in dat vertrouwelijke informatie die de ambtenaar in zijn/haar werk krijgt, alleen voor dat werk gebruikt mag worden.

Het personeel dat al in dienst was voordat het afleggen van de eed of belofte is ingevoerd heeft een schriftelijke verklaring wat betreft de eed of belofte ondertekend op grond van de Nota Integriteit van 29 april 2004.

De verklaringen met betrekking tot eed of belofte en de autorisatieformulieren SUWI worden in het personeelsdossier opgenomen.

4.5. Tijdelijk personeel

Medewerkers zonder ambtelijke status moeten ook een schriftelijke verklaring wat betreft de eed of belofte tekenen. Krijgt de tijdelijke medewerker ook toegang tot Suwinet-inkijk dan wordt ook een "Formulier Autorisatie SUWI " getekend.

Hoofdstuk 5 Controle op gebruik

5.1. Bureau Keteninformatisering Werk en Inkomen (BKWI)

5.1.1. Logging gegevens

Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker 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 burgerservicenummer 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.

5.1.2. Rapportage

Het aanvragen van een rapportage gaat uit van de zogenaamde security-officer in nauwe samenspraak met de applicatiebeheerder. De aanvraag wordt gedaan bij de helpdesk van het Inlichtingenbureau (IB), dus niet bij het BKWI. De gemeenten hebben al contacten met het IB vanwege de samenloopgevallen. Het BKWI doet echter de logging en maakt de rapportages. Het BKWI heeft standaardrapportages ontwikkeld omtrent de logging van het gebruik van Suwinet-Inkijk. Daarnaast kan de gemeente vragen om specifieke rapportages, bijvoorbeeld naar aanleiding van incidenten.

De zogenoemde logging-gegevens betreffen:

1. Inkijkacties.
2. Opvragingen unieke BSN nummers.
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.

<u>Periodiek terugkerende acties</u>

1. *De security officer van Suwinet vraagt een keer per kwartaal een standaard BKWI-rapportage op in het kader van de beveiliging. Aan de hand van deze rapportage wordt desgewenst een specifieke rapportage opgevraagd. De specifieke rapportage moet minimaal 1 keer per kalenderjaar worden opgevraagd.*
2. *De security officer vergelijkt wanneer er een specifieke rapportage is opgevraagd de geraadpleegde sofinummers in Suwinet met de sofinummers van de inwoners van de gemeente Stadskanaal.*
3. *De security officer bespreekt de standaard/ en specifieke rapportage met de applicatiebeheerder Suwinet.*
4. *Bij onregelmatigheden licht de security-officer de verantwoordelijke leidinggevende in.*
5. *De leidinggevende spreekt als hiertoe aanleiding bestaat met zijn/haar medewerker.*

5.2. Security-officer

De security-officer heeft de taak om de controle op de logging te vervullen. Hij/zij wordt formeel hiervoor door het college aangewezen. De security-officer is medeverantwoordelijk voor het opgestelde beveiligingsbeleid en heeft een rol in het vergroten van de bewustwording bij de medewerkers van het correct omgaan met informatie.

De security-officer monitort de uitvoering van het opgestelde beleid.
Hij/zij is degene die:

1. Onderzoekt of er een logische verklaring is voor geconstateerde afwijkingen. Bijvoorbeeld een overwerkactie, waardoor het Suwinet op tijdstippen buiten de normale kantooruren kan zijn gebruikt. Als alle aanwijzingen naar één medewerker wijzen, wordt het van groot belang te weten of de logincodes en wachtwoorden strikt persoonlijk worden gebruikt, ook de betrokken medewerker zal hierop bevraagd moeten worden. Blijken wachtwoorden uitgewisseld te zijn, dan zal het onderzoek zich moeten uitstrekken naar de degenen die zich mogelijk ook toegang tot Suwinet verschaft kunnen hebben.
2. Wanneer blijkt dat één of meerdere medewerkers doelbewust ongeoorloofd gebruik gemaakt hebben van hun bevoegdheid van toegang tot Suwinetgegevens, dan zal een disciplinaire maatregel volgen. Een en ander in nauw overleg met de leidinggevende waarmee een korte lijn noodzakelijk is.
3. De security-officer neemt deel aan het overleg over de jaarlijkse actualisatie van de informatiebeveiligingsplannen BRP en waardedocumenten en Suwinet, dat gaat over informatisering van de gehele gemeente Stadskanaal. Een vast agendapunt, dat in dit overleg ingebracht kan worden, is het Suwinet-gebruik.

