Informatiebeveiligingsplan Wijzer 2015

Bussum, 2015

Hoofdstuk 1. Inleiding

1.1 Doel van informatiebeveiliging

De primaire en ondersteunende processen binnen Wijzer, de Uitvoeringsdienst Sociaal Domein van de gemeenten Naarden, Muiden en Bussum, zijn in hoge mate afhankelijk van adequate informatievoorziening en betrouwbare informatiesystemen.

Het informatiebeveiligingsbeleid inzake Wijzer is er op gericht om de beschikbaarheid, de betrouwbaarheid, de integriteit en de vertrouwelijkheid van de gegevens binnen Wijzer en de (geautomatiseerde) uitwisseling van gegevens met partners (waaronder Suwi[1]) te waarborgen.

Door middel van de nota Beleid Informatiebeveiliging Wijzer 2015 is het beveiligingsbeleid vastgesteld. De nota bevat kaders en uitgangspunten. Het voorliggende beveiligingsplan geeft uitvoering aan het beleid en vormt daarmee een actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door de inzet van mensen en middelen.

1.2 Definitie informatiebeveiliging

Onder informatiebeveiliging wordt verstaan:

"Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces".

"Betrouwbaarheid" is de overkoepelende term voor beschikbaarheid (continuïteit, responstijd), integriteit (juistheid, volledigheid, tijdigheid, geoorloofdheid) en vertrouwelijkheid (exclusiviteit). Hiermee wordt aangegeven in welke mate de organisatie zich kan verlaten op een informatiesysteem voor haar informatievoorziening. Dit betreft zowel de technische, de organisatorische, als de menselijke aspecten.

1.4 Juridisch kader

In deze paragraaf wordt het juridische kader geschetst waar Wijzer zich voor wat betreft informatiebeveiliging voor gegevensuitwisseling aan dient te houden.

1.4.1 Wet Bescherming Persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) stelt dat persoonsgegevens alleen voor welbepaalde uitdrukkelijke omschreven en gerechtvaardigde doeleinden mogen worden verkregen.

Ingevolge de Wbp moeten persoonsgegevens in overeenstemming met de Wbp en op behoorlijke en zorgvuldige wijze worden verwerkt. Op hoofdlijnen betekent dit:

- persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld;
- voor de verwerking dient een van de in de Wbp genoemde rechtvaardigingsgronden te bestaan;
- slechts onder bepaalde voorwaarden mogen persoonsgegevens voor andere doeleinden worden gebruikt dan waarvoor ze zijn verzameld;
- persoonsgegevens mogen slechts worden verwerkt voor zover zij voor het doel toereikend, ter zake dienend en niet bovenmatig zijn;
- de organisatie treft de nodige maatregelen zodat de persoonsgegevens, gelet op het doel waarvoor ze worden verwerkt, juist en nauwkeurig zijn;
- de organisatie legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking;

[1] Structuur Uitvoeringsorganisatie werk en inkomen

de verantwoordelijke dient er tevens voor te zorgen dat ook de bewerker voldoende waarborgen biedt met betrekking tot technische en organisatorische beveiliging;
- de organisatie informeert de betrokkene over de verwerking van zijn persoonsgegevens en biedt zij de betrokkene de gelegenheid tot inzage in zijn persoonsgegevens; indien de gegevens feitelijk onjuist blijken te zijn of voor het doeleinde onvolledig, niet ter zake dienend of anderszins in strijd met de wet worden verwerkt, komt betrokkene het recht op correctie toe; in enkele gevallen kan betrokkene tevens gebruik maken van het recht van verzet;

Volgens de Wbp dient iedere geautomatiseerde gegevensverwerking “bestemd voor de verwezenlijking van een doeleinde” te worden gemeld bij het College bescherming persoonsgegevens (Cbp). Wanneer de gemeente een privacyfunctionaris heeft aangesteld en heeft aangemeld bij het Cbp, is het voldoende de gegevensverwerking bij deze functionaris aan te melden.

Wijzer wordt eveneens door de Wbp verplicht passende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beschermen tegen een onwettige verwerking.

1.4.2 Specifiek Suwi wet- en regelgeving en de Participatiewet

Ook in de wetgeving zijn bepalingen opgenomen die tot doel hebben de persoonlijke levenssfeer van betrokkenen te beschermen. Voor Wijzer is dit onder andere de Wet Structuur uitvoering werk en inkomen (wet Suwi), het Suwi-besluit en de Regeling Suwi.

Uit de Suwi regelgeving vloeien doel en taken van Wijzer en de overige Suwi partijen voort.
De sectorale wetgeving regelt onder meer de informatievoorziening van de Suwi-organisaties onderling en aan derden. Daarbij is bepaald dat de gegevensstromen tussen de Suwi-organisaties via het Suwi-net verlopen. Gegevensstromen waarin de Suwi regelgeving niet voorziet mogen, zonder goedkeuring van de Minister, niet plaatsvinden. Voor zover in de wet Suwi niet van de Wbp wordt afgeweken, geldt de Wbp.

Er wordt binnen het Suwi-net gebruik gemaakt van meerdere verzamelingen van persoonsgegevens, elk met haar eigen verantwoordelijkheid. De gegevens die worden uitgewisseld tussen de Suwi-organisaties vallen binnen het domein waarvoor de verantwoordelijkheden op basis van afspraken worden ingevuld. Dit betekent dat gezamenlijk het vereiste niveau van beveiliging en de benodigde maatregelen worden vastgesteld. De uitvoering van de maatregelen ligt vervolgens bij de Suwi-organisaties en bij het BKWI[2]. Naast persoonsgegevens van inwoners omvat het domein ook persoonsgegevens van medewerkers. Dit betreft gegevens van medewerkers (persoonsnamen) die worden vastgelegd in logbestanden.

Vanaf 2004 dient iedere gemeente overeenkomstig artikel 6.4 van de Regeling Suwi in een beveiligingsplan aan te geven op welke wijze zij invulling geeft aan de beveiliging van de gegevensuitwisseling in het kader van Suwi.

Daarnaast is de Participatiewet relevant. In de Participatiewet is een aparte paragraaf opgenomen over de regels die van toepassing zijn bij de uitwisseling van persoonsgegevens. Deze paragraaf kan als volgt op hoofdlijnen worden geschetst:
- werkgevers hebben een informatieplicht om inlichtingen te verstrekken omtrent de aanvrager van een uitkering en een uitkeringsgerechtigde betreffende omstandigheden die noodzakelijk zijn voor de uitvoering van de wet;
- diverse instanties zoals het UWV, de SVB, overige gemeenten, College voor zorgverzekeringen, pensioenfondsen, etc. hebben een informatieplicht aan de gemeente indien noodzakelijk voor de uitvoering van de Participatiewet;
- medewerkers die met persoonsgegevens in aanraking komen hebben een geheimhoudingsplicht, tenzij het voor de uitvoering van de Participatiewet noodzakelijk is deze persoonsgegevens te verstrekken aan anderen.
- de gemeente heeft een inlichtingenverplichting binnen gestelde regels ten aanzien van diverse instellingen, zoals het UWV, de SVB, de belastingdienst, overige gemeenten, etc. Voor de verstrekking van gegevens tussen instanties wordt gebruik gemaakt van het Burger Service Nummer (BSN).

[2] Bureau Keteninformatisering Werk en Inkomen

1.4.3 Specifiek Jeugdwet

In de Jeugdwet staat dat het college gegevens verwerkt ten behoeve van de totstandbrenging van een doelmatig, doeltreffend en samenhangend gemeentelijk beleid ten aanzien van preventie, jeugdhulp, de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering en het advies- en meldpunt huiselijk geweld en kindermishandeling en ten behoeve van de toegang van jeugdigen en hun ouders tot de jeugdhulp.

Jeugdhulpaanbieders, aanbieders van preventie, gecertificeerde instellingen en de raad voor de kinderbescherming verstrekken kosteloos gegevens aan het college, ten behoeve van deze verwerking. Deze verstrekking kan zowel een structureel als incidenteel karakter hebben.

Deze gegevens kunnen persoonsgegevens zijn, voor zover deze gegevens noodzakelijk zijn voor het doelmatig en doeltreffend functioneren van de toegang tot de jeugdhulp, de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering. Dit kunnen zijn het burgerservicenummer en bijzondere persoonsgegevens zijn als bedoeld in artikel 16 van de Wet bescherming persoonsgegevens. De gegevens, alleen mogen alleen worden gebruikt voor een specifiek doel en niet voor andere doeleinden of daarmee niet verenigbare doeleinden. In diverse aanpalende wetgeving is aangegeven aan wie gegevens mogen worden verstrekt (Wbp, Jeugdwet, WGBO, Wmo, etc.)

1.4.4 Specifiek Wmo

In de Wmo staat dat gemeenten bevoegd zijn om de volgende gegevens te *verwerken*:

- Persoonsgegevens van de cliënt. Hieronder valt informatie over de gezondheid, die is bedoeld om de behoefte aan ondersteuning te kunnen vaststellen en om in kaart te brengen of iemand in aanmerking komt voor een maatwerkvoorziening.
- Gegevens van de echtgeno(o)t(e), ouders, inwonende kinderen en huisgenoten, om te kunnen vaststellen welke hulp zij kunnen bieden. Deze informatie maakt ook duidelijk of iemand in aanmerking komt voor een maatwerkvoorziening.
- Gegevens van mantelzorgers en andere personen uit een sociaal netwerk (met dezelfde reden en doel als hierboven).

Gemeenten mogen aanbieders van maatwerkvoorzieningen de volgende persoonsgegevens (waaronder informatie over de gezondheid) *verstrekken*:

- Gegevens uit het onderzoek die uitsluitsel geven of iemand in aanmerking komt voor een maatwerkvoorziening.
- Met uitdrukkelijke toestemming van de cliënt: gegevens die het college heeft verkregen op grond van de uitvoering van de Jeugdwet, de Participatiewet of de Wet gemeentelijke schuldhulpverlening. De data kunnen ook verstrekt zijn door een zorgverzekeraar, een zorgaanbieder of het CIZ.
- Relevante gegevens van zorgverzekeraars en zorgaanbieders vanuit uitvoering van de Zorgverzekeringswet of van het CIZ, om een passend integraal aanbod te waarborgen.
- Bij AMvB kan worden bepaald op welke wijze persoonsgegevens worden verwerkt en volgens welke technische standaarden. En aan welke veiligheidseisen moet worden voldaan.
- In de Uitvoeringsregeling Wmo 2015 staat dat de gegevensverwerking, bedoeld in artikel 5.2.9, zesde lid, van de wet, voldoet aan NEN-ISO-IEC 27001 en NEN-ISO-IEC 27002 of gelijkwaardig is aan deze normen. Met de Nota informatiebeveiliging Wijzer 2015 en dit beveiligingsplan wordt voldaan aan deze ISO of gelijkwaardige normen.

1.4.5 Belastingzaken

Als de gegevensverwerking noodzakelijk is voor de uitvoering van een publiekrechtelijke taak dan mogen deze gegevens op grond van de Wet bescherming persoonsgegevens (Wbp, artikel 8) worden

gevraagd en verwerkt. Het uitgangspunt moet zijn dat er zo min mogelijk wordt verwerkt maar wel zoveel mogelijk als nodig is voor het doel van de vraag.

1.4.6 Wet gemeentelijke schuldhulpverlening

Als de gegevensverwerking noodzakelijk is voor de uitvoering van een publiekrechtelijke taak dan mogen deze gegevens op grond van de Wet bescherming persoonsgegevens (Wbp, artikel 8) worden gevraagd en verwerkt. Het uitgangspunt moet zijn dat er zo min mogelijk wordt verwerkt maar wel zoveel mogelijk als nodig is voor het doel van de vraag.

1.4.7 Overige wetgeving

Naast de sectorale wet- en regelgeving en de WBP geldt er diverse andere wet- en regelgeving, zoals de Wet voor Computercriminaliteit, de Auteurswet en de Archiefwet. Vanwege het algemene karakter van dit voorliggende beleid van dit onder het gemeentebrede informatiebeleid.

Hoofdstuk 2. Reikwijdte

2.1 Wet- en regelgeving

Het informatiebeveiligingsbeleid Wijzer 2015 omvat de uitvoering van:

a. de Wet Structuur uitvoering werk en Inkomen (SUWI);
b. de Participatiewet, de Wet werk en bijstand;
c. de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ);
d. de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW);
e. het Besluit bijstandverlening zelfstandigen (Bbz 2004) en voormalige regelingen in het kader van gesubsidieerde arbeid;
f. de Wet gemeentelijke schuldhulpverlening;
g. de Wet maatschappelijke ondersteuning 2007 (oud) en de Wet maatschappelijke ondersteuning 2015;
h. de Jeugdwet;
i. Wet Schuldsanering Natuurlijke Personen;
j. de Wet inburgering;
k. de lokale verordeningen en regelingen voor de minima, zoals het Doe-budget en de PC-regeling;
l. de lokale verordeningen en regelingen voor kwijtschelding van de gemeentebelasting;
m. de lokale verordeningen en regelingen voor het leerlingenvervoer;
n. Samenwerkingsmodel Nazorg volwassen (ex)gedetineerden;
o. de uit voornoemde wetten voortkomende algemene maatregelen van bestuur, ministeriële regelingen, verordeningen en nadere regels.
p. Andere nog te treffen regelingen op het terrein van het Sociaal Domein indien en voorzover de uitvoering daarvan wordt opgedragen aan Wijzer.

2.2 Uitgangspunten

Binnen het werkveld Werk en Inkomen moeten de gemeenten zich conformeren aan de richtlijnen van het Bureau Keteninformatisering Werk & Inkomen (BKWI). Het doel van beveiliging is het waarborgen van de continuïteit van de bedrijfsvoering en het beperken van schade door proberen beveiligingsincidenten en eventuele gevolgen te voorkomen.

Het huidige informatiebeveiligingsbeleid ziet vooral op de keten Werk & inkomen en kwam voort uit eisen vanuit de Suwiregeling. Informatieveiligheid dient echter te zien op de gehele uitvoering

Sociaal Domein. Dat wordt in de voorliggende nota geformaliseerd. De eisen inzake Suwi zijn echter universeel relevant, waardoor deze als norm gehanteerd worden.

Norm 1.3 BKWI Beveiligingsplan
De gemeente heeft een formeel vastgesteld beveiligingsbeleid en –plan met ingang van 1 september 2015. Dat betekent dat dit door de colleges moet worden vastgesteld. Het plan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door inzet van mensen en middelen.

Norm 1.4 BKWI Uitdragen
Het uitdragen van het beveiligingsbeleid en –plan is een aandachtspunt en moet geborgd worden. Het plan moet van hoog tot laat goed bekend zijn en gedragen worden in de organisatie. Dit gebeurt door plaatsing op intranet, uitreiking aan de medewerkers, periodiek in teamoverleggen op de agenda plaatsen en dit vastleggen in de notulen.

Norm 1.5 BKWI Actualiseren
Het beleid moet regelmatig geactualiseerd worden. Voor de eerste maal in 2017.

Norm 2.2 BKWI Functiescheiding
De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van de gegevens moeten beschreven zijn en duidelijk en afhankelijk van de omvang van de organisatie gescheiden belegd zijn.

Norm 2.3. BKWI Security Officer
De Security Officer bevordert en adviseert over de informatiebeveiliging, verzorgt rapportages over de status en controleert dat, overeenkomstig de wettelijke eisen. Hij rapporteert rechtstreeks aan de bestuurlijk verantwoordelijke.

Norm 13.1 BKWI Autorisatiestructuur
Het toegangsbeheer tot de applicaties ligt bij de organisatie. Er moet een procedure beschikbaar zijn waarin de criteria staan vermeld om toegang te verlenen tot de applicaties. Het afdelingshoofd stelt de autorisatiestructuur vast.

Norm 13.5 BKWI Controle
Periodiek moet controle op toegangsrechten en gebruik plaatsvinden.

Gewijzigd dienstverleningsconcept.
De integrale vraagverheldering en het principe 1 huishouden, 1 plan, 1 regie leidt ook tot intern hergebruik of uitwisseling van gegevens die op grond van verschillende wettelijke bevoegdheden of bepalingen verkregen zijn. Duidelijk moet zijn dat dit alleen kan waar de wet dit toestaat of als er een ondubbelzinnige toestemmingsverklaring is afgegeven.

Incidentregistratie
Ter voorkoming van het verspreiden van virussen moet een adequaat backupsysteem aanwezig zijn. Incidenten moeten worden geregistreerd.

Inrichting beveiligingsorganisatie
De rollen, taken, bevoegdheden en verantwoordelijkheden moeten duidelijk zijn beschreven. Informatiebeveiliging is een lijnverantwoordelijkheid.

Wpb
Op grond van de Wet bescherming persoonsgegevens (Wbp) kan een klant bij de afdeling inzage vragen in of correctie vragen van gegevens. Zulke verzoeken vereisen een zorgvuldige behandeling. Datzelfde geldt, in nog sterkere mate, bij de verstrekking van gegevens aan derden. Naast deze privacyaspecten van de gegevensuitwisseling moeten ook algemene beveiligingsaspecten in acht te worden genomen. In artikel 13 Wbp is namelijk bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de

verwerking en de aard van de te beschermen gegevens met zich brengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De vraag welke beveiligingsmaatregelen door gemeenten moeten worden genomen in het kader van de gegevensuitwisseling die plaatsvindt via het SUWII-net dient te worden beantwoord aan de hand van de maatregelen omschreven in de zogenaamde risicoklassen. Het CBP gaat in haar rapport “Beveiliging van persoonsgegevens, achtergrondstudies en verkenningen 23” uit van de navolgende vier risicoklassen:

Risicoklasse 0	publiek niveau;
Risicoklasse I	basis niveau;
Risicoklasse II	verhoogd risico;
Risicoklasse III	hoog risico.

In dit plan zal aangegeven worden op welke manier deze risicoklassen van toepassing zijn bij Wijzer.

Hoofdstuk 3. Beveiligingsbeleid

Het gemeentelijk management moet aantonen dat zij het belang van informatiebeveiliging ondersteunt. Hiervoor moet informatiebeveiligingsbeleid opgesteld worden voor de hele organisatie. Voor Wijzer is een specifieke nota opgesteld die fungeert als leidraad voor het beveiligingsplan. Dit plan is de concrete invulling van het opgestelde beleid. Voor het beleidsdocument wordt verwezen naar het document: ” Nota Informatiebeveiliging Wijzer 2015”.

Hoofdstuk 4. Beveiligingsorganisatie

4.1 Organisatorische infrastructuur voor informatiebeveiliging

De beveiligingsorganisatie is zodanig vormgegeven dat het hoogste management betrokken is en dat taken, verantwoordelijkheden en bevoegdheden gescheiden zijn belegd opdat geen rolvermenging of rolconflicten kunnen ontstaan (norm 2.2. BKWI).

Beveiligingsfunctionarissen gemeentebreed
De gemeentesecretaris is met de vaststelling van het gemeentelijke beleidsplan 2011 aangewezen als hoofd informatiebeveiliging. Het afdelingshoofd F&I is aangewezen als coördinator informatiebeveiliging.

Binnen de afdeling F&I is er ten behoeve van het Sociaal Domein een Security Officer aangewezen, die specifiek verantwoordelijk is voor en belast is met het beheer en de beheersing van beveiligingsprocedures en -maatregelen in het kader van Suwinet en het verdere informatiebeveiligingsbeleid van Wijzer. De Security Officer bevordert en adviseert gevraagd en ongevraagd over de beveiliging (van o.a. Suwinet), verzorgt rapportages over de status, controleert dat de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van beveiliging van gegevens, waaronder Suwinet. In het kader van onafhankelijk toezicht op de controle & kwaliteitsborging van het informatiebeveiligingsbeleid van Wijzer maakt de Security Officer geen deel uit van Wijzer. De security-officier rapporteert aan de coördinator informatiebeveiliging en het afdelingshoofd van Wijzer en zo nodig rechtstreeks aan de verantwoordelijke portefeuillehouder (Norm 2.3 BKWI).

Beveiligingsfunctionarissen Wijzer
Het afdelingshoofd van Wijzer is belast met het adviseren over en het uitvoeren van het informatiebeveiligingsbeleid en is als ‘eigenaar’ van specifieke systemen die de afdeling gebruikt primair verantwoordelijk voor het beheer en beveiliging van die systemen.

De teamleiders van Wijzer zijn belast met dagelijks toezicht op het naleven van beveiligingsaspecten en het vergroten van bewustwording bij de medewerkers.

Applicatiebeheerder Wijzer
De applicatiebeheerder van Wijzer is belast met het functioneel beheer van de applicaties bij Wijzer, het autoriseren en beheren van toegang(srechten) tot de systemen conform de vastgestelde autorisatiestructuur en het instellen van formele controles volgens het informatiebeveiligingsplan of op last van de Security Officer.

Hoofdstuk 5. Classificatie en beheer van bedrijfsmiddelen

5.1 Verantwoording van ICT-bedrijfsmiddelen

In deze paragraaf wordt aangegeven op welke manier Wijzer haar bedrijfsmiddelen beveiligt tegen storingen. Met name wordt het in kaart brengen en beheren van de bedrijfsmiddelen bedoeld.
Alle belangrijke informatiebedrijfsmiddelen zijn bij de gemeente beveiligd.
Voor wat betreft een actueel overzicht van bedrijfsmiddelen en de beveiliging hieromtrent, kan vermeld worden dat in Bussum gewerkt wordt met het ITIL-proces (ITIL staat IT Infrastructure Library). Dit proces helpt de afdeling F&I bij het managen van bedrijfsprocessen.
De ITIL aanpak kan opgesplitst worden in deelgebieden t.w. configuratiebeheer, versie/licentiebeheer en Topdesk. In Topdesk worden de incidenten vastgelegd en de wijzigingen.

5.2 Classificatie van informatie

In deze paragraaf wordt aangegeven op welke wijze informatie binnen Wijzer is gecategoriseerd.
Binnen de afdeling wordt gewerkt met persoonsgegevens die aangemerkt kunnen worden als bijzondere persoonsgegevens zoals beschreven in artikel 16 WBP. Omdat deze gegevens niet specifiek onderscheiden kunnen worden binnen de gegevensuitwisseling en gezien het grote aantal uitwisselingen, wordt de risicoklasse van de gegevens vastgesteld op een combinatie van II en III.
(zie ook hoofdstuk 2 reikwijdte-uitgangspunten)
Logbestanden en de gebruikersadministratie bevatten gegevens van medewerkers. De gegevens die worden vastgelegd in deze bestanden worden vastgelegd in risicoklasse I.

Om te voorkomen dat medewerkers van Wijzer bij een eventuele crash van het netwerk of incidenten gegevens over langere tijd kwijt zijn, is er een zogenaamde ‘spiegel-uitwijk’ op de Huizerweg gestationeerd. De ‘spiegel-uitwijk’ is een realtime schaduwsysteem. Dit betekent dat alle gegevens die op dit moment worden bewerkt, tegelijkertijd in de spiegelomgeving plaatsvinden. Het betreft alle data, rapporten, beschikkingen, etc.

Hoofdstuk 6. Beveiligingseisen ten aanzien van personeel

6.1 Beveiligingseisen bij aanname van personeel

Door middel van deze paragraaf wordt in kaart gebracht op welke manier Wijzer aandacht schenkt aan informatiebeveiliging.

Vast personeel
Personeel dat in dienst is bij de gemeente valt direct onder het ambtenarenreglement. Dit betekent dat zij bij benoeming niet apart een verklaring dienen te ondertekenen dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In het ambtenarenreglement is dit reeds opgenomen.

Wel krijgen medewerkers na hun benoeming een gemeentebrede introductie. Als ambtenaar verplicht je je alle zaken waarvan je weet of vermoedt dat ze een vertrouwelijk karakter hebben, geheim te houden.

Tijdelijk personeel
Tijdelijke medewerkers tekenen een integriteitsverklaring. Niet duidelijk is waar deze verklaring wordt gearchiveerd. Dit moet worden geborgd. Iedere medewerker die gebruik moet maken van het GBA, tekent het protocol inzake toegang tot het GBA.

6.2 Training voor gebruikers

Wijzer instrueert de individuele gebruikers omtrent correcte omgang met ICT-voorzieningen.
Binnen de afdeling wordt met betrekking tot SUWI-net een gebruikershandleiding verzonden aan alle nieuwe gebruikers. Dit moet worden opgenomen in checklist 'nieuw personeel'.
Tijdens de algemene introductie van nieuwe medewerkers worden zij in kennis gesteld van het gebruik van privacygevoelige informatie.

6.3 Reageren op incidenten en storingen

In deze paragraaf is aangegeven op welke manier Wijzer incidenten die de beveiliging aantasten verwerkt en registreert.
Wanneer zich binnen Wijzer een storing op ICT niveau voordoet wordt dit via de Wijzer Helpdesk gemeld aan de applicatiebeheerder van Wijzer. Kan deze het probleem niet oplossen dan wordt geëscaleerd naar de gemeentelijke servicedesk van de afdeling F&I. Iedere medewerker bij Wijzer is bekend dat storingen aan ICT voorzieningen via de applicatiebeheerder van Wijzer gemeld moeten worden.
Na ontvangst van een melding wordt door de servicedesk een callnummer gegenereerd. Na afhandeling van de melding krijgt de applicatiebeheerder die de storing heeft doorgegeven een melding dat de call is afgehandeld.

In het kader van ITIL worden beveiligingsincidenten door ICT gerapporteerd en gedocumenteerd. Bij het opstellen van de jaarplanning worden zogenaamde "to do "punten opgesteld en wordt gekeken welke doelstellingen zijn behaald in het afgelopen jaar.

6.3.1 Rapporteren van onvolkomenheden in de software
Bij Wijzer is de applicatiebeheerder verantwoordelijk voor het beheer van Suwi-net. Dit betekent dat hij ook degene is die de autorisaties verstrekt aan individuele medewerkers.
Bij eventuele problemen op software gebied is hij degene die als aanspreekpunt fungeert voor de medewerkers. Mochten de problemen niet gelijk door hem op te lossen zijn, wordt het probleem doorgegeven aan of de servicedesk van F&I of de Servicedesk van het Inlichtingenbureau, die dan verdere actie onderneemt.
Wanneer het onvolkomenheden betreft in software dat standaard door F&I is uitgeleverd op een werkplek, is de servicedesk van F&I het eerste aanspreekpunt.

6.3.2 Lering trekken uit incidenten
Met de komst van ITIL is ook een apart software pakket aangeschaft dat fungeert als een registratiesysteem voor servicecalls. Wanneer gebruikers problemen hebben met applicaties, wordt via de applicatiebeheerder Wijzer contact opgenomen met de servicedesk van F&I. Zij maken vervolgens een call van de melding, waarna de oplossing wordt gezocht.
Alle calls worden geregistreerd. Ook wordt vastgelegd wanneer er welke wijzigingen hebben plaatsgevonden.

6.3.3. Incidentenregistratie
- Overtredingen, gebreken of incidenten met betrekking tot informatiebeveiliging en privacybeveiliging worden geregistreerd en onderzocht door de Security Officier, die ter zake incidenteel of periodiek rapporteert en aanbevelingen doet.

- Afdelingshoofd, teamleiders en applicatiebeheerders van Wijzer zijn ter zake meldingsplichtig aan de Security Officer.

Hoofdstuk 7. Fysieke beveiliging en beveiliging van de omgeving

7.1 Beveiligde ruimten

Deze paragraaf geeft inzicht in de wijze waarop Wijzer de ICT voorzieningen heeft beschermd tegen ongeoorloofde toegang, schade en storingen.
De afdeling is zeer afhankelijk van ICT-voorzieningen voor het verrichten van de primaire processen. Uitval van deze voorzieningen heeft als risico dat betaling niet of niet tijdig kunnen worden gedaan. Om de risico's te borgen bevinden de servers, met daarop de data van de softwarepakketten, zich niet fysiek op Wijzer.
De servers zijn geplaatst in ruimtes bij de afdeling F&I en de toegang tot deze ruimtes is enkel toegestaan voor medewerkers van F&I. Door middel van het fysiek afsluiten van deze ruimten is ongeoorloofde toegang geborgd. Een alarmsysteem beveiligt de ruimtes.
Backup omgeving is gelocaliseerd bij de Huizerweg in Bussum. Eénmaal per week wordt er op tape een backup gemaakt.
Bij storingen aan de ICT-voorzieningen worden door de afd. F&I monteurs ingeschakeld om de geconstateerde problemen op te lossen. Dit gebeurt na overleg met de applicatiebeheerder Wijzer.

7.2 Fysieke beveiliging van de omgeving

Bij de gemeente Bussum is een deel van het gebouw toegankelijk voor publiek. Dit betreft de ruimte van de centrale balie en de wachtruimte van Wijzer die zonder beperkingen te betreden zijn voor bezoekers.
De voor publiek vrij toegankelijke ruimten zijn in zoverre gedefinieerd dat de toegangsdeuren naar de niet voor publiek toegankelijk ruimten alleen geopend kunnen worden met een elektronische sleutel (druppel) of door de receptionist. Klanten kunnen niet zelfstandig de deuren openen.
De omgeving van Wijzer kan kort gezegd in vier zones ingedeeld worden.

Zone 0: de omgeving en het gebouw
- het gebouw is voorzien van inbraakbeveiliging, ter afhandeling van een inbraakincident geldt een gemeentelijk protocol
- de contactpersonen die verwittigd worden bij een beveiligingsincident staan genoemd in het protocol
- de personeelsingang wordt beveiligd door middel van een elektronische sleutel en 24 uurs camerabewaking.

Zone 1: de wachtruimten en spreekkamers
- In de wachtruimten wordt door een daartoe aangestelde beambte en/of de receptionist opgetreden bij dreigende situaties.
- De wachtruimte wordt bewaakt door middel van videobewaking.
- In de spreekkamers is stil alarm aanwezig en binnen (hand)bereik van de medewerkers.
- Eén spreekkamer is voorzien van een beveiligingscamera.
- Voor de afhandeling van dreigende situaties geldt het draaiboek veiligheid.(agressieprotocol)

Zone 2: de werkruimten
- Voor toegang tot zone 2 wordt een badgesysteem gehanteerd
- Voor bezoekers van de werkruimten geldt dat zij bij de receptie een bezoekersbadge krijgen uitgereikt welke zichtbaar gedragen moet worden gedurende het bezoek.
- Bezoekers zonder badge moeten worden aangesproken,
- Bezoekers moeten worden opgehaald bij de receptie en weer teruggebracht.
- Onderhoudsmedewerkers van leveranciers, installatiebedrijven etc. die geacht worden werkzaamheden te verrichten dienen zich te kunnen legitimeren als zijnde medewerker van

het betreffende bedrijf. De begeleiding vindt plaats door de afdeling F&I. (Team Facilitair Beheer)

Zone 3: ICT-ruimte

- Deze zone is gesitueerd op de eerste verdieping.
- Bezoekers (waaronder inwoners) zijn niet toegestaan.
- Dient niet als opslagruimte.
- De toegang is enkel mogelijk met een afzonderlijke sleutel.
- Bij de afdeling F&I is altijd bekend wanneer onderhoudsmedewerkers werkzaamheden komen verrichten.
- Alleen actieve apparaten bevinden zich in de server ruimte.

7.3 Fysieke toegangsbeveiliging

Omdat onze afdeling op verschillende manieren betreden kan worden, zijn ook afzonderlijke maatregelen genomen om dit te beveiligen. In deze paragraaf staat op welke manier dit is gebeurd.

Personeelsingang
Deze ingang is gelegen aan de Landstraat en wordt beveiligd met behulp van een pasjessysteem en 24 uurs camerabewaking. Alle medewerkers van de gemeente zijn in bezit van een elektronische sleutel om de toegangsdeur te openen van fietsenkelder en trappenhuis.

Hoofdingang
Deze ingang is gelegen aan de Brinklaan.
Toegang van de publiekstoegankelijke ruimten naar de werkruimten van medewerkers is beveiligd door middel van deuren die enkel met een elektronische sleutel geopend kunnen worden. Eventueel kunnen de deuren op verzoek van de medewerker door de receptionist geopend worden.

Serverruimte
Melding in de hal vindt plaats bij de receptie. Toegang tot de afdeling is geregeld met een aparte sleutel, die enkel de medewerkers van F&I bezitten. De serverruimten zijn ook nog apart beveiligd met behulp van een deur.

7.4 Toegangsbeveiliging bij werkzaamheden

Wanneer externen werkzaamheden moeten verrichten aan ICT-voorzieningen van Wijzer worden deze ingehuurd via de afdeling F&I. De afdeling F&I is verantwoordelijk voor de benadering van de firma's en eventuele planning. Uiteraard worden enkel bonafide bedrijven benaderd om werkzaamheden voor de gemeente te verrichten. Als extra beveiliging, wordt de serverruimte bij onderhoudswerkzaamheden enkel betreden in aanwezigheid van een medewerker van de afdeling F&I. Onderhoudsmonteurs en anderen werken niet zonder toezicht in deze ruimte.
Daarnaast is toegang tot de serverruimte van de afd. F&I enkel mogelijk met een aparte sleutel. Slechts medewerkers van F&I zijn in het bezit hiervan.

Het risico dat derden inzage hebben in persoonsgegevens is bij Wijzer voldoende ondervangen. Voordat applicaties met persoonsgegevens geopend kunnen worden, moet de gebruiker verschillende inlogcodes invoeren. Zonder login kan zelfs geen gebruik gemaakt worden van het gemeentelijke netwerk.

7.5 Extern gebruik van gegevens

Het is alle medewerkers van Wijzer niet toegestaan om dossiers of digitale bestanden met klantgegevens mee te nemen buiten de beveiligde zone. Ook niet als men periodiek of tijdens ziekte wil thuiswerken.

De vraagverhelderaars zijn overigens wel uitgerust met een laptop die zij gebruiken tijdens het huisbezoek. Zij kunnen via een beveiligde internetverbinding inloggen op RD-web.

Een uitzondering is het team sociale recherche. In verband met het horen van verdachten kan het noodzakelijk zijn om dossiers dan wel digitale bestanden mee te nemen naar bijvoorbeeld het politiebureau. Op de onregelmatige tijdstippen waarop aanhoudingen plaatsvinden kan het ook noodzakelijk zijn om de gegevens een dag voorafgaand aan het verhoor al mee te nemen naar huis. Wanneer gegevens meegenomen worden buiten de beveiligde zone, dan worden dossiers, USB-sticks en laptops te allen tijden meegenomen in de woning van de medewerker en nooit achtergelaten in de auto. Er wordt uitsluitend gebruik gemaakt van USB-sticks met wachtwoordbeveiliging. De laptops zijn eveneens met een wachtwoord beveiligd en na afloop van de actie waarbij de laptop of de USB-stick noodzakelijk was, worden alle bestanden op het netwerk van de gemeente geplaatst en gewist van de laptop c.q. USB-stick.

RD Web
Thuiswerken wordt mogelijk gemaakt via RD Web. Het privacy protocol gebruik van elektronische communicatiemiddelen is van toepassing. Dit protocol is vastgesteld op 5 november 2013 en gepubliceerd op Intranet.

Hoofdstuk 8. Beheer van communicatie- en bedieningsprocessen

8.1 Bedieningsprocedures en verantwoordelijkheden

In deze paragraaf is beschreven welke procedures er gelden binnen Wijzer op het gebied van aanpassingen, incidenten en functiescheiding op ICT-gebied.

Wijzer garandeert een correcte en veilige bediening van ICT-voorzieningen.
De implementatie van eventuele patches wordt geregeld door F&I. In overleg met de applicatiebeheerder Wijzer wordt een datum geprikt om tot feitelijke installatie over te gaan.
Wanneer op ICT gebied veranderingen plaatsvinden worden de medewerkers van de dienst daarover in kennis gesteld via de applicatiebeheerder.
Enkel medewerkers van F&I. zijn bevoegd om wijzigingen in de ICT-infrastructuur aan te brengen. Op deze manier wordt voorkomen dat op verschillende plaatsen binnen de organisatie wijzigingen plaats moeten vinden en kunnen de zaken collectief beheerst worden.
De gemeente maakt bij calamiteiten op ICT-gebied gebruik van een vastgestelde methode. Deze ITIL-methode geeft aan dat problemen door middel van een procedure worden afgehandeld. Verdere informatie is te vinden bij de afdeling F&I.

Iedere medewerker van de gemeente heeft enkel toegang tot ICT-voorzieningen die noodzakelijk zijn voor de uitoefening van zijn/haar werkzaamheden. Er is duidelijk sprake van functiescheiding. Per functionaris verschillen, indien van toepassing, de autorisaties. (a.h.v. toegekende autorisaties aan “Gebruikersgroepen”) Op deze manier wordt misbruik van voorzieningen tegengegaan.
Achteraf vindt er controle plaats op het gebied van de rechtmatigheid van het gebruik van de applicaties. Deze controle wordt voor Wijzer uitgevoerd door de applicatiebeheerder.

Voor de uitvoerende werkzaamheden bij Wijzer wordt gebruik gemaakt van diverse automatiseringspakketten waaronder GWS4all, Suwinet, het regiesysteem Top en het Digitaal Leefplein van de regio. Van GWS4all is zowel een testomgeving als een productieomgeving voorhanden. Nieuwe releases of patches worden eerst getest in de testomgeving alvorens gekopieerd wordt naar de productieomgeving. Voor Top en Suwinet is er een ‘demo-omgeving’ waarin nieuwe medewerkers kunnen oefenen voordat zij daadwerkelijk met de applicaties aan de slag gaan. De regio is verantwoordelijke voor het beheer van het Digitaal Leefplein.
Het team sociale recherche maakt geen gebruik van deze systemen maar werkt met Liaan SZFraude voor de uitvoerende werkzaamheden. In de bijlage staan alle applicaties vermeld die bij Wijzer worden gebruikt.

8.2 Systeemplanning en acceptatie

Aangegeven wordt op welke manier nieuwe patches en releases worden geïmplementeerd.
Bij F&I wordt periodiek bekeken of de capaciteit van de verschillende servers van de gemeente nog voldoende is. De medewerkers van Wijzer hebben hierin geen rol anders dan het via de applicatiebeheerder signaleren naar de afdeling F&I dat vertraging in de verwerking van gegevens binnen het systeem ontstaat.
Nieuwe releases en updates van GWS worden eerst in de testomgeving uitgeprobeerd, alvorens implementatie in de productieomgeving plaatsvindt. Op deze wijze wordt het risico van foutmeldingen geminimaliseerd. Bij de feitelijke implementatie van wijzigingen wordt overleg gevoerd tussen F&I en de applicatiebeheerder van Wijzer.

8.3 Bescherming tegen kwaadaardige software

Deze paragraaf geeft de maatregelen weer die zijn genomen om het binnendringen van kwaadaardige software te voorkomen en te ontdekken.
De gemeente gebruikt voor haar netwerk een firewall om kwaadaardige aanvallen van buitenaf te voorkomen. De verantwoordelijkheid van deze firewall ligt bij F&I.
Naast het gebruik van een firewall, gebruikt de gemeente ook antivirus software.
Deze antivirus software is zowel op de servers geplaatst als op alle werkplekken. F&I garandeert dat gebruikt gemaakt wordt van de laatste geactualiseerde versie (hierover zijn contracten afgesloten met leveranciers). USB-sticks dienen voor gebruik op het netwerk bij de afdeling F&I gescand te worden op virussen en kwaadaardige software.
Voor het gebruik van USB-sticks wordt gesteld dat deze enkel mogen worden gebruikt met toestemming van de leidinggevende. Hierbij wordt ook gesteld dat de functionaris wordt geacht activiteiten die risico's kunnen opleveren, zoals het verspreiden van virussen of het plaatsen van gevoelige data te vermijden.

Hoofdstuk 9. Toegangsbeveiliging

9.1 Beleid ten aanzien van toegangsbeveiliging

Aangegeven wordt welke richtlijnen met betrekking tot toegangsbeveiliging bij de gemeente zijn gedefinieerd. Binnen Wijzer is vastgelegd dat enkel personen die binding hebben met de primaire processen toegang krijgen tot GWS4all, Top, Digitaal Leefplein, Liaan SZFraude en Suwinet. In het kader van de informatievoorziening ontvangt iedere medewerker enkel autorisaties voor de voor hem relevante applicaties. Het afdelingshoofd bepaalt in relatie tot de taakuitoefening welke functionarissen toegang hebben tot de onderscheiden systemen aan de hand van een door hem vast te stellen autorisatiestructuur.

9.2 Management van toegangsrechten/autorisatiebeheer

9.2.1 Registratie van gebruikers

Nieuwe medewerkers ontvangen via F&I binnen afgesproken termijnen een user-id en een gebruikersprofiel. Afhankelijk van de afdeling waar de nieuwe medewerker is geplaatst vindt toewijzing van applicaties aan het desbetreffende gebruikersprofiel plaats. Voor alle Wijzer medewerkers geldt dat zij bij indiensttreding, via/door de applicatiebeheerder, voor alle benodigde pakketten voor de functie, een gebruikersID en wachtwoord krijgen. Bij uitdiensttreding ziet de applicatiebeheerder erop toe dat iedereen weer wordt afgemeld/verwijderd voor de toegewezen software. Dit gaat a.d.h.v. een checklist van alle applicaties die binnen Wijzer voorhanden zijn.

Binnen Wijzer is afgesproken dat enkel medewerkers die werkzaam zijn in het primaire proces, de handhavers en de sociale rechercheurs toegang krijgen tot SUWI-net en wordt enkel voor hen een

gebruikersaccount en wachtwoord aangemaakt. Naast inloggen op het gemeentelijk netwerk is een aparte inlog noodzakelijk voor GWS4All en SUWI-net.

9.2.2 Speciale bevoegdheden

Er zijn bij Wijzer geen medewerkers met speciale bevoegdheden aanwezig. Met speciale bevoegdheden wordt bedoeld dat het mogelijk is als gebruiker de normale beveiliging in systemen of toepassingen te omzeilen.

9.2.3 Beheer gebruikerswachtwoorden

Om te voorkomen dat medewerkers gedurende zeer lange tijd hetzelfde wachtwoord gebruiken, dienen zij na een afgesproken periode het netwerkwachtwoord te wijzigen. Voor GWS4ALL en o.a. het SUWI-net wordt na een bepaalde periode automatisch om een nieuw wachtwoord gevraagd. Dit om misbruik van de wachtwoorden te voorkomen. De frequentie waarmee dit gebeurt is 90 dagen.

9.2.4 Verificatie van de toegangsrechten

Periodiek controleert de applicatiebeheerder de toegangsrechten van de medewerkers, door middel van het opvragen van de loggings. Dit om misbruik van de userID / wachtwoorden te voorkomen. Binnen Wijzer wordt per pakket per medewerker een bepaalde set van data-gegevens beschikbaar gesteld, dit is afhankelijk van de functie van de medewerker. M.b.t. het SUWI-net vraagt de applicatiebeheerder van Wijzer periodiek specifieke rapportages bij het BKWI op over onder andere de logging.

9.3 Verantwoordelijkheden van gebruikers

De richtlijnen die gelden binnen Wijzer met betrekking tot gebruik van wachtwoorden en apparatuur staan verwoord in dit hoofdstuk en zijn opgenomen in de bijlage als ‘de 10 gouden regels’ (zie bijlage). Dit document wordt aan alle (nieuwe) Wijzer medewerkers uitgereikt en moet een vast onderdeel worden van de checklist ‘nieuwe personeel’.

Effectieve beveiliging vereist de medewerking van de gebruikers. Zij moeten daarom worden gewezen op hun verantwoordelijkheid voor het handhaven van effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden en de beveiliging van gebruikersapparatuur.

9.3.1 Gebruik van wachtwoorden

Medewerkers van Wijzer zijn zelf verantwoordelijk voor het voorkomen van ongeautoriseerde toegang. Dit betekent dat zij op een verantwoorde wijze om moeten gaan met wachtwoorden en registratie daarvan. Kenbaar gemaakt is dat wachtwoorden strikt persoonlijk zijn en niet uitgewisseld moeten worden tussen collega’s (uitzonderlijke noodsituaties uitgesloten).
Na eerste aanmelding dient de gebruiker het wachtwoord te wijzigen in een voor hem makkelijk te onthouden combinatie. Periodiek verschijnt de melding dat het wachtwoord voor netwerktoegang of / is verlopen en dat een nieuw wachtwoord moet worden ingevoerd.

9.3.2 Onbeheerde gebruikersapparatuur

Voorkomen moet worden dat tijdelijk onbeheerde gebruikersapparatuur ongeoorloofd gebruikt wordt om toegang te krijgen tot persoonsgegevens.
In principe is geen enkele computer toegankelijk voor klanten of derden. Enkel de medewerkers van Wijzer zijn bevoegd tot gebruik hiervan. Ongeoorloofd gebruik door klanten is niet mogelijk.
Bij het verlaten van de van de werkplek door de medewerker wordt na enkele minuten de schermbeveiliging ingeschakeld die alleen met het eigen wachtwoord opgeheven kan worden. Ook het gebruik van de “windows” toets + L, waardoor direct de schermbeveiliging wordt aangeroepen bij het verlaten van de werkplek, wordt gepropageerd. Bij het opstarten van elk werkstation is de gebruiker verplicht een user-id en wachtwoord in te geven voordat van het gemeentelijke netwerk gebruik gemaakt kan worden. Om vervolgens de afzonderlijke applicaties te starten moet ook per applicatie een user-id en wachtwoord ingevoerd worden.

9.3.3 Cleandesk policy

De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegden niet in afwezigheid van een medeweker aan gegevens kan komen. Dat betekent dat het werkstation bewust moet worden vergrendeld met behulp van de screensaver wanneer de werkplek wordt verlaten. Ook mogen geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau of in een kast blijven liggen. Aan het eind van de dag moeten alle dossiers zijn teruggebracht naar het dynamisch archief (lectrievers). Met name omdat er zoveel mogelijk papierloos en flexibel gewerkt gaat worden.

9.3.4 Lectrievers

Voor de lopende persoonsdossiers binnen Wijzer zijn een tweetal lectrievers beschikbaar. Deze lectrievers worden 's ochtends geopend en aan het einde van de werktijd afgesloten. Dossiers kunnen gedurende de dag worden opgehaald en teruggebracht. De gesloten dossiers worden gearchiveerd in de kelder en vallen onder de verantwoordelijkheid van F&I.

9.3.5 Printers

Documenten kunnen slechts worden uitgeprint met behulp van een elektronische sleutel waarmee kan worden ingelogd. Na het printen moet weer worden uitgelogd. Prints mogen niet onbeheerd bij de printers blijven liggen en moeten einde werktijd altijd zijn opgehaald.

9.4 Verantwoordelijkheden t.a.v. netwerken

Belangrijk om te noemen is dat de afdeling F&I de toegang tot de interne en externe netwerkdiensten dient te beheren en te beheersen.
Binnen de gemeente Bussum wordt gebruik gemaakt van een gemeentelijk netwerk (Intranet) dat onder verantwoordelijkheid valt van F&I. De concrete invulling staat verwoord in de onderstaande sub-paragrafen.

9.4.1 Beleid ten aanzien van netwerkdiensten

Iedere medewerker van Wijzer ziet na het inloggen op het gemeentelijke netwerk enkel de applicaties waar hij voor geautoriseerd is.

9.4.2 Datatransport

Alle datatransport vindt plaats door middel van vaste bekabeling welke gecontroleerd is op betrouwbaarheid. Het datanetwerk is getoetst aan vastgestelde normen.

Hoofdstuk 10. Ontwikkeling en onderhoud van systemen

10.1 Beveiligingseisen voor systemen

Aangegeven is op welke wijze de infrastructuur van het netwerk is ingericht bij Wijzer.
Bij de gemeente Bussum wordt gebruikt gemaakt van één groot netwerk, verdeeld over verschillende servers.
Elke medewerker van de gemeente kan inloggen op iedere werkplek binnen de gemeente. Op elke werkplek is de inlogprocedure gelijk.
Het beheer en onderhoud van de informatiseringsnetwerken is de verantwoordelijkheid van F&I.

10.2 Beveiliging van toepassingssystemen

Bij Wijzer is het individuele werkstation van de medewerker beveiligd. Hier staat vermeld op welke manier dit gebeurt. Iedere medewerker moet zijn eigen toegekende inlognaam en wachtwoord intoetsen alvorens verbinding met het gemeentelijke netwerk kan worden gemaakt.
Iedere medewerker die de mogelijkheid heeft om van de applicatie Suwi-inkijk gebruik te maken heeft een aparte inlognaam ontvangen, voorzien van een wachtwoord.

Velden met sleutelgegevens zijn afgeschermd om wijzigingen aan de instellingen te voorkomen.

10.3 Cryptografische beveiliging

Binnen de gemeente wordt geen gebruik gemaakt van cryptografische versleuteling bij data verzending.

10.4 Beveiligen van systeembestanden

Servers van de gemeente zijn helemaal niet toegankelijk voor individuele gebruikers. Enkel bepaalde medewerkers van F&I zijn bevoegd om systeembestanden te benaderen.

10.5 Beveiliging bij ontwikkel- en ondersteuningsprocessen

Met de komst van het ITIL proces worden wijzigingen in applicaties automatisch gevolgd via een vastgestelde procedure.

Hoofdstuk 11. Continuïteitsmanagement

Binnen Wijzer is een proces gestart dat er op gericht is om calamiteiten en incidenten tot een aanvaardbaar niveau te beperken. Welke concrete maatregel worden genomen staat in deze paragraaf.

11.1 Aspecten van continuïteitsmanagement

Binnen Wijzer is het primaire proces beveiligd tegen uitval van het ICT-systeem. Wanneer er verstoringen optreden voor het primaire proces, worden noodplannen in werking gezet. Inzake calamiteiten zoals brand, bommeldingen etc. is het calamiteitenplan van kracht.

Op dit moment wordt door Wijzer in samenwerking met F&I gebruik gemaakt van de zogenaamde uitwijkprocedure en backup procedure. Op de Huizerweg in Bussum is een volledig tweede systeem beschikbaar. Er zijn noodplannen beschikbaar zodra bijvoorbeeld stroomstoringen optreden. (noodaggregaat).

Hoofdstuk 12. Naleving

12.1 Naleving van wettelijke voorschriften

In deze paragraaf wordt de link gelegd tussen informatiebeveiliging en ander, flankerende, wetgeving. Wijzer heeft op verschillende onderdelen te maken met wetgeving waar zij aan moet voldoen. Zaken die te maken hebben met de WBP, Archiefwet en Wet SUWI zijn beschikbaar in het afdelingsarchief Wijzer en het algemene archief dat in het hoofdgebouw (afdeling F&I, team DIV) is gevestigd.
Wijzer maakt gebruik van verschillende applicaties. Er kan een onderscheid gemaakt worden tussen applicaties die enkel gebruikt worden door onze dienst en applicaties die (concern) gemeentebreed worden gebruikt.

Voor de applicaties die enkel gebruikt worden bij Wijzer is het hoofd Wijzer verantwoordelijk. Alle gebruikte applicaties staan vermeld in de bijlage.

De informatie inzake deze en de overige applicaties wordt centraal via ICT geregistreerd en gedocumenteerd.

NB. Naast bovengenoemde verantwoordelijkheden voor ICT-voorzieningen is het hoofd van Wijzer primair verantwoordelijk voor de beveiliging van de in gebruik zijnde fysieke archieven. Aanvragen en afmelden van autorisaties (in een logboek) t.b.v. Bussums personeel met toegang tot de externe koppelingen naar de gemeenten Muiden en Naarden ligt in handen van de applicatiebeheerder van Wijzer.

12.2 Beoordeling van de naleving van het beveiligingsbeleid en de technische vereisten

12.2.1 Privacy protocol

In 2015 is een regionaal privacy protocol vastgesteld door de colleges van de regiogemeenten. In dit protocol is opgenomen hoe met gegevensverwerking moet worden omgegaan en hoe de uitwisseling met partners plaats vindt. Dit protocol is besproken in de werkoverleggen van de verschillende teams en alle medewerkers van Wijzer hebben digitaal een exemplaar ontvangen. Dit privacy protocol is geen statisch document maar zal gedurende de tijd worden aangepast en uitgebreid, waar nodig. Het privacy protocol is opgenomen als bijlage.

12.2.2 Protocol internetgebruik en e-mail gebruik

Binnen de gemeente is een protocol van kracht waarin medewerkers op de hoogte gesteld worden van de richtlijnen hoe om te gaan met internetgebruik- en e-mail gebruik.
Dit protocol is ook nog voor iedere medewerker toegankelijk via het gemeentelijk intranet.

Hoofdstuk 13. Managementcyclus

13.1 Aandachtspunten

Dit plan bevat een uitwerking van de normen van het BKWI, beveiligingsmaatregelen en een beperkte uitwerking van het privacy protocol. Veel is geregeld en vastgelegd maar er zijn ook nog verbeter- en aandachtspunten in de dagelijkse praktijk. De volgende zaken moet nader geregeld en/of uitgewerkt worden.

13.1.1 Verbeter/aandachtspunten in relatie tot BKWI normen

<u>Norm 1.4 BKWI Uitdragen</u>
Dit beveiligingsbeleid en –plan moet periodiek op de agenda's van de werkoverleggen komen. Het moet worden gepubliceerd op Intranet en (eventueel) in een voorlichtingsbijeenkomst onder de aandacht worden gebracht. Regelmatig moet worden verwezen naar de '10 gouden regels' (zie bijlage).

<u>Norm 1.5 BKWI Evalueren en actualiseren en rapporteren</u>
Het beveiligingsbeleid en – plan moet minimaal jaarlijks worden geëvalueerd en geactualiseerd. Het college wordt in kennis gesteld door middel van een rapportage. Deze rapportage wordt gebruikt om de gemeenteraad te informeren over de stand van zaken rond het beveiligingsbeleid. Door aan te sluiten bij de P&C cyclus wordt deze norm geborgd.

<u>Norm 2.2 BKWI functiescheiding</u>
Nader onderzocht moet worden waar er sprake is van onverenigbare functies en hoe dit gescheiden kan worden.

<u>Norm 2.3 BKWI Security Officer</u>
Er moet een Security Officer worden aangewezen die zorgt voor het beheer van de beveiligingsprocedures, veilig gebruik bevordert en adviseert. Deze verzorgt rapportages over de status en controleert en zorg voor de naleving. De Security Officer is eindverantwoordelijk en rapporteert rechtstreeks den de bestuurlijk verantwoordelijke.

Norm 13.1 BKWI Autorisatiestructuur
Er moet een formele autorisatieprocedure zijn. Deze procedure is op basis van functieverdeling. Het informatiebeveiligingsplan regelt autorisatie, authenticatie en logging.

Norm 13.5 BKWI Controle
Periodiek moeten de toegangsrechten en loggings worden gecontroleerd.

13.1.2 Verbeter/aandachtspunten in relatie tot het privacy protocol

Hoewel in regionaal verband het privacy protocol in relatie tot regie verder wordt uitgewerkt, moet lokaal aandacht zijn voor de volgende punten:

- De integriteitsverklaring wordt door inhuurmedewerkers ondertekend maar archivering moet worden geborgd.
- De toestemmingsverklaring van inwoners over gegevensverstrekking moet worden geborgd
- Klachten- en bezwaarprocedure is al opgenomen in het privacy protocol

13.1.3 Verbeter/aandachtspunten met betrekking tot gegevensverwerking/deling

Er ligt veel (wettelijk) vast over gegevensverwerking. Om te borgen dat de verwerking correct en volgens de protocollen gebeurt, moet het volgende nader worden onderzocht, uitgewerkt en geïmplementeerd:

- Per proces moet beschreven zijn wat de risico's en beheermaatregelen zijn inzake privacy en beveiliging
- Per proces moet worden beschreven wat het doel en de grondslag is
- Gebruikers mogen alleen toegang hebben tot de persoonsgegevens die voor hen noodzakelijk zijn voor de uitvoering van hun taken. De beschrijvingen van de werkprocessen vormen hierbij het uitgangspunt
- Er moet intern geaudit worden op gegevensverwerking

13.1.4 Overige aandachtspunten

- Risico analyses per proces uitvoeren inzake privacy en beveiliging
- Afspraken maken met het college over de wijze van rapporteren
- Professionals trainen in bewustwording met betrekking tot informatiebeveiliging, privacy en gegevensverwerking

13.2 Verbeterplan

Nu de aandachtspunten/verbeterpunten in kaart zijn gebracht moet een verbeterplan worden opgesteld. Daarvoor moet een projectgroep(je) worden ingesteld onder leiding van de Security Officer. Deze bepaalt wie erbij betrokken moet worden, welke punten prioriteit hebben, wat er gedaan moet worden, hoeveel tijd het mag kosten en wanneer het plan gereed is. Het plan wordt vastgesteld door het managementteam Wijzer. Na vaststelling kan het plan worden uitgevoerd.

13.3 Acties

De volgende acties zullen moeten worden uitgevoerd:

Welke	Wie	Wanneer
Integriteitsverklaring inhuurkrachten borgen	Teamleiders	Augustus 2015
Toestemmingsverklaring borgen	Teamleider VVK/VVH	Augustus 2015
Het afdelingshoofd stelt een autorisatiestructuur vast	Afdelingshoofd	Augustus 2015
Per proces wordt de gegevensverwerking, de risico's, de instructies en de autorisatie beschreven.	Bedrijfsvoering	Voor 1 januari 2017
Plan maken interne audit op gegevensverwerking	Bedrijfsvoering	Vóór 1 januari 2016
Aanpassen checklist 'nieuw personeel' door opname gebruikershandleiding Suwi en instructie beveiligingsbeleid	Bedrijfsvoering	Augustus 2015
Afspraken maken met college over rapporteren aan de Raad	Beleid	Voor 1 januari 2016
Publicatie beveiligingsbeleid en –plan op intranet en distributie per mail aan medewerkers.	Bedrijfsvoering	Na vaststelling B&W
Professionals trainen in bewustwording van privacy en informatiebeveiliging	Bedrijfsvoering	2x per jaar. Voor het eerst in najaar 2015
Verstrekken handleiding en 10 gouden regels opnemen in checklist nieuw personeel	Bedrijfsvoering	Augustus 2015
Controle en naleving cleandesk policy	Management Wijzer	Periodiek
Verbeterplan opstellen	Bedrijfsvoering	Voor 1 januari 2016

13.4 Evaluatie en bijstelling

Als het verbeterplan is uitgewerkt en geïmplementeerd zal na een vooraf vastgestelde periode een evaluatie moeten plaatsvinden. De eerder aangestelde projectleider is daartoe de aangewezen persoon. Deze zorgt voor een puntsgewijze evaluatie, waarbij wordt aangegeven of er opnieuw actie moet worden ondernomen en er nog bijstelling plaats moet vinden. Als alles is afgerond volgens eerder vastgesteld plan, kan een nieuw (aangepast) beveiligingsplan worden opgesteld.

Bijlagen

Bijlage 1. Privacy Protocol Sociaal Domein

Inleiding

De gemeenten Naarden, Muiden en Bussum willen integrale en effectieve ondersteuning bieden aan haar inwoners bij vragen en problemen op het gebied van zorg, welzijn en inkomen. Ondersteuning die aanvullend is op de eigen mogelijkheden van de inwoner en zijn (of haar) sociale netwerk. Ondersteuning als inwoners zichzelf melden, maar ook proactief op basis van signalen dat ondersteuning noodzakelijk en gewenst is.

Om dit mogelijk te maken moeten wij persoonsgegevens verwerken en uitwisselen met partners in de regio, zoals instellingen voor thuiszorg of jeugdzorg. Dat willen we rechtmatig en zorgvuldig doen. We willen transparant en duidelijk zijn hoe we omgaan met de privacy van onze inwoners en betrokkenen. In dit protocol is uitgewerkt hoe wij dit doen. Het protocol bevat algemene regels, geen antwoord op elke vraag. Het antwoord is namelijk sterk afhankelijk van een zorgvuldige afweging van belangen die per situatie kan verschillen.

Dit protocol is opgesteld binnen de context van het sociaal domein waarin, op basis van wet- en regelgeving (zie hiervoor de bijlage: Van toepassing zijnde wet- en regelgeving), er duidelijke kaders zijn voor het omgaan met privacy. Het vormt geen zelfstandige grondslag voor gegevensuitwisseling en –verwerking. Het protocol is bedoeld als leesbare uitwerking van deze regels voor inwoners, medewerkers en anderen. En moet leiden tot een eenduidige werkwijze voor het verwerken van gegevens voor alle gemeenten in de regio.

Belangrijke begrippen

Betrokkene	de (natuurlijke) persoon op wie een persoonsgegeven betrekking heeft.
Bestand	een gestructureerde verzameling persoonsgegevens, die volgens bepaalde criteria toegankelijk is;
Bewerker	een partij die in opdracht persoonsgegevens verwerkt, maar die niet direct onder de verantwoordelijkheid/ aansturing van de gemeente Naarden, Muiden of Bussum valt;
Bijzondere persoonsgegevens	persoonsgegevens over religie/ levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele geaardheid, lidmaatschap van een vakvereniging, strafrechtelijke gegevens, persoonsgegevens over hinderlijk/ onrechtmatig gedrag in verband met een opgelegd verbod;
Persoonsgegevens	alle gegevens die betrekking hebben op een geïdentificeerde of een identificeerbare natuurlijke persoon (betrokkene);
Verantwoordelijke	degene die (binnen de eindverantwoordelijkheid van het college) de uitvoerende verantwoordelijkheid heeft voor het beheer van persoonsgegevens. Dit is voor het Sociaal Domein het afdelingshoofd;
Verwerking van persoonsgegevens	elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, samenbrengen, met elkaar in verband brengen, afschermen, wissen of vernietigen;
Verwijzer	een beroepskracht die op basis van contacten met een inwoner een behoefte aan ondersteuning ziet en de inwoner aanmeldt.
Wijzer	Uitvoeringsdienst Sociaal Domein voor de gemeenten Naarden, Muiden en Bussum

Doel van de gegevensverwerking

Doel van de gegevensverwerking binnen het Sociaal Domein is het bieden van ondersteuning aan inwoners van onze gemeenten bij vragen of behoeften op het gebied van zorg, welzijn en inkomen, aansluitend op de mogelijkheden waarover zijzelf en hun sociale netwerk beschikken.

Om dit doel te bereiken moeten wij persoonsgegevens verwerken, waaronder ook *bijzondere persoonsgegevens* (namelijk strafrechtelijke gegevens en gezondheidsgegevens), passend bij het doel van de gegevensverwerking, dus in termen van het effect op de benodigde ondersteuning, waarbij niet meer wordt vastgelegd dan noodzakelijk!

In brede zin omvat de verwerking ook het evalueren van de ondersteuning en het voldoen aan verplichtingen ten aanzien van (financiële) verantwoording en beleidsontwikkeling/ onderzoek. Maar in deze gevallen (met uitzondering van onderzoek naar een individuele persoon) worden de gegevens bewerkt zodat deze niet te herleiden zijn naar geïdentificeerde / te identificeren personen.

Toepassingsgebied

Dit protocol is van toepassing op de verwerking van persoonsgegevens binnen het Sociaal Domein (zorg, welzijn en inkomen), niet op de verstrekking van gegevens *aan* de gemeente door andere partijen (zorgaanbieders, scholen of 'Veilig Thuis'). Welke informatie zij mogen verstrekken wordt bepaald door de privacywetgeving waaronder de betreffende partij valt en hun eigen privacyregelingen.

Verantwoordelijkheden van management en medewerkers

Alle medewerkers van Wijzer en alle ingehuurde medewerkers hebben een integriteitsverklaring getekend, waarin het omgaan met vertrouwelijke gegevens (zoals plicht tot geheimhouding) is vastgelegd. Iedereen die (binnen het doel van de gegevensbewerking) bevoegd is om persoonsgegevens te bewerken zorgt ervoor dat:

- deze gegevens rechtmatig verkregen zijn en juist, volledig en ter zake zijn;
- er afdoende maatregelen genomen zijn om deze gegevens te beveiligen;
- verwerking gebeurt conform dit protocol en ontvangen instructies over beveiliging van persoonsgegevens.

De hoofdregels voor zorgvuldig omgaan met privacy

1. de verwerking van persoonsgegevens moet passen binnen het doel waarvoor deze verstrekt zijn. Er mogen niet méér persoonsgegevens verwerkt worden dan noodzakelijk;
2. elke betrokkene heeft recht om te weten wat er over hem is vastgelegd. Het recht op inzage (en afschrift, correctie of vernietiging) beperkt zich tot de *eigen gegevens*;
3. het opvragen van of verstrekken van gegevens aan derden gebeurt op basis van een *wettelijke grond* of op basis van *bewuste toestemming van de betrokkene* als deze ontbreekt. Als de noodzakelijke hulpverlening niet op gang kan komen omdat de noodzakelijke toestemming geweigerd wordt kan in bepaalde gevallen worden afgeweken van deze regel.

De hoofdregels zijn redelijk overzichtelijk en duidelijk, de werkelijkheid is weerbarstiger. Hoe complexer een zaak, hoe meer de afweging gemaakt moet worden tussen het verwerken van extra persoonsgegevens versus de noodzaak voor ondersteuning.
De behandelend ambtenaar moet zich continu afvragen: is het noodzakelijk voor gestelde doel, is er een wettelijke grondslag, kan het ook met minder/ anders, is het nog proportioneel, zijn er beperkingen of specifieke regels, is er sprake van een vitaal belang of is de veiligheid van betrokkene of anderen in gevaar?

Informeren en het vragen van toestemming

Binnen het Sociaal Domein wordt een heel scala aan vragen en aanvragen behandeld, van eenvoudig tot en met 'multiprobleem gezinnen' met een complexe problematiek. *Voor veel taken is er een wettelijke basis voor het verwerken van gegevens*, en over het algemeen is het verband tussen de benodigde gegevens en het doel bij deze zaken duidelijk zichtbaar. Denk aan het aanvragen van een uitkering of een rolstoel. Wij gaan ervan uit dat dit duidelijk is voor de betrokkene, en dat toelichting op de gegevensverwerking niet noodzakelijk is tenzij de betrokkene hier behoefte aan heeft.

Bij zaken waarbij wij vermoeden dat de relatie tussen doel en gegevens voor de betrokkene minder duidelijk is, en/of waar toestemming voor verwerking noodzakelijk is, wordt de betrokkene *zo spoedig mogelijk (waar mogelijk vooraf) geïnformeerd*:

- Met welk doel de gegevens worden verwerkt;
- Indien van toepassing, welke verwijzer de betrokkene aangemeld heeft en welke gegevens deze heeft verstrekt;
- Bij wie welke gegevens opgevraagd gaan worden en aan wie welke gegevens verstrekt worden om de benodigde ondersteuning te kunnen leveren;
- Welke rechten de inwoner heeft als het gaat om de verwerking van zijn gegevens en hoe deze rechten uit te oefenen.

Als *toestemming voor het verwerken van gegevens noodzakelijk* is dan wordt de cliënt zo vroeg mogelijk in het traject om toestemming gevraagd, maar vóórdat er gegevens worden opgevraagd bij of verstrekt aan derden. De gegeven toestemming wordt vastgelegd in het dossier. De medewerker maakt de afweging of vastlegging middels een aantekening in het dossier volstaat of dat, gezien de belangen/ risico's, er een *toestemmingsformulier* getekend moet worden.

Verwijzing en (anonieme) signalen

Als gemeente ontvangen wij verwijzingen en signalen over een behoefte aan ondersteuning. Deze signalen en verwijzingen kunnen zowel via professionele verwijzers (zoals artsen) binnenkomen als via (al dan niet anonieme) inwoners. Wij gaan er bij professionele verwijzers van uit dat zij, vanuit hun professionaliteit en hun eigen privacy regels, vooraf de betrokkene hebben geïnformeerd en toestemming hebben gevraagd voor aanmelding en het verstrekken van gegevens. Dit wordt bij voorkeur schriftelijk vastgelegd.
Als er geen toestemming wordt gegeven of kan worden gegeven maar er is wel een dringende noodzaak (vitaal belang) dan zal een professionele verwijzer vanuit een wettelijke plicht alsnog een signaal afgeven.

Bij professionele verwijzers informeren wij de betrokkene over wie de aanmelding gedaan heeft en welke gegevens verstrekt zijn. Bij signalen van anderen (al dan niet anoniem) vermelden wij de naam alleen met toestemming van de melder. Zowel aanmeldingen als signalen *bespreken wij met de betrokkene vóór verdere verwerking*, tenzij er aanwijzingen zijn dat de veiligheid van betrokkene, gezin of anderen wordt bedreigd.

Toegang tot persoonsgegevens in het bestand

De persoonsgegevens in het bestand zijn afgeschermd op basis van autorisaties: enkel voor degenen die de ondersteuning (passend binnen het doel) moeten kunnen leveren, de direct leidinggevenden en degenen die belast zijn met de afhandeling van bezwaren en klachten over de geboden ondersteuning. Lees- en schrijfrechten (opnemen in bestand, aanvullen, wijzigen) zijn vastgelegd, passend bij de rol. Daarnaast wordt toegang gegeven als een wettelijke plicht daartoe noodzaakt.

Verstrekken van persoonsgegevens aan derden

Onder *'derden'* rekenen we in dit document alle partijen buiten de betrokkene en degenen die in opdracht van Wijzer gegevens verwerken (hetzij onder rechtstreeks gezag of als bewerker op basis van een bewerkingsovereenkomst) en die *ontvanger* van persoonsgegevens zijn. Bij de verstekking aan derden wordt *toestemming van de betrokkene* gevraagd (zie 'informeren en het vragen van toestemming') als een wettelijke grond voor het delen van informatie zonder toestemming ontbreekt. Toestemming waarbij de betrokkene zich ervan bewust is waarvoor toestemming gegeven wordt, en weet dat hij/zij het recht heeft om dit verzoek te weigeren! Onder deze noemer valt ook het verstrekken van persoonsgegevens in een extern overleg.

Verstrekken van persoonsgegevens zonder toestemming

In bijzondere gevallen kan besloten worden om *zonder voorafgaande toestemming* persoonsgegevens te verstrekken aan derden. In het geval dat er sprake is van een zeer ernstige situatie of dringende noodzaak, of als vitale belangen van de betrokkene (of anderen) in gevaar zijn (bijvoorbeeld bij dringende zorg of huiselijk geweld). Of als er sprake is van noodzaak, maar pogingen om toestemming te krijgen niet geslaagd zijn of toestemming vragen niet mogelijk is.

Bij een dergelijke beslissing wordt altijd vooraf overleg gevoerd met minimaal één collega en de leidinggevende, en deze beslissing wordt met argumentatie vastgelegd in het dossier. De betrokkene wordt zo spoedig mogelijk geïnformeerd over de verstrekking, dit wordt alleen uitgesteld als er concrete aanwijzingen zijn dat de veiligheid van de betrokkene, gezin of anderen wordt bedreigd.

Recht op informatie, inzage, afschrift, correctie en vernietiging

Iedere inwoner, die tenminste 16 jaar oud is en '*in staat is tot een redelijke waardering van zijn belangen ter zake*'[3], heeft het *recht op inzage* in en eventueel een *afschrift (kopie)* van de *eigen* gegevens. Andere mensen mogen deze gegevens niet inzien. Er zijn twee uitzonderingen op deze regel:
a. de wettelijk vertegenwoordiger van de betreffende inwoner
b. of een jongere van minimaal 12 jaar als het een jeugddossier betreft. Deze jongere moet dan wel in staat zijn tot waardering van zijn belangen.

Elke inwoner heeft ook het *recht op correctie of vernietiging* als de vastgelegde gegevens onjuist zijn, of als er onvoldoende relatie is tussen de gegevens en het doel van verstrekken.

Een dossier kan gegevens van meerdere personen omvatten. En dat betekent dat we bij het behandelen van de vraag om inzage beoordelen of er *geen belangen van anderen geschaad kunnen worden*. Dat kan betekenen dat (delen van) het dossier niet ingezien mogen worden. Het is aan de medewerker om een zorgvuldige afweging te maken tussen het recht op inzage van de eigen gegevens en de belangen van de andere betrokkenen. Persoonlijke werkaantekeningen en stukken die nog in bewerking zijn, worden niet gezien als onderdeel van het dossier en worden niet ter inzage/als afschrift gegeven.

Inzage en afschrift kan worden gevraagd bij de medewerker die het dossier behandeld, of door een schriftelijke aanvraag in te dienen. Een verzoek voor correctie of vernietiging moet schriftelijk worden ingediend. Inzage, afschrift, correctie of vernietiging moet 'zo spoedig mogelijk' worden gerealiseerd. Als uitgangspunt hanteren wij afhandeling van de aanvraag binnen 4 weken (en daadwerkelijke vernietiging als dit wordt toegewezen binnen 3 maanden). Inzage in het dossier is gratis, voor een afschrift kunnen kosten in rekening worden gebracht. Deze kosten worden vooraf bekend gemaakt.

De wettelijk vertegenwoordiger

De wettelijk vertegenwoordiger oefent de rechten van een betrokkene uit:
1. als deze nog geen 12 jaar oud is;
2. samen met de betrokkene als deze 12 jaar of ouder is maar nog geen 16 jaar oud is;
3. als de betrokkene 16 jaar of ouder is, maar door de leidinggevende niet in staat wordt geacht tot '*een redelijke waardering van zijn belangen ter zake*'

Is er bij punt 3 geen wettelijk vertegenwoordiger, dan worden de rechten uitgeoefend door echtgenoot/ partner, ouder, meerderjarige broer of zus of meerderjarig kind. De leidinggevende kan de rechten beperken of weigeren op grond van zwaarwegende belangen van de betrokkene.

Bewaren en vernietigen van persoonsgegevens

We hebben de wettelijke plicht om informatie gedurende een bepaalde tijd te bewaren, en moeten deze daarna vernietigen. Wij bewaren en vernietigen persoonsgegevens op basis van vaste (en over het algemeen wettelijk/landelijk vastgestelde) bewaar- en vernietigingstermijnen die kunnen verschillen per soort 'zaak'.

[3] Privacy reglement Bureau Jeugdzorg, artikel 13 lid 2

Bezwaar- en klachtenprocedure

Als een betrokkene *bezwaar* heeft tegen verwerking van zijn/haar gegevens of als inzage, correctie of vernietiging wordt geweigerd dan kan hij/zij bezwaar indienen via de onafhankelijke gemeentelijke bezwaarprocedure.

Bezwaar kan worden gemaakt als er sprake is van een besluit in de zin van de algemene wet bestuursrecht. Belanghebbenden kunnen op grond van de regels van die wet bezwaar maken tegen besluiten van het college of die namens het college worden genomen in mandaat op verzoeken van betrokkene (of diens wettelijk vertegenwoordiger).

De volgende besluiten zijn aangewezen:

- Het besluit op een verzoek om inlichtingen over de van aanmelding vrijgestelde gegevensverwerkingen;
- Het besluit op een verzoek om inzage in de gegevens;
- Het besluit op een verzoek om correctie van de gegevens;
- Het besluit op een verzoek om opgave van de derden die u hebt ingelicht over een correctie;
- Het besluit op een verzet aangetekend op grond van artikel 40 of artikel 41 van de Wbp.

Het bezwaarschrift moet worden gericht:
Aan : Burgemeester en wethouders van Bussum
Adres : Postbus 6000, 1400 HA Bussum
Termijn : Binnen zes weken na bekendmaking van de beschikking
Kosten : Geen

Inwoners van Naarden en Muiden moeten hun bezwaarschrift tegen de verwerking van de persoonsgegevens bij het college van hun woonplaats indienen.

Inhoud van het bezwaarschrift

Een bezwaarschrift moet:

1. Ondertekend zijn;
2. De naam en het adres van de indiener bevatten;
3. Dagtekening bevatten (datum);
4. Omschrijving van het besluit waartegen het bezwaar is gericht bevatten;
5. De gronden van het bezwaar bevatten (waarom bent u het er niet mee eens).

Tenslotte kunnen inwoners bij het college van hun woonplaats een klacht (in het kader van de privacy) indienen. Hoe dat in zijn werk gaat, staat op de website van de betreffende gemeente.

Lijst van toepassing zijnde regelgeving

- Artikel 8 Europees Verdrag voor de Rechten van de Mens
- Artikel 10 Grondwet
- Artikel 272 Wetboek van strafrecht
- Wet bescherming persoonsgegevens (Wbp)
- Wet maatschappelijke ondersteuning (WMO)
- Wet op de jeugdzorg (Wjz), en vanaf 2015 de Jeugdwet
- Wet en besluit politiegegevens
- Wet inzake de geneeskundige behandelingsovereenkomst
- Wet op de beroepen in de individuele gezondheidszorg
- Archiefwet, archiefbesluit en archiefregelingen
- Beroepscode van de Nederlandse Vereniging van Maatschappelijk Werkers
- Gedragscode van het Nederlands Instituut voor Psychologen
- Gedragscode van de Nederlandse Vereniging voor Onderwijskundigen en Pedagogen
- Handreiking Bemoeizorg van KNMG, GGD Nederland en GGZ Nederland

Bijlage 2. Tien gouden regels

De 10 gouden regels voor het gebruik van informatie, informatiesystemen en netwerken, zoals bij de medewerkers van Wijzer wordt uitgedragen.

Wij vragen even om jouw aandacht!

Afhankelijk van jouw functie heb jij toegang tot diverse informatiesystemen binnen Wijzer. Wij willen je erop attenderen dat het gebruik van deze systemen verbonden is aan een aantal verplichtingen. Met deze *tien gouden regels* vatten wij de belangrijkste hiervan samen. Wij verzoeken je deze goed door te lezen omdat zij deel uitmaken van je functie binnen Wijzer.

1. **Wachtwoorden zijn strikt persoonlijk**
   Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden of een collega en bewaar ze op een *veilige* plek, dus *niet* in je agenda of op een geel briefje!

2. **Melden van beveiligingsincidenten**
   Binnen de gemeente waar je werkt is een collega belast met het uitvoeren van activiteiten rond het thema informatiebeveiliging. Bij ons is dat de Applicatie beheerder Wijzer. Het is belangrijk om dit te weten, omdat beveiligingsincidenten bij deze persoon zo snel als mogelijk gemeld dienen te worden. Voorbeelden voor incidenten zijn een virusmelding op het systeem, waarmee je op dat moment werkt, een inbraak of een poging tot inbraak, of een deur die op slot had moeten zijn maar niet op slot is.

3. **Geheimhoudingsplicht**
   Binnen Wijzer wordt veel met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI en in de CAO zijn daarom geheimhoudingsbepalingen opgenomen die inhouden dat je de persoonsgegevens niet verder bekend mag maken dan voor de uitoefening van je functie noodzakelijk is. Dit betreft persoonsgegevens die jou uit hoofde van je functie bekend worden, alsmede overige informatie waarvan je weet of redelijkerwijze kunt vermoeden dat geheimhouding verplicht is.

4. **Gedragscode Internet- en e-mail-gebruik**
   In de gedragscode Internet- en e-mailgebruik zijn regels neergelegd die aangeven hoe de medewerkers behoren om te gaan met Internet en e-mail op de werkplek. Tevens bevat de code regels voor de manier waarop controle op het gebruik van de werkplek kan plaatsvinden. Deze gedragscode is op Intranet te vinden.

   E-mail verkeer geldt inmiddels als algemeen geaccepteerde correspondentie, gelijk aan brieven. E-mails kunnen, mits de betrouwbaarheid van het e-mail adres voldoende is aangetoond, gelden als bewijsstuk. Een e-mail is als het ware schriftelijke correspondentie, al dan niet voorzien van een handtekening, dat door middel van een elektronisch medium wordt verstuurd.

   Contactpersonen kunnen door middel van het verzenden van e-mails op een snelle manier informatie uitwisselen over individuele klanten.
   E-mail verkeer tussen klanten en medewerkers wordt ten zeerste afgeraden omdat deze correspondentie niet centraal wordt geregistreerd (voorzetting huidige werkwijze).
   E-mails die klanten versturen aan hun contactpersoon worden niet gezien als bewijsstuk.

5. **Kennisnemen van het informatiebeveiligingsbeleid**
   Het binnen Wijzer geldende informatiebeveiligingsbeleid en de bijbehorende richtlijnen, instructies en protocollen zijn op iedereen van toepassing. Vraag je leidinggevende voor meer informatie hierover.

6. **Gegevensverstrekking aan derden via de telefoon**
   Het uitgangspunt is dat er niet aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dat betekent dat er ook geen telefonische informatie over klanten wordt verstrekt aan personen of instanties die beweren namens de betrokkene te bellen. Vragen dienen schriftelijk te worden ingediend. Enkel in uitzonderlijke gevallen kan informatie verstrekt worden aan derden, indien de identiteit van deze voldoende vastgesteld kan worden (bijvoorbeeld door middel van terugbellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie **niet** mogelijk is.

7. **Clear desk / clear screen policy**
   De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegden niet in jou afwezigheid aan deze gegevens kunnen komen. Dat betekent dat jij je werkstation bewust dient te vergrendelen met behulp van de screensaver wanneer jij je werkplek verlaat. Ook mogen geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau of in een kast blijven liggen.

8. **Geen vertrouwelijke gegevens in de prullenbak**
   De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen Wijzer. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden. Daarom zijn er special gekenmerkte papiercontainers aanwezig. Maak hiervan gebruik en stop vertrouwelijke gegevens *nooit* in de prullenbak of in een bak op je kamer die bestemd is voor oud-papier.

9. **Aanspreken van onbekende personen zonder bezoekersbadge