Gemeente Oude IJsselstreek

14uit27471

gemeente Oude IJsselstreek

Bezoekadres:
Staringstraat 25, Gendringen
Postbus 42
7080 AA Gendringen
Telefoon: (0315) 292 292
Fax: (0315) 292 293
E-mail: info@oude-ijsselstreek.nl
Internet: www.oude-ijsselstreek.nl

D66
t.a.v. fractie Oude IJsselstreek
Venus 13
7071 VE ULFT

Uw kenmerk:
Ons kenmerk: 14uit27471

Verzenddatum: 17 MRT 2014

Onderwerp: Schriftelijke vragen beveiliging Suwinet

Geachte mevrouw Van der Meer,

Op 10 februari heeft u ons vragen gesteld over de beveiliging van Suwinet. Dit naar aanleiding van het rapport 'de burger bediend in 2013'. In deze brief geven wij daar antwoord op.

Vragen D'66

1. Welke maatregelen heeft u genomen sinds het verschijnen van het rapport "De burger bediend in 2013? En hoever bent u daarmee?
2. Aan welke normen wordt nu voldaan?
3. Welke maatregelen heeft u vooruitlopend op het voldoen aan de normen genomen om de privacy van onze inwoners te waarborgen?
4. Wanneer verwacht u aan alle zeven te voldoen zoals beschreven in het rapport?
5. Kunnen wij van u een tijdspad verwachten met welke vervolgstappen u gaat nemen met een terugkoppeling over de voortgang.

Antwoorden college

1. In het in 2006 opgestelde en aangenomen beveiligingsplan ISWI zijn een reeks van algemene beveiligingsmaatregelen opgenomen ter beveiliging en gebruik van Suwinet. Na het verschijnen van het rapport "De burger bediend" heeft er bij het ISWI een inventarisatie plaats gevonden. Uit die inventarisatie bleek dat niet aan alle normen voor de beveiliging van Suwinet werden voldaan. Gedoeld werd dan vooral op het zeer frequent het personeel erop wijzen van het gebruik van Suwinet en de controle daarop. De oplossing voor de tekortkomingen is nu vastgelegd in een nieuw plan dat op 17 februari 2014 door het AB ISWI is vastgesteld en op 11 maart 2014 is vastgesteld door het college van Burgemeester en Wethouders. Dit plan vindt u als bijlage bij deze brief.

2/3/4/5 Bijgaand plan voorziet in de eisen die aan het gebruik van Suwinet-Inkijk worden gesteld.
De belangrijkste punten zijn:
1. het hebben van een beveiligingsplan
2. het instellen van een securityofficer en de taakomschrijving
3. het instellen van een overleggroep informatiebeveiliging
4. het vaststellen van de te volgen procedures
    a. autorisaties en applicatiebeheer
    b. controle gebruik Suwinet-Inkijk
    c. opvragen gegevens
    d. correctie gegevens
5. het uitdragen van het beveiligingsplan binnen de organisatie
6. jaarlijkse evaluatie van het beveiligingsbeleid.

Ingevolge de wet Suwi zijn de ketenpartners verantwoordelijk voor het gebruik en misbruik van Suwinet-Inkijk. Hoewel het ISWI een gebruiker is van Suwinet-inkijk, is volgens de wet de gemeente verantwoordelijk voor de beveiliging van Suwinet. In geval van een intergemeentelijk samenwerkingsverband dient het plan eveneens door de colleges van de deelnemende gemeenten te worden vastgesteld.

Er wordt met het voorliggende plan aan alle normen voldaan.

Met vriendelijke groet,
burgemeester en wethouders,

Mevrouw G.H. Tamminga
secretaris

De heer J.P.M. Alberse
burgemeester

14int00175

ISWI

Aalten

Oude IJsselstreek

Intergemeentelijk Samenwerkingsverband Werk en Inkomen

Beveiligingsplan Suwinet-Inkijk

Intergemeentelijk samenwerkingsverband ISWI
Januari 2014

Inhoudsopgave

Bijlagen

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-Inkijk.

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 inkomen (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-Inkijk en het DKD zijn uitsluitend toegankelijk voor de medewerkers die zich bezighouden met de uitvoering van de WWB, IOAW, IOAZ, en Bbz.
Suwinet-Inkijk mag (nog) niet gebruikt worden voor andere doeleinden, zoals de uitvoering van de Wet kinderopvang, de Schuldhulpverlening 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 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. Binnen de organisatie moeten medewerkers verantwoordelijkheden krijgen voor het uitvoeren van dit plan. De medewerkers worden tijdens het werkoverleg betrokken bij de ontwikkeling en implementatie hiervan.

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 dat de wijzigingen worden vastgesteld door het Dagelijks Bestuur.

Rolverdeling en bijbehorende verantwoordelijkheden

In deze paragraaf wordt beschreven wie welke rol heeft in de informatiebeveiliging. Het is natuurlijk mogelijk dat rollen elkaar overlappen.

Beheer en onderhoud van het beveiligingsplan:
Verantwoordelijk: directeur ISWI
Uitvoerend: security officer

Controle op uitvoering beveiligingsplan:
Security officer

Bevorderen informatiebeveiliging:
Security officer

Evaluatie van het beveiligingsplan:
Security officer

Een uitgebreide taakbeschrijving van de security officer is opgenomen in een bijlage.

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:

a. Eens per kwartaal tijdens het periodiek werkoverleg als vast agendapunt;
b. Bij individuele- en functioneringsgesprekken;

en verder;

c. 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;
d. Worden nieuwe medewerkers door de security officer bekendgemaakt met de beveiligingsprocedures;
e. Vindt jaarlijks een evaluatie plaats van het beveiligingsplan door de overleggroep informatiebeveiliging;
f. Aanbieding van het geactualiseerde Beveiligingsplan ter vaststelling aan het Dagelijks Bestuur

.

De punten a en b zijn nader uitgewerkt in de bijlage "Procedure communicatie over beveiliging". Het gestelde onder c en d behoort tot het takenpakket van de security officer. Voor de punten e en f zie hieronder.

Overleggroep Informatiebeveiliging

Voor de totstandkoming van en periodieke afstemming (minimaal eenmaal per jaar) over voorliggend Beveiligingsplan is een overleggroep Informatiebeveiliging ingesteld.
Deze overleggroep Informatiebeveiliging bestaat uit de volgende functies:

- Directeur ISWI
- Teamleider Inkomen;
- Intern controleur (security officer);
- Teamleider Werk.
- Teamleider administratie

Jaarlijkse actualisering

De security officer roept jaarlijks de Overleggroep bijeen voor een evaluatie van de beveiligingsmaatregelen over de afgelopen periode.

Het beveiligingsplan en de aangedragen en genomen beveiligingsmaatregelen worden jaarlijks geëvalueerd en eventueel bijgesteld door de overleggroep Informatiebeveiliging. De security officer stelt hiervan een verslag op en biedt dit met een eventueel geactualiseerd beveiligingsplan Suwinet aan ter vaststelling door het Dagelijks Bestuur.

De 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 ISWI 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 volgende applicaties zijn in gebruik bij het ISWI:
- Suwinet-Inkijk;
- GWS4all :
- Module documentenuitvoer (MDU).
- Webapplicatie GBA via CompeT&T....

In dit hoofdstuk wordt alleen de applicatie Suwinet-Inkijk nader besproken.
De autorisatie voor het gebruik van de overige programma's wordt door de beherende teams geregeld. Verder wordt gewerkt met Outlook, Word en Excel.
De modules documentenuitvoer (MDU) is een documentengenerator die aansluit op Word en GWS4all, waardoor vanuit GWS4all rapportages, beschikkingen, brieven, ed. kunnen worden vervaardigd en geraadpleegd.

Applicatie Suwinet-Inkijk

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

<u>Suwinet-Inkijk</u>
Geautoriseerde medewerkers van het ISWI, het UWV en de SVB kunnen online elkaars gegevens raadplegen. Deze gegevens hebben o.a. betrekking op:
- Inschrijving als werkzoekende bij het UWV;
- Re-integratiegegevens van het UWV;
- Gegevens betreffende actuele adresgegevens, loondienst, Ziektewet- en WAO/WIA/Wajong-uitkeringen van het UWV;
- Uitkeringsgegevens m.b.t. de WWB, IOAW, IOAZ van de gemeenten
- Re-integratiegegevens van de gemeenten (nog niet verplicht);
- Boetewaardig gedrag.

Daarnaast kunnen de gemeenten putten uit gegevens van het Kadaster, de Belastingdienst, de Dienst Uitvoering Onderwijs (DUO), Rijksdienst voor het Wegverkeer (RDW) en het Bedrijvenregister.

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

<u>Samenloopapplicatie</u>
Maandelijks levert het ISWI voor elke gemeente het 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 het ISWI gestuurd, die vervolgens een onderzoek kan instellen naar mogelijke fraude.

Beveiliging: Het aan te leveren bestand wordt maandelijks samengesteld door de applicatiebeheerder, 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. Suwinet Mail is bij het ISWI (nog) niet ingericht.

Beveiliging: (nog) niet van toepassing.

DKD
Het Digitaal Klant Dossier is een onderdeel van Suwinet-Inkijk. 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 zijn er op aangesloten, zoals DUO, de Belastingsdienst, Zorgverzekeraars, Onderwijs en Justitie.

Beveiliging: Het DKD is een onderdeel van Suwinet-Inkijk. 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 de afdelingen Inkomen, Werk en Administratie 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.

De medewerkers met een autorisatie voor Suwinet-Inkijk moeten een zorgvuldigheidsverklaring ondertekenen.

Extern personeel
Extern personeel moet eveneens een zorgvuldigheidsverklaring ondertekenen. Deze verklaring wordt ondertekend op de eerste werkdag.

Bewustwording medewerkers
Aan alle medewerkers van het ISWI (die gebruik maken van de Suwinet-Inkijk applicatie) is het Beveiligingsplan uitgereikt. Het plan is mondeling toegelicht. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld (logging). Van deze log gegevens 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-Inkijk. Als het vermoeden van ongeoorloofd gebruik van dat medium bestaat kan specifieke informatie bij het BKWI worden opgevraagd.

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

- Het bestaan van 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-Inkijk wordt geconstateerd;
- Dat bij bovenstaande constatering de teamleider hierover contact opneemt met de betreffende medewerker(s).

In de bijlage "Procedure controle gebruik Suwinet-Inkijk" wordt nader ingegaan op de gelogde gegevens en de interne controle op rechtmatig gebruik van Suwinet-Inkijk.

Aan het gebruik van de informatiesystemen is een aantal verplichtingen verbonden. Alle medewerkers krijgen dit document uitgereikt.

Nieuwe medewerkers krijgen dit document zo spoedig mogelijk na indiensttreding met een mondelinge toelichting uitgereikt. Het uitreiken en het geven van informatie is één van de taken van de security officer.

Instructie incidenten en storingen

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de security officer of bij de teamleider, waarna een onderzoek wordt ingesteld naar eventuele gevolgen van het geconstateerde incident. Incidenten en het resultaat van het verrichte onderzoek worden besproken in de Overleggroep.

4. Fysieke beveiliging omgeving

Publieke ruimte

Persoonlijke cliëntcontacten vinden plaats op de diverse locaties van het ISWI. Bezoekers melden zich bij binnenkomst bij de receptie. Zij hebben slechts onder begeleiding toegang tot de spreekruimten.
De spreekkamers zijn voorzien van een alarmknop.

Werkruimte

De werkruimte van de medewerkers is gehuisvest in het bedrijfsverzamelgebouw "De Molenbeek". Gedeelten van het bedrijfsverzamelgebouw zijn niet toegankelijk voor bezoekers, maar uitsluitend voor personen die in het bezit zijn van een toegangspas. Dat is het eigen personeel en ingehuurd extern personeel. Daarnaast wordt aan medewerkers van onderhoudsbedrijven toegang verleend voor het verrichten van onderhoudswerkzaamheden. De werkruimtes op de Leerwerkcentra zijn niet afgesloten middels een toegangspas, maar deze zijn zodanig ingericht dat ten alle tijden zicht is op de werkplekken van de consulenten. Onbevoegden zijn nooit alleen in de werkruimtes.

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 komen in een prullenbak of een bak die bestemd is voor oud papier. Het vernietigen van deze gegevens moet op een veilige 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 10 minuten geen gebruik van is gemaakt automatisch vergrendeld en kunnen alleen door het ingeven van een wachtwoord weer worden geactiveerd.

Archiefruimten
Actuele cliëntendossiers worden bewaard in dossierkasten. Als er niemand aanwezig is gaan de dossierkasten op slot. De beëindigde cliëntendossiers worden overgeplaatst naar het statisch archief.

Printers
Er wordt gebruik gemaakt van centraal opgestelde printers. Indien een printopdracht wordt gegeven dient de medewerker deze onmiddellijk zelf op te halen. Mochten er toch uitgeprinte stukken achterblijven, dan worden deze aan het einde van de dag in een afgesloten papiercontainer gedeponeerd.

5. Beheer van werkprocessen

Procesbeschrijvingen en werkinstructies

De werkprocessen en instructies liggen vast in GWS4all. De workflow van een in GWS4all vastgelegde aanvraag bestaat uit meerdere fasen, waaraan een aantal taken is gekoppeld die de medewerker moet doorlopen alvorens de aanvraag voor verdere afhandeling te kunnen doorfaseren. Elke wijziging in de werkwijze wordt direct doorgevoerd in GWS4all, waardoor de medewerkers altijd over bijgewerkte werkprocessen beschikken.

Testen en implementatie applicaties

Voor het gebruik van GWS4all zijn er twee omgevingen gecreëerd: een productieomgeving en een testomgeving.
Regelmatig wordt de productieomgeving gekopieerd naar de testomgeving. De testomgeving wordt vooral gebruikt door de medewerkers van de uitkeringsadministratie. Maar ook alle andere medewerkers die toegang hebben tot GWS4all kunnen gebruik maken van de testomgeving.
Updates en patches worden eerst in de testomgeving geplaatst. Pas als de testresultaten goed zijn volgt installatie in de productieomgeving.

6. Toegangsrechten en autorisatiebeheer

Beleid ten aanzien van autorisaties

Het gebruik van Suwinet-Inkijk is voorbehouden aan de medewerkers van het ISWI die belast zijn met het vaststellen van het recht op uitkering, terugvordering en verhaal, re-integratie en de fraudepreventiemedewerker.
De security officer geeft aan de applicatiebeheerder, onder verantwoordelijkheid van de teamleiders, 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-Inkijk

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) stelt rapportages op over de logging van het gebruik van Suwinet-Inkijk. Deze rapportages worden beschikbaar gesteld aan de betreffende Ketenpartners. Aan de hand hiervan wordt gecontroleerd op het gebruik van Suwinet-Inkijk en wordt geprobeerd een goed beeld te krijgen van de wijze waarop Suwinet-Inkijk 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-Inkijk 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-Inkijk. Deze controle is nader uitgewerkt in de bijlage "Procedure controle gebruik Suwinet-Inkijk".

Autorisatieplan medewerkers

In de bijlage "Autorisaties Suwinet-Inkijk" 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-Inkijk. In de bijlage "Procedure controle gebruik Suwinet-Inkijk" 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 bespreekt dit rapport in de overleggroep Informatiebeveiliging.

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-Inkijk). Om toegang tot hun gegevens te krijgen moeten zij inloggen met hun DigiD-code bij www.mijnoverheid.nl of werk.nl
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.
In de bijlage "Procedure correctie gegevens" zijn protocollen opgenomen voor inzage en correctie. Medewerkers kunnen hiermee te maken krijgen en moeten hiervan op de hoogte zijn.

Autorisaties Suwinet-Inkijk
Er zijn verschillende functies binnen het ISWI die geautoriseerd zijn om gebruik te maken van Suwinet-Inkijk, te weten:
- De security officer (gebruikersbeheer);
- De medewerkers en teamleiders van de teams Werk, Inkomen en Administratie;
- De medewerkers debiteurenadministratie (raadplegen);
- De intern controleur (raadplegen);
- De medewerker bezwaar en beroep (raadplegen);
- De medewerker handhaving / fraudepreventie
- De applicatiebeheerder

Eindverantwoordelijke voor het gebruik en de beveiliging is de directeur.

De security officer
De intern controleur is aangewezen als security officer. Deze functionaris is belast met de volgende taken:
- Het verlenen van toegang tot en het autoriseren voor het gebruik van Suwinet-Inkijk;
- Het 3 maandelijks opvragen van loggings rapporten bij het BKWI;
- Het opvragen van specifieke rapportages bij het BKWI als hier aanleiding toe is;
- Het signaleren van gewenste aanpassingen van het beveiligingsplan op actualiteit en volledigheid hiervan;
- Zorgen voor het actueel houden van de applicatie, waardoor een goed gebruik van Suwinet-Inkijk en het DKD mogelijk is;
- Storingen die aan derden, zoals het Inlichtingenbureau of de softwareleverancier moeten worden gemeld, direct doorgeven.

De medewerkers en teamleiders Werk, Inkomen, Administratie
Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op:
- aanvragen WWB, IOAW, IOAZ, WI;
- heronderzoeken (zowel rechtmatigheids- als doelmatigheidsonderzoeken);
- re-integratiewerkzaamheden;
- debiteurenonderzoek
- inburgeringswerkzaamheden;
- fraude onderzoeken;
- die gevallen waarin de consulent dit nodig oordeelt; in deze gevallen wordt het raadplegen van Suwinet-Inkijk nader gemotiveerd in de rapportage van de consulent.

De medewerker debiteurenadministratie
Deze medewerker is geautoriseerd voor het raadplegen van Suwinet-Inkijk in verband met:
- Debiteurenheronderzoeken ter vaststelling van de actuele woonplaats, de draagkracht, de hoogte van het inkomen en de werkgever;
- Die gevallen waarin de medewerker dit nodig oordeelt; in deze gevallen wordt het raadplegen van Suwinet-Inkijk nader gemotiveerd in de rapportage van de medewerker.

Medewerkers Uitkeringsadministratie
De medewerkers Uitkeringsadministratie zijn geautoriseerd voor het raadplegen van Suwinet-Inkijk in verband met werkzaamheden betreffende de uitkeringsverwerking

Medewerker bezwaar en beroep
De medewerker bezwaar en beroep is geautoriseerd voor het raadplegen van Suwinet-Inkijk in verband met de afhandeling van bezwaar- en beroepszaken.

Intern controleur
De intern controleur is geautoriseerd voor het raadplegen van Suwinet- Inkijk in verband met steekproefsgewijze controle van de rechtmatigheid van de gerapporteerde bevindingen van de consulenten.

De medewerker handhaving / fraudepreventie
Deze medewerker is geautoriseerd een risicoanalyse te maken met betrekking tot uitkeringsaanvragen en het opsporen van fraude. De medewerker heeft tevens toegang tot de gegevens van de Kamer van Koophandel en de Rijks Dienst Wegverkeer.

De applicatiebeheerder
Deze is verantwoordelijk voor de goede werking van de applicatie en het invoeren en verwijderen van autorisaties.

Geoorloofd / ongeoorloofd gebruik
Als de geautoriseerde medewerkers Suwinet-Inkijk gebruiken voor de hiervoor gemelde gevallen dan is er sprake van geoorloofd gebruik. Wordt Suwinet-Inkijk om andere redenen gebruikt, dan is er in principe sprake van ongeoorloofd gebruik. Dit ongeoorloofd gebruik wordt onderzocht door de security officer en gemeld aan de eindverantwoordelijke: de teamleider dan wel de directeur.

Wachtwoord
Suwinet-Inkijk vraagt zelf om de aanmaak / periodieke wijziging van een wachtwoord; daar heeft de security officer geen invloed op.

Procedure controle gebruik Suwinet-Inkijk

Algemeen
Door het Bureau Keteninformatisering Werk & Inkomen (BKWI) worden rapportages samengesteld over de logging van het gebruik van Suwinet-Inkijk.

Het doel van deze logging is naast wetenschappelijke en statistische doeleinden het tegengaan en controleren van onrechtmatig, onregelmatig of doel overschrijdend gebruik van Suwinet-Inkijk.

De volgende gegevens worden gelogd:

- Het tijdstip van iedere log-in, log-out en andere actie;
- De gebruikersnaam van degene die inlogt of uitlogt;
- Burger Service Nummers (BSN) of andere zoeksleutels waarvan gegevens worden opgevraagd worden als actie geregistreerd;
- Elke actie, zoals de bekeken kolom- of overzichtspagina's.

Op verzoek verstrekt het BKWI (via het inlichtingenbureau) een overzicht van de volgende gegevens:

- Inkijkacties;
- Opvragingen unieke BSN;
- Geldige ten opzichte van ongeldige rollen;
- Inlog pogingen;
- Administrator account;
- Accounts per status;
- Opvragingen per pagina;
- Aantal geregistreerde accounts ten opzichte van de actieve accounts;
- Aantal opvragingen binnen / buiten kantoortijd.

Deze lograpporten worden iedere drie maanden door de security officer opgevraagd of gedownload en gecontroleerd. Als uit deze controle onregelmatigheden blijken, dan vraagt de security officer een specifieke rapportage op.

Controle gebruik Suwinet-Inkijk

- De security officer download of vraagt drie-maandelijks de via het Inlichtingenbureau beschikbaar gestelde BKWI-rapportages op;
- De security officer bepaalt of en van welke medewerker(s) specifieke raadpleeggegevens worden opgevraagd; dit gebeurt aan de hand van een steekproef;
- De security officer controleert de rapportages op onregelmatigheden. Bij geconstateerde onregelmatigheden wordt een specifieke rapportage opgevraagd. Ook kunnen van medewerker(s) raadpleeggegevens worden opgevraagd;
- De security officer gaat na of er geregistreerde accounts zijn die volgens de BKWI rapportages niet actief zijn geweest in de controleperiode en achterhaalt welke medewerkers geen of (te) weinig gebruik maken van Suwinet-Inkijk en wat daarvan de reden is;

- De security officer beoordeelt de geanonimiseerde en op naam gestelde rapportages en doet verslag van de bevindingen aan de directeur;
- De controleverslagen worden bewaard en de resultaten worden opgenomen in het verslag van de jaarlijkse evaluatie van het beveiligingsverslag.

Procedure autorisaties

Inleiding

De procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor Suwinet-Inkijk en de controle hierop.
De procedure bestaat uit drie afzonderlijke deelprocedures die apart kunnen worden uitgevoerd:

- Autorisaties tot Suwinet-Inkijk;
- Periodieke controle autorisaties;
- Toekennen van een tijdelijk wachtwoord.

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

Om toegang te krijgen tot de gegevens is naast de specifieke autorisatie in de desbetreffende applicatie tevens een bevoegdheid nodig op het netwerk en/of het systeemniveau. Deze laatstgenoemde bevoegdheden worden beheerd door systeembeheer.
De bevoegdheden binnen de applicatie Suwinet-Inkijk worden beheerd door de applicatiebeheerder onder verantwoordelijkheid van de security officer.

Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het de directeur.
De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij Suwinet-Inkijk berust bij de teamleiders. De uitvoering hiervan en het up to date houden van de procedure ligt bij de security officer.

Uitvoering

Autorisatie tot Suwinet-Inkijk

- Autorisaties voor Suwinet-Inkijk worden per medewerker/per rol toegekend;
- De teamleider verzoekt de security officer de nieuwe medewerker toegang te verlenen tot Suwinet-Inkijk; tevens kent zij het autorisatieniveau toe;
- Bij tussentijdse wijzigingen in taak/functie verzoekt de teamleider de security officer het autorisatieniveau -voor zover van toepassing- te wijzigen of de toegekende autorisaties in te trekken. Bij vertrek van de medewerker worden de hem/haar toegekende autorisaties direct beëindigd;
- Een verzoek aan de security officer tot toekenning, wijziging of beëindiging gebeurt met een standaardformulier (zie Formulier aanvraag autorisaties en Formulier intrekken of wijzigen autorisaties);
- De gebruiker krijgt van de security officer een melding als de autorisaties zijn geregeld. Ook krijgt de nieuwe gebruiker een korte instructie over de wijze van aanmelden en het direct aanpassen van het wachtwoord;
- Suwinet-Inkijk is voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes;
- De wachtwoorden voor Suwinet-Inkijk zijn maximaal 90 dagen geldig.

- Als een gebruiker gedurende 90 dagen achtereen niet heeft ingelogd wordt het wachtwoord automatisch geblokkeerd;
- Na drie maal foutief inloggen wordt het account automatisch geblokkeerd. Alleen de security officer kan het account weer vrijgeven;
- Het originele autorisatieformulier wordt door de security officer gearchiveerd.
- de security officer draagt er zorg voor dat applicatiebeheer de wijzigingen in de applicatie verwerkt.

Periodieke controle autorisaties

De security officer controleert jaarlijks de actualiteit en rechtmatigheid van de ingevoerde autorisaties. De wijze van controleren is als volgt:

- De security officer draait een lijst van gebruikers, gebruikersgroepen en ingevoerde autorisaties voor Suwinet-Inkijk uit;
- De security officer maakt een inventarisatie van de gebruikers, gebruikersgroepen en de toegekende autorisaties;
- Vervolgens controleert de security officer of het overzicht van de actieve gebruikers en de samenstelling van de gebruikersgroepen nog actueel zijn en of de bij die gebruikersgroepen behorende autorisaties nog juist zijn;
- Voor zover nodig actualiseert de security officer het gebruikersoverzicht en de gebruikersgroepen.

Formulier aanvraag autorisatie

Formulier aanvraag autorisatie

Naam medewerker	
Organisatieonderdeel	
Functie	
Naam applicatie	
Waarvoor wordt de applicatie gebruikt?	
Gevraagde autorisatie/rollen	
Aanvrager verklaart dat de informatie waartoe hij/zij toegang heeft uitsluitend zal worden gebruikt voor werkzaamheden die hij/zij uit hoofde van zijn/haar functie nodig heeft en niet zal doorgeven aan derden.	**Datum .....** **Handtekening .....**
Teamleider /directeur	**Naam .....** **Datum.....** **Handtekening .....**
Autorisatie ingevoerd door applicatiebeheer	**Naam .....** **Datum.....** **Handtekening .....**
Voor akkoord security officer	**Naam.....** **Datum .....** **Handtekening .....**

Formulier intrekken of wijziging autorisatie

Formulier intrekken of wijzigen autorisatie

Naam medewerker	
Organisatieonderdeel	
Functie	
Naam applicatie	
Reden intrekking/ wijziging autorisatie	
Reden gewijzigde autorisatie	
Teamleider /directeur	**Naam .....** **Datum.....** **Handtekening .....**
Intrekking / wijziging Autorisatie ingevoerd door applicatiebeheer	**Naam .....** **Datum.....** **Handtekening .....**
Voor akkoord security officer	**Naam.....** **Datum .....** **Handtekening .....**

Procedure opvragen en inzage gegevens

Telefonisch opvragen van gegevens

Het uitgangspunt is dat geen telefonische informatie over personen wordt verstrekt.

Het voeren van telefoongesprekken brengt risico's met zich mee omdat de identiteit van de gesprekspartner verkeerd kan worden vastgesteld en dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben.

Een verzoek om informatie moet schriftelijk worden ingediend en als de verzoeker informatie vraagt namens een cliënt moet het verzoek te zijn voorzien van een machtiging van de betreffende cliënt.

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 vast contactpersoon. Het UWV heeft een speciaal telefoonnummer geopend voor medewerkers van Sociale Diensten.

De cliënt verzoekt inzage in zijn cliëntdossier

1. De cliënt moet een afspraak maken;
2. Het dossier moet worden opgeschoond;
3. De cliënt moet zich legitimeren met een geldig identificatiebewijs;
4. Vermeld de datum van inzage en eventuele opmerkingen van de cliënt in het dossier nadat deze zijn gegevens heeft ingezien;
5. Als de cliënt het niet eens is met bepaalde gegevens dan kan hij een verzoek tot correctie indienen (zie procedure correctie gegevens).

Inzage door gemachtigde

1. De gemachtigde verzoekt schriftelijk of mondeling inzage in cliëntgegevens, voor zover niet te raadplegen via het klantbeeld (DKD);
2. De gemachtigde moet een afspraak maken;
3. Het dossier moet worden opgeschoond;
4. De gemachtigde moet zich legitimeren met een geldig identificatiebewijs;
5. De gemachtigde moet een door de cliënt gedateerde en ondertekende machtiging overleggen;
6. Controleer of de handtekening van de cliënt op de machtiging overeenstemt met de handtekening op een geldig legitimatiebewijs van de cliënt (kopie hiervan zit in dossier);
7. Vermeld, nadat de gemachtigde het cliëntendossier heeft geraadpleegd, de datum van inzage en eventuele opmerkingen van de gemachtigde in het cliëntendossier;
8. Als de gemachtigde het niet eens is met bepaalde gegevens kan hij namens de betreffende cliënt een verzoek tot correctie indienen (zie procedure correctie gegevens).

Procedure correctie gegevens

Verzoek om correctie door de cliënt

De cliënt verzoekt om correctie (mondeling of schriftelijk).

Het verzoek tot correctie wordt mondeling gedaan:

1. Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs;
2. Laat de cliënt het verzoek indienen via een standaardformulier;
3. Maak een kopie van het verzoek;
4. Verstrek de kopie als ontvangstbevestiging aan de cliënt;
5. Beoordeel of het verzoek niet beschouwd moet worden als bezwaarschrift;
6. Moet het verzoek behandeld worden als bezwaarschrift, draag het verzoek over aan de medewerker bezwaar en beroep;
7. De beoordeling van het verzoek om correctie wordt vastgelegd in een rapport;
8. Via de teamleider gaat de rapportage naar de administratie voor verdere afhandeling;
10. De cliënt krijgt een beslissing op zijn verzoek tot correctie;
11. Het rapport wordt met het verzoek opgeborgen in het dossier van de cliënt.

Het verzoek tot correct wordt schriftelijk gedaan:

1. Stuur een ontvangstbevestiging naar de cliënt;
2. Zie de punten 5 tot en met 11 hierboven.

Verzoek om correctie door gemachtigde

Het verzoek om correctie wordt door een gemachtigde gedaan:

1. Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs;
2. Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig is omschreven;
3. Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs;
4. Laat de gemachtigde een officieel verzoek indienen via een standaardformulier;
5. Maak een kopie van het verzoek;
6. Verstrek de kopie als ontvangstbevestiging aan de gemachtigde;
7. Beoordeel of het verzoek niet beschouwd moet worden als bezwaarschrift;
8. Moet het verzoek behandeld worden als bezwaarschrift, draag het verzoek over aan de medewerker bezwaar en beroep;
9. De beoordeling van het verzoek om correctie wordt vastgelegd in een rapport;
10. Via de teamleider gaat de rapportage naar de administratie voor verdere afhandeling;
12. De gemachtigde krijgt een beslissing op zijn verzoek tot correctie;
13. Het rapport wordt met het verzoek opgeborgen in het dossier van de cliënt.

Verzoek om correctie door derden

Een derde verzoekt om correctie. Dit is niet mogelijk.

Terugmelding door een medewerker van een van de ketenpartners

1. Er wordt een werkproces ingeboekt op naam van de medewerker;
2. Na afhandeling terugmelding wordt een bericht gestuurd aan de terugmelder.

Procedure communicatie over beveiliging

Inleiding
De procedure voorziet in het vastleggen van de communicatie rond het beveiligingsproces.

Communicatie over het onderwerp informatiebeveiliging kan plaatsvinden in drie situaties:

- Beveiliging als onderwerp op het periodieke werkoverleg;
- Beveiligingsonderwerpen bij individuele en functioneringsgesprekken;
- Beveiliging als onderwerp bij informatieverstrekking om het beveiligingsbewustzijn van het eigen personeel te verhogen.

Verantwoordelijkheid
De verantwoordelijkheid voor deze procedure ligt te allen tijde bij de verantwoordelijke, het dagelijks bestuur en namens deze de directeur.
De security officer zorgt er enerzijds voor dat nieuwe ontwikkelingen op het gebied van informatiebeveiliging binnen de organisatie bekend worden gemaakt en anderzijds dat het gewenste niveau van kennis en bewustzijn met betrekking tot informatiebeveiliging wordt bereikt.

Ook worden de betrokken medewerkers onder verantwoordelijkheid van de security officer jaarlijks (via werkoverleg) geïnstrueerd over de mogelijke risico's en (verplichtende) richtlijnen en procedures om schade en incidenten te voorkomen.

De security officer is verantwoordelijk voor het up to date houden van deze procedure.

Uitvoering

<u>Periodiek werkoverleg</u>

De directeur draagt er zorg voor dat op het periodieke werkoverleg de gelegenheid wordt geboden om over het onderwerp beveiliging te spreken.
Het onderwerp wordt hetzij op initiatief van de leidinggevende, hetzij op verzoek van één van de medewerkers op de agenda geplaatst.
Onderwerpen die aan de orde kunnen komen zijn (niet limitatief):

- De functionaliteit van de beveiligingsprocedures;
- Tekortkomingen, aanpassingen en adviezen op het gebied van regelgeving;
- Attenderen op ongewenste situaties;
- Beveiligingstekortkomingen in operationele handelingen;
- Gevaarlijk of ongewenst gedrag van medewerkers.

De verslaglegging van de beveiligingsonderwerpen welke zijn besproken tijdens het werkoverleg worden toegezonden en bewaard door de security officer.

<u>Beveiliging bij individuele of functioneringsgesprekken</u>
Iedere medewerker wordt in de gelegenheid gesteld om beveiligingsonderwerpen te bespreken waarvan de inhoud vertrouwelijk of delicaat is. De aangewezen gesprekspartners daarvoor zijn:

- De directeur;
- De teamleider;
- De security officer;
- Een vertrouwensmedewerker (op uitnodiging van de melder).

Het onderwerp beveiliging komt ook aan de orde in de periodieke functioneringsgesprekken.

- De medewerker kan in eerste instantie terecht bij zijn of haar direct leidinggevende. Daarnaast kan ook rechtstreeks contact worden opgenomen met de directeur of de security officer Deze zijn gehouden de vertrouwelijk verstrekte informatie ook als zodanig te behandelen;
- Vrijwillig verstrekte informatie mag nimmer leiden tot repercussie op de informatie verstrekkende medewerker;
- De security officer beoordeelt de verkregen informatie en bespreekt deze informatie met de directeur of teamleider. De informatie en de verstrekker worden daarbij zo deugdelijk mogelijk anoniem gemaakt;
- Individueel verkregen informatie wordt ook op individuele basis teruggekoppeld met de informatie verstrekkende medewerker;
- De security officer of andere genoemde medewerkers die vertrouwelijke informatie ontvangen handelen naar de aard en inhoud van die informatie.

Taakbeschrijving security officer

Inleiding

De directeur heeft een security officer benoemd. Deze functionaris is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Beveiligingsplan. Zij bevordert de informatiebeveiliging en de communicatie naar de medewerkers betreffende dit onderwerp. De security officer roept eens per jaar de Overleggroep Informatiebeveiliging bijeen voor een evaluatie van de voorgaande periode. Zij maakt hiervan een verslag en biedt dit met een eventueel aangepast Beveiligingsplan ter vaststelling aan het de directeur.

Taken security officer

De security officer:

- Bevordert en adviseert op het gebied van de informatiebeveiliging;
- Controleert of en in hoeverre beveiligingsmaatregelen worden nageleefd;
- Voert periodieke controles uit op een rechtmatig gebruik van Suwinet-Inkijk;
- Doet voorstellen tot implementatie of aanpassing van plannen en werkprocessen op het gebied van de beveiliging;
- Houdt toezicht op het feit dat nieuwe medewerkers (ook extern personeel) worden geïntroduceerd en bekend gemaakt met de beveiligingsprocedures;
- Ziet erop toe dat het beveiligingsplan Suwinet-Inkijk aan alle huidige en toekomstige medewerkers (ook extern personeel) wordt uitgereikt;
- Fungeert als centraal aanspreekpunt op het gebied van informatiebeveiliging;
- Onderneemt actie voor de jaarlijkse evaluatie en het actueel houden van het beveiligingsplan.