Gemeente Westvoorne

GEMEENTEBLAD

Officiële uitgave van de gemeente Westvoorne

Nr. 515266

23 november

2022

Informatiebeveiligingsplan Suwinet 2014

1. Inleiding

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

Algemeen
De huidige techniek maakt het mogelijk om allerlei gegevens op te slaan in databases en deze aan elkaar te koppelen. Daardoor zijn de gegevens niet alleen binnen de eigen organisatie te raadplegen maar kunnen ook persoons- en uitkeringsgegevens worden geraadpleegd die zijn vastgelegd in de databases bij andere organisaties. Omgekeerd kunnen andere organisaties een deel van de bij het team Werk en Inkomen geregistreerde gegevens inzien. Dit is mogelijk met Suwinet.

De wetgever streeft daarbij een klantvriendelijke benadering na. Voorkomen moet worden dat de cliënt steeds weer dezelfde informatie moet verstrekken bij de verschillende uitkeringsinstanties. Het is daarom niet alleen mogelijk gegevens van andere organisaties in te zien en te gebruiken, maar het is zelfs een verplichting.

Voor het bereiken van bovenstaande doelstellingen is landelijk het Digitaal Klantdossier (DKD) ingevoerd en vanaf 1 januari 2008 is de Wet eenmalige gegevensuitvraag werk en nkomen (WEU) van kracht. Centraal daarbij staat het Burgerservicenummer (BSN) van de personen op wie de gegevens betrekking hebben. Gegevens van cliënten worden aan de hand van het BSN met elkaar in verband gebracht. Suwinet en het DKD zijn uitsluitend toegankelijk voor de medewerkers die zich bezighouden met de uitvoering van de WWB, IOAW, IOAZ, Bbz. Suwinet mag (nog) niet gebruikt worden voor andere doeleinden, zoals de uitvoering van de Wet kinderopvang, Schuldhulpverlening, kwijtschelding gemeentelijke belastingen en Wet Maatschappelijke Ondersteuning.

Het DKD maakt klantgegevens ketenbreed beschikbaar zodat:
- Gegevens nog maar één keer hoeven te worden uitgevraagd en vastgelegd;
- De ketendienstverlening kan worden verbeterd omdat UWV, SVB en gemeenten een completer beeld van een cliënt hebben.

Daarnaast biedt het DKD burgers de mogelijkheid om een deel van hun door de ketenpartners vastgelegde gegevens te raadplegen via internet en om gebruik te maken van elektronische diensten (zoals aanvragen van uitkeringen).

De aangesloten ketenpartners, waaronder de gemeenten, moeten volgens de WEU elkaars gegevens (her)gebruiken en mogen niet langer gegevens van of aan de cliënt vragen als deze als via het DKD zijn te verkrijgen.

Omdat het hier de uitwisseling van zeer privacygevoelige informatie betreft moeten de uitvoerende instanties hier dan ook zeer zorgvuldig mee omgaan. Daarom bepaalt art. 6.4 van de Regeling SUWI dat alle Ketenpartners over een deugdelijk beveiligingsplan moeten beschikken.

Uitvoering en evaluatie
Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt. De basis hiervoor is het Beveiligingsplan.

Daarnaast moet door de security officer worden vastgesteld of de maatregelen door de medewerkers worden nageleefd en het verdient aanbeveling om minimaal eenmaal per jaar het beleid te evalueren en zo nodig te herzien.

Het voorliggend Beveiligingsplan bevat ook een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden bezien op actualiteit. In het Beveiligingsplan is daarom de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen in procedures

geregeld. Belangrijk in dit verband is dat het Beveiligingsplan jaarlijks opnieuw wordt bekeken op actualiteit en jaarlijks vastgesteld wordt door het College van B&W.

Rolverdeling en bijbehorende verantwoordelijkheden
In deze paragraaf wordt beschreven wie welke rol heeft in de informatiebeveiliging.

- College van B&W: Is bestuurlijk verantwoordelijk voor de informatieveiligheid, stelt het beleid vast en draagt het uit. Het College informeert de Raad, zodat die zijn controlerende taak kan waarmaken.
- De lijnmanager is (primair) verantwoordelijk voor de bedrijfsvoering van het betreffende gemeentelijke proces waar informatieveiligheid een integraal onderdeel van is.
- De Chief Information Security Officer (CISO): is belast met de gemeentelijke informatieveiligheid en heeft een onafhankelijke staffunctie.
- De functioneel beheerder beheert de gebruikersadministratie van Suwinet.

Een uitgebreide taakbeschrijving van de Security Officer is opgenomen in de bijlage 'Taakbeschrijving Security Officer'.

Overlegstructuur
Informatiebeveiliging is uitermate belangrijk voor het werk binnen de gemeente waar veelvuldig met privacygevoelige informatie wordt gewerkt en dit hoort dan ook bij de professionele en bekwame uitvoering van het werk. Er moet daarom ruim aandacht worden besteed aan de communicatie rond informatiebeveiliging en wel op zodanige wijze dat de informatiebeveiliging ook echt gaat leven bij de medewerkers. Dit onderwerp zal in ieder geval bij de volgende overlegmomenten aan de orde komen:
1. Eens per half jaar tijdens het periodiek werkoverleg als vast agendapunt;
2. Bij het individueel werkgesprek en voortgangsgesprekken;

en verder;
3. Verzorgt de security officer ten minste eenmaal per jaar het geven van voorlichting en instructie aan medewerkers d.m.v. toetsing van de opgestelde beveiligingsprocedures in de praktijk;
4. Worden nieuwe medewerkers door de Security Officer bekendgemaakt met de beveiligingsprocedures;
5. Vindt jaarlijks een evaluatie plaats van het beveiligingsplan;
6. Aanbieding van het geactualiseerde Beveiligingsplan ter vaststelling aan het College van B&W.

De punten 1 en 2 zijn nader uitgewerkt in de bijlage "Procedure communicatie over beveiliging". Het gestelde onder 3 en 4 behoort tot het takenpakket van de security officer.

Jaarlijkse actualisering
Het beveiligingsplan en de beveiligingsmaatregelen worden jaarlijks geëvalueerd en eventueel bijgesteld. De security officer stelt hiervan een verslag op en biedt dit met een eventueel geactualiseerd beveiligingsplan aan ter vaststelling door het College van B&W.

Bij de jaarlijkse evaluatie geconstateerde afwijkingen worden schriftelijk vastgelegd en 5 jaar bewaard bij het Beveiligingsplan. Op de eventueel geconstateerde tekortkomingen of problemen wordt actie ondernomen.

2. Inventarisatie software en beveiligingsmaatregelen

Inleiding
Het team Werk, Inkomen & Service maakt gebruik van een aantal applicaties. In deze applicaties worden gegevens geregistreerd, welke kunnen worden geraadpleegd. Per applicatie is het nodig het gewenste beveiligingsniveau te benoemen. Hierop kunnen vervolgens maatregelen worden afgestemd.

De zijn diverse applicaties zijn in gebruik, waaronder:
1. Suwinet;
2. GWS4all (inclusief Suite4Werk);
3. Module documentenuitvoer (Doc4all);
4. Module documentenuitvoer (MDU);
5. Outlook, Word en Excel.

In dit hoofdstuk wordt alleen de applicatie Suwinet nader besproken. De applicaties genoemd onder nummer 2 t/m 5 worden onderhouden door Syntrophos (gemeenschappelijke regeling ICT Voorne-Putten). Om deze applicaties te kunnen gebruiken hebben we een aparte toegangstoken waarmee we

op het netwerk van gemeente Spijkenisse kunnen inloggen. De beveiliging van deze applicaties is ondergebracht bij de gemeenschappelijke regeling Syntrophos.

De modules documentenuitvoer (Doc4all en MDU) zijn documentengenerators die aansluiten op Word en GWS4all, waardoor vanuit GWS4all rapportages, beschikkingen, brieven, ed. kunnen worden vervaardigd en geraadpleegd.

Applicatie Suwinet
Het Suwinet kent verschillende functionaliteiten, te weten:
- Een raadpleegfunctie (Suwinet);
- Het uitwisselen van gegevens, de samenloopapplicatie;
- Suwinet-Mail;
- Het Digitaal Klant Dossier.

Suwinet
Geautoriseerde medewerkers van de gemeente, het UWV en de SVB kunnen online elkaars gegevens raadplegen. Daarnaast kunnen de gemeenten putten uit gegevens van het Kadaster, toeslagen van de Belastingdienst, Dienst Uitvoering Onderwijs (DUO), Rijksdienst voor het Wegverkeer (RDW) en het Bedrijvenregister.

Beveiliging: In Suwinet zijn zeer privacygevoelige gegevens verzameld. De toegangsverlening tot Suwinet is geregeld in het hoofdstuk Toegangsrechten en autorisatiebeheer en in de bijlage "Procedure autorisaties".

Samenloopapplicatie
Maandelijks levert elke gemeente haar actuele uitkeringenbestand aan bij het Inlichtingenbureau. Via deze instantie worden de gegevens vergeleken met de gegevens van het UWV, de Belastingdienst, de Dienst Uitvoering Onderwijs (DUO – IB Groep), Justitie (detentie). Bij samenloopgevallen wordt een signaal naar de gemeente gestuurd, die vervolgens een onderzoek kan instellen naar mogelijke fraude.

Beveiliging: Het aan te leveren bestand wordt maandelijks samengesteld door de Administratie van team WIS, die het bestand vervolgens naar het Inlichtingenbureau verzendt via de beveiligde site van het Inlichtingenbureau. Terugkoppeling van gegevens gaat eveneens via deze site.

Suwinet Mail
Dit is een beveiligde mailfunctionaliteit. Hiermee kan privacygevoelige informatie tussen Sociale Diensten, het UWV en de SVB worden uitgewisseld.

Beveiliging: Naast het feit dat Suwinet-Mail eenvoudig in gebruik is, worden de risico's die zijn verbonden aan het mailen van klantgegevens aanzienlijk verkleind doordat het via een besloten netwerk plaatsvindt.

DKD
Het Digitaal Klant Dossier is een onderdeel van Suwinet. Het is een elektronisch dossier waarin gegevens zijn opgeslagen van het UWV, SVB, RDW en de gemeenten.

Vanuit het Digitaal Klantdossier is een groot aantal gegevenselementen uit GWS via webservice te raadplegen. Deze gegevens zijn ca. 24 uur per dag raadpleegbaar, ook in het weekend. Hiermee wordt voldaan aan de verplichting om 7 dagen per week minimaal 20 uur per dag raadpleegbaar te zijn.

De ketenpartners kunnen de gegevens in het DKD raadplegen en (her)gebruiken. Hierdoor hoeven de cliënten voortaan maar eenmaal gegevens aan te leveren; de cliënt kan zijn gegevens zelf ook bekijken. Hij ziet niet alle informatie die medewerkers van de ketenpartners te zien krijgen, maar een deel ervan. Deze gegevens vindt hij in het z.g. klantbeeld; de klant logt hierop in met zijn DigiD code en zijn Burgerservicenummer. Ook kan hij gebruik maken van elektronische diensten, zoals correctieservice en digitale aanvragen.

Het DKD verkeert in een groeiproces en zal steeds verder uitbreiden. Steeds meer partners zullen erop worden aangesloten, zoals DUO, de Belastingsdienst, Zorgverzekeraars, Onderwijs, Justitie en de sector Zorg en Wonen.

Beveiliging: Het DKD is een onderdeel van Suwinet. Hiervoor zijn geen aanvullende maatregelen noodzakelijk. De continue gegevensoverdracht vanuit GWS4all loopt via een speciaal hiervoor aangewezen beveiligde lijn.

3. Beveiligingseisen medewerkers

Vast personeel
Binnen het team Werk, Inkomen & Service wordt met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens heeft de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI zijn geheimhoudingsbepalingen opgenomen, waarin is bepaald dat de persoonsgegevens niet verder bekend gemaakt mogen worden dan voor de uitoefening van de functie noodzakelijk is. Bovendien wordt in artikel 125a van de Ambtenarenwet geheimhouding opgelegd aan ambtenaren.

Nieuwe medewerkers moeten een Verklaring omtrent het Gedrag overleggen voordat ze definitief worden benoemd. Daarnaast is het afleggen van de eed/gelofte ingevoerd.
In de vastgestelde nota "Gedragscode integriteit voor ambtenaren" en het "Privacyreglement email en internetgebruik" is de geheimhoudingsplicht en het zorgvuldig omgaan met informatie gemeentebreed geregeld. Deze nota's zijn van toepassing op het personeel dat in dienst is van de gemeente Westvoorne. De medewerkers met een autorisatie voor Suwinet moeten daarnaast een zorgvuldigheidsverklaring ondertekenen.

Tijdelijk & extern personeel
Personeel dat werkzaamheden verricht bij de gemeente en niet in een ambtelijk dienstverband is benoemd krijgt geen toegang tot Suwinet.

Bewustwording medewerkers
Aan alle medewerkers van team Werk, Inkomen & Service (die gebruik maken van de Suwinet applicatie) is het Beveiligingsplan uitgereikt. Het plan is mondeling toegelicht. Gebruikers van Suwinet moeten weten dat over hen gegevens worden vastgelegd en verzameld (logging). Van deze loggegevens worden geanonimiseerde rapporten opgesteld door het Bureau Keteninformatisering Werk en Inkomen (BKWI). Aan de hand van deze rapporten controleren de Ketenpartners of er onjuist gebruik of misbruik is gemaakt van Suwinet. Als het vermoeden van ongeoorloofd gebruik van dat medium bestaat kan specifieke loginformatie bij het BKWI worden opgevraagd.

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

- Het bestaan van de logging-applicatie;
- De (aard van de) gegevens die worden verzameld;
- Doelen van de logging;
- Het gebruik van de gelogde gegevens; deze worden niet voor andere doeleinden gebruikt dan waarvoor ze zijn vastgelegd;
- De wijze en het moment waarop en door wie een onrechtmatig of doel overschrijdend gebruik van het Suwinet wordt geconstateerd;
- Dat bij bovenstaande constatering de Security Officer hierover contact opneemt met de betreffende medewerker(s).

In de bijlage "Procedure controle gebruik Suwinet" wordt nader ingegaan op de gelogde gegevens en de interne controle op rechtmatig gebruik van Suwinet. Aan het gebruik van de informatiesystemen is een aantal verplichtingen verbonden.

Instructie incidenten en storingen
Het is belangrijk dat beveiligingsincidenten worden gemeld bij de Security Officer of bij de lijnmanager, waarna een onderzoek wordt ingesteld naar eventuele gevolgen van het geconstateerde incident. Incidenten en het resultaat van het verrichte onderzoek worden besproken en gemeld aan de lijnmanager.

4. Fysieke beveiliging omgeving

Publieke ruimte
Persoonlijke cliëntcontacten vinden plaats in het gemeentehuis van Westvoorne. Bezoekers melden zich bij binnenkomst in het gemeentehuis bij de receptie. Zij hebben slechts onder begeleiding toegang tot de spreekruimten.

De spreekkamers zijn voorzien van een alarmknop. Er is een Agressieprotocol 2013 vastgesteld. De medewerkers die contact hebben met publiek hebben een agressietraining gevolgd.

Werkruimte
De werkruimte van de medewerkers is gehuisvest in het gemeentehuis. De werkruimten van het gemeentehuis zijn niet toegankelijk voor bezoekers, maar uitsluitend voor personen die in het bezit zijn van een toegangsbadge. Dat is het eigen personeel en ingehuurd externpersoneel. Daarnaast wordt aan medewerkers van onderhoudsbedrijven toegang verleendvoor het verrichten van onderhoudswerkzaamheden.

Opgeruimd bureau
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 kasten die na werktijd worden afgesloten.

Oud papier
Met vertrouwelijke gegevens, waaronder persoonsgegevens, moet zeer zorgvuldig worden omgegaan. Vertrouwelijke gegevens mogen niet terecht in een prullenbak of een bak die bestemd is voor oud papier. Het vernietigen van deze gegevens moet op een veilig manier plaatsvinden. Daarom is een speciale afgesloten papiercontainer geplaatst waarin het te vernietigen materiaal wordt verzameld. De inhoud van deze containers wordt regelmatig aangeleverd bij een vernietigingsbedrijf.

Schermbeveiliging
De PC schermen worden nadat er gedurende 30 minuten geen gebruik van is gemaakt automatisch vergrendeld en kunnen alleen door het ingeven van een wachtwoord weer worden geactiveerd. Bij het verlaten van de werkplek moeten de medewerkers direct de PC schermen vergrendelen.

Archiefruimten
Lopende cliëntendossiers worden bewaard in dossierkasten evenals cliëntendossiers die onlangs zijn afgesloten. Als er niemand aanwezig is gaan de dossierkasten op slot. De beëindigde cliëntendossiers worden na verloop van tijd verplaatst naar het archief. De beveiliging van archiefstukken is een taak van de gemeente op grond van de Archiefwet.

Printers
De printer staat binnen de afgesloten werkruimte van team Werk, Inkomen & Service. Er zwerven geen "vergeten" documenten rond. Mochten er toch uitgeprinte stukken achterblijven dan worden deze aan het einde van de dag in een afgesloten papiercontainer gedeponeerd.

5. Toegangsrechten en autorisatiebeheer

Beleid ten aanzien van autorisaties
Het gebruik van Suwinet is voorbehouden aan de medewerkers van team Werk, Inkomen & Service. De autorisaties voor Suwinet worden per medewerker per rol toegekend.

De Security Officer geeft aan, onder verantwoordelijkheid van de lijnmanager welke autorisaties een medewerker nodig heeft voor het uitvoeren van zijn taken.

De wijze waarop de autorisaties worden toegekend, gewijzigd of ingetrokken is nader geregeld in de bijlage "Procedure autorisaties".

Controle op het gebruik van Suwinet
Het Bureau Keteninformatisering Werk en Inkomen (BKWI) stelt rapportages op over de logging van het gebruik van Suwinet. Deze rapportages worden beschikbaar gesteld aan de betreffende Ketenpartners. Aan de hand hiervan wordt gecontroleerd op het gebruik van Suwinet en wordt geprobeerd een goed beeld te krijgen van de wijze waarop Suwinet door de medewerkers wordt geraadpleegd.

Bij een vermoeden van onjuist gebruik van dit medium kan specifieke informatie per onderdeel of per medewerker worden opgevraagd. De medewerkers die gebruik maken van Suwinet worden in kennis gesteld van het feit dat gegevens van hun raadpleegactiviteiten worden vastgelegd en dat deze gegevens worden gebruikt voor de controle op een rechtmatig gebruik van Suwinet. Deze controle is nader uitgewerkt in de bijlage "Procedure controle gebruik Suwinet".

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

Er vindt een periodieke controle plaats op het rechtmatig gebruik van Suwinet. In de bijlage “Procedure controle gebruik Suwinet” is de controleprocedure vastgelegd.

Alle autorisaties zijn vastgelegd in het Overzicht autorisaties. Het overzicht is te uitgebreid om onderdeel uit te maken van dit Beveiligingsplan. Bovendien vinden hierin regelmatig wijzigingen plaats. De Security Officer bewaart alle verzoeken om verstrekking, wijziging of intrekking van autorisaties.

De Security Officer controleert de actualiteit en de rechtmatigheid van de ingevoerde autorisaties t.o.v. de toegekende autorisaties en stelt het Overzicht autorisaties op. De Security Officer stelt een rapport op van de bevindingen van de autorisatiecontrole en rapport dit jaarlijks aan B&W.

7. Verzoek inzage dossier en correctie door cliënt en/of gemachtigde

Behalve de Ketenpartners kunnen ook cliënten hun gegevens raadplegen in het DKD (onderdeel van Suwinet). Om toegang tot hun gegevens te krijgen moeten zij inloggen met hun DigiD-code.

Als een cliënt een correctie van een bepaald gegeven wil kan hij hiertoe een verzoek indienen bij de Security Officer. In het DKD, waarin de gegevens worden geraadpleegd, is bij een aantal gegevens een digitale correctieservice opgenomen. Dat wil zeggen dat een cliënt rechtstreeks van uit het DKD een elektronisch correctieverzoek kan indienen. Desgewenst kan hij dit ook schriftelijk of mondeling doen. Bij de overige gegevens staat vermeld hoe een eventuele correctie kan worden aangevraagd.

Daarnaast kan een cliënt ook inzage vragen in zijn papieren bijstandsdossier; ook in dit geval kan hij om correctie van een bepaald gegeven verzoeken.