5.3. Applicatiebeheerder

De applicatiebeheerder is specifiek een medewerker die uit hoofde van zijn/haar functie is aangewezen ten behoeve van onderhoud en exploitatie van de geautomatiseerde gedeeltes (software) van het Suwinet.

1. Bij eventuele beveiligingsincidenten of problemen op software gebied is de applicatiebeheerder meldpunt en aanspreekpunt voor de medewerkers. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak. Als de problemen niet gelijk op te lossen zijn, wordt het probleem doorgegeven aan de afdeling ICT die dan verder actie onderneemt. Wanneer het onvolkomenheden betreft in de standaard software op een werkplek, is de servicedesk van de afdeling ICT het eerste aanspreekpunt.
2. Beheren en uitgeven van wachtwoorden is de verantwoordelijkheid van de applicatiebeheerder. Een medewerker ontvangt eerst een account, nadat hij/zij het Formulier Autorisatie SUWI volledig heeft ingevuld en dit formulier is voorzien van de benodigde handtekeningen.
3. Zodra een medewerker de gemeente verlaat, verwijdert de applicatiebeheerder in opdracht van de leidinggevende het account. Hij krijgt hierover bericht van de afdeling ICT.
4. Wanneer een account langer dan 3 maanden niet wordt gebruikt zal de applicatiebeheerder dit account verwijderen. De betreffende gebruiker van wie zijn account is verwijderd zal een nieuwe aanvraag moeten doen en hij of zij zal de gehele aanvraagprocedure opnieuw moeten doorlopen.
5. De logginggegevens (zie hiervoor onder 5.1.1 en 5.1.2) worden door de applicatiebeheerder beoordeeld en voorgelegd aan de security-officer.

<u>Periodiek terugkerende acties</u>

1. *De applicatiebeheerder controleert een keer per kwartaal op verlopen accounts. Deze verlopen accounts moeten worden verwijderd.*
2. *De logginggegevens worden door de applicatiebeheerder in nauw overleg met de security-officer beoordeeld.*

5.4. Regulier overleg binnen de afdeling Maatschappelijke Zaken

Het overleg over het beveiligingsbeleid Suwinet is op de onderstaande wijze uitgewerkt.

Periodiek terugkerende acties

1. *Incidenteel overleg is afhankelijk van gebeurtenissen of zodra de security-officer of de applicatiebeheerder daartoe aanleiding ziet.*
2. *Periodiek overleg heeft plaats naar aanleiding van de BKWI-rapportage (per kwartaal; in het 4e kwartaal wordt het beveiligingsbeleid over het gehele kalenderjaar beoordeeld op correctheid en werking).*
3. *BKWI-rapportages worden voorgelegd aan het management als daar aanleiding toe is. Afhankelijk van de bevindingen zullen deze leiden tot verbetervoorstellen.*
4. *Specialistisch advies over informatiebeveiliging wordt ingewonnen indien noodzakelijk. Dit kan betekenen dat intern overlegd wordt met de afdeling ICT of dat externe specialisten worden ingehuurd.*

5.5. Externe audit

Op grond van artikel 5.22 van de Regeling SUWI over de opzet, het bestaan en de werking van de beveiliging van Suwinet moeten de Suwi-partijen jaarlijks rapporteren voor 15 maart. Deze rapportage moet zijn vergezeld van een oordeel en een rapport van bevindingen van een register edp-auditor. De audit betreft zowel een proces-audit als een technische audit.

Deze verplichting geldt (nog) niet voor de gemeente (zie ook onder 1.2). Op grond van audit-bevindingen zou de gemeente zich kunnen verantwoorden. In de Regeling SUWI is nog geen verplichting omschreven aan wie de gemeente moet rapporteren c.q. verantwoording schuldig is.

Hoofdstuk 6 Overige maatregelen

De maatregelen hieronder hebben betrekking op de werkplek, die voldoende beveiligd moet zijn tegen onbevoegden.

Periodiek terugkerende acties

a. *Een zogenaamde "clear desk policy" en "clear screen policy". Dit betekent dat de medewerkers zich er van bewust zijn dat op de werkplek geen dossiers, Suwinet uitdraaien e.d. mogen blijven liggen, als zij deze verlaten.*

b. *Vertrouwelijke gegevens gaan op de werkplek in de bak, die bestemd is voor oud papier. Dit papier wordt vervolgens dagelijks naar de papiercontainer gebracht. Deze ruimte is alleen toegankelijk voor ambtenaren. Een gecontracteerd bedrijf haalt de volle containers op en versnippert het papier.*

c. *Het "Privacyreglement e-mail-, internet- en telefoongebruik" van de gemeente hanteren over hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek.*

d. *Aanspreken van onbekende personen als een medewerker van de afdeling iemand in de gang van de afdeling tegenkomt waar officieel geen publiek zonder begeleiding mag komen. De medewerker dient 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 hen beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naar toe te begeleiden.*

e. *Gegevensverstrekking aan derden via de telefoon bij uitzondering. Het brengt het risico 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 een schriftelijk verzoek worden ingediend, voorzien van een machtiging. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker altijd teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven als het verzoek afkomstig van een vaste, bekende contactpersoon.

6.1. Inzage en correctie

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

Klanten hebben het wettelijke recht om hun dossier in te zien. Als een klant ziet dat er iets niet klopt in zijn gegevens kan hij met zijn Digid bij het Digitaal Klant Dossier (DKD) een (digitaal) verzoek tot correctie insturen. Het DKD is raadpleegbaar via www.mijnoverheid.nl of www.werk.nl. Wanneer voor een gegeven geen digitaal correctieverzoek kan worden verstuurd, staat aangegeven waar de klant zich kan melden.

Werkwijze bij een correctieverzoek
1. Een burger dient een correctieverzoek in voor de gegevens over hem/haar opgenomen in het DKD of een ketenpartner doet mededeling over een geconstateerde afwijking tussen één of meerdere gegevens opgenomen in DKD en de gegevens waarvan men kennis heeft of kennis heeft gekregen.

2. De terugmelding of het correctieverzoek worden middels een beveiligd e-mail bericht ontvangen door de daartoe aangewezen medewerker van de afdeling Maatschappelijke Zaken.

3. Naar aanleiding van een correctieverzoek of terugmelding wordt overgegaan tot een onderzoek. De daartoe aangewezen medewerker van de afdeling Maatschappelijke Zaken is verantwoordelijk voor de afhandeling van de terugmelding.

4. De burger, die een correctieverzoek heeft ingediend, of de ketenpartner, die een terugmelding heeft gedaan, wordt zo spoedig mogelijk doch binnen zeven werkdagen na de ontvangst hiervan in kennis gesteld of naar aanleiding van het verzoek of de terugmelding gegevens in DKD zijn verbeterd, aangevuld of verwijderd. Ook de afwijzing van zijn/haar correctieverzoek wordt de burger binnen zeven werkdagen meegedeeld.

5. Blijkt uit het onderzoek dat het gegeven of de gegevens verbeterd, aangevuld of verwijderd moeten worden dan zorgt de daartoe aangewezen medewerker dat hieraan uitvoering wordt gegeven.

Bijlage 1: Formulier Autorisatie SUWI

Formulier Autorisatie SUWI

Gelieve deze kolom in te vullen

Naam applicatie	
Organisatie onderdeel	
Personeelsnummer	
Voorletters	
Achternaam	
Functie	
Waarvoor wilt u de applicatie gebruiken	
Gevraagde standaardautorisatie	
Eventueel gevraagde extra gegevens buiten de standaardautorisatie	
Aanvrager is bewust van het feit dat hij/zij werkt met vertrouwelijke privacygevoelige informatie en verklaart dat de informatie waartoe zij/hij toegang heeft uitsluitend zal worden gebruikt voor werkzaamheden die zij/hij uit hoofde van haar/zijn functie nodig heeft en deze niet aan derden door zal geven.	Stadskanaal:…….(datum) Handtekening:……
Accordering leidinggevende gebruiker.	Stadskanaal:…….(datum) Handtekening:……
Accordering informatiebeheerder.	Stadskanaal:…….(datum) Handtekening:…….
Gewenste autorisatie op systeemniveau aangebracht door de systeembeheerder.	Stadskanaal:…….(datum) Handtekening:…….
Gewenste autorisatie op applicatieniveau aangebracht door de applicatiebeheerder van de afdeling Maatschappelijke Zaken.	Stadskanaal:…….(datum) Handtekening:…….

Bijlage 2: Controleplan BRP / Suwinet audit

Datum test	Verwijzing naar Informatie beveiligingsplan	**Te testen maatregelen**	**Bevindingen**
	4. Diefstal, sabotage, virussen en fraude	- De kritische ruimten zijn afdoende beveiligd. Dit betreft (volgens het beveiligingsplan) de volgende ruimten: * Computerruimte * Werkplekken afdeling Maatschappelijke Zaken * Spreekkamers A22 * Applicatiebeheerders Afdeling Dienstverlening	
	5. Onbevoegd gebruik	- Richtlijnen en voorschriften voor het aanvragen, wijzigen en intrekken van autorisaties.	
		- Registratie en bijhouding van de gebruikers en de aan hen individueel verleende bevoegdheden, alsmede het daarvan periodiek (minimaal eens per jaar) rapporteren aan de manager van de afdeling Maatschappelijke Zaken	
		- De richtlijnen en procedures voor logische informatiebeveiliging met betrekking tot de BRP applicatie. Deze omvatten o.a. voorschriften voor het aanvragen, wijzigen en intrekken van autorisaties en voor het registreren en controleren van deze werkzaamheden.	
		Conform hoofdstuk 5 van het beveiligingsplan Suwinet: - Registratie en bijhouding van de gebruikers op Suwinet die werkzaam zijn in het primaire proces en de aan hen individueel verleende autorisaties - Eens per halfjaar beoordelen van de BKWI-rapportage. Calamiteiten worden aan het management gemeld. - Vodu tijdig d.w.z. vóór 28 februari van enig kalenderjaar aangeleverd.	
		- Elke medewerker heeft een individueel bevoegdheidsprofiel dat is toegesneden op de taak en functie.	
		- Autorisatie voor de BRP-gegevens gebeurt via een door het bevoegde gezag vastgestelde procedure binnen de kaders van de privacy verordening van het BRP.	

Datum test	Verwijzing naar Informatie beveiligingsplan	**Te testen maatregelen**	**Bevindingen**
		- Alle gebruikers zijn verplicht tot het gebruiken van een individueel user ID. Een user ID is een identificatie van de gebruiker. Het wachtwoord dient ter controle van de authenticiteit van de gebruiker.	
		- De gebruikers en de aan hen verleende bevoegdheden worden geregistreerd. Het verlenen, wijzigen en intrekken van de bevoegdheden vindt plaats aan de hand van een formele procedure waarbij deze activiteiten schriftelijk worden vastgelegd.	
		- De applicatiebeheerder draagt de zorg voor registratie en autorisatie van de gebruikers van de vitale BRP applicaties en Suwinet (Inkijk).	
		- Alle BRP- en Suwinetgebruikers zijn verplicht tot het gebruik van een individueel user ID en wachtwoord, ook voor het netwerk.	
		- Alle BRP gebruikers, rechtstreeks, via DDS en Suwinet, worden regelmatig, minimaal eenmaal per jaar, geïnstrueerd over bevoegd gebruik en het feit dat elk gebruik wordt geprotocolleerd t.b.v. burger zelf.	
		- De wachtwoorden op de server, het netwerk en de applicaties voldoen aan de eisen van de code voor informatie beveiliging. - Dat zijn de volgende eisen: * BRP- en Suwinetwachtwoord kent tenminste 6 posities * geldigheidstermijn van hooguit 60 dagen * het nieuwe wachtwoord verschilt op tenminste vier posities met de drie voorgaande wachtwoorden * na het ingeven van drie foute wachtwoorden wordt een blokkering toegepast * het wachtwoord is door geen enkele gebruiker op te vragen	

Datum test	Verwijzing naar Informatie beveiligingsplan	**Te testen maatregelen**	**Bevindingen**
		- De wachtwoorden en user ID t.b.v. het BRP en Suwinet worden alleen aan individuele personen verstrekt. - Toegang tot het BRP en Suwinet is alleen mogelijk na persoonlijke identificatie. - De verstrekte persoonlijke identificaties tot het BRP- en Suwinetsysteem wordt periodiek gecontroleerd op geldigheid en actualiteit. - Van deze activiteit is een controle verslag actualisaties opgesteld.	
		- Alle gebruikers en de aan hen verleende bevoegdheden worden geregistreerd en de gebruikersprofielen van personen die niet meer werken bij de gemeente Stadskanaal worden verwijderd.	
		- Bij eventuele beveiligingsincidenten of problemen op Suwinet gebied is de applicatiebeheerder meldpunt en aanspreekpunt voor de medewerkers. Wanneer het onvolkomenheden betreft in de standaard software op een werkplek, is de servicedesk van automatisering (OGD) het eerste aanspreekpunt.	
	6. Beschikbaarheid	- De gegevens op de bedrijfskritische server worden eens per werkdag gekopieerd naar een verwijderbare gegevensdrager zoals een back-up tape.	
		- De dagelijkse back-up en de periodieke (wekelijkse) back-up worden opgeslagen in een beveiligde ruimte buiten het gemeentehuis. Dit gebeurt in het bedrijfsverzamelgebouw A22 aan de Aziëlaan 22.	
		- Er is een geldig en actueel extern uitwijk contract afgesloten - Er is een uitwijkprocedure opgesteld voor het besluitvormings traject dat aan de uitwijk voorafgaat en de organisatorische en administratieve afwikkeling daarvan.	

Datum test	Verwijzing naar Informatie beveiligingsplan	**Te testen maatregelen**	**Bevindingen**
		- De uitwijkprocedure en de uitwijkvoorziening wordt periodiek (jaarlijks) getest teneinde ervan verzekerd te zijn dat die procedure en de voorziening in de praktijk ook daadwerkelijk naar behoren functioneert .	
		- Er is een gemeentelijk uitwijkteam geformeerd.	
		- De brondocumenten worden minimaal vijf werkdagen in een afsluitbare kast in een beveiligde ruimte bewaard.	
		- Er zijn dusdanige beschikbaarheidvoorzieningen getroffen dat gewaarborgd is dat de uitvalduur van de informatievoorziening van de kritische bedrijfsprocessen, waaronder het BRP, niet langer dan 48 uur bedraagt.	
		- Voor de applicatie BRP is een herstelprocedure gemaakt die jaarlijks wordt beproefd door de applicatiebeheerder. Deze procedure bewerkstelligt dat binnen maximaal 24 uur nadat het BRP systeem weer in de lucht is alle mutaties zijn gereconstrueerd. Hierdoor is de gemeente Stadskanaal na maximaal 48 uur zowel technisch als organisatorisch als qua gegevens weer compleet.	
		- Tenminste eenmaal per jaar wordt een volledige systeemback-up gemaakt. Deze systeemsave wordt altijd voorafgaand aan en na afloop van een wijziging van het besturingssysteem uitgevoerd. De laatste systeemback-up wordt op een externe en beveiligde locatie opgeslagen, namelijk in een kluis in het bedrijfsverzamelgebouw A22. Tevens wordt de eerstvolgende weeksave (systeemsave) bewaard in het bedrijfsverzamelgebouw A22 te Stadskanaal.	

Datum test	Verwijzing naar Informatie beveiligingsplan	**Te testen maatregelen**	**Bevindingen**
		- Er is een medewerker aangewezen die verantwoordelijk is voor het beheer van de afgesloten verzekeringen. - De verzekeringbeheerder draagt zorg voor de verzekering van de standaard risico's zoals: * brand, * diefstal en inbraak * de beperking van de financiële gevolgen van aansprakelijkheid. * de beperking van de bedrijfsvoeringschade na het optreden van een calamiteit.	
	7. Personeel	- Er wordt onder verantwoordelijkheid van de manager van de afdeling Maatschappelijke Zaken een adequate functiescheiding toegepast. Dit om het risico van nalatigheid en opzettelijk misbruik te verminderen. Daarbij is aandacht besteed aan de werkzaamheden: * gegevensinvoer * systeem- en netwerkbeheer * administratieve controle op de beveiliging.	
		- De security-officer heeft de taak om de controle op de "logging" te vervullen. Hij/zij wordt formeel hiervoor door het bestuur van de gemeente Stadskanaal aangewezen. De security-officer is medeverantwoordelijk voor het opgestelde beveiligingsbeleid en heeft een rol in het vergroten van de bewustwording bij de medewerkers van het correct omgaan met informatie.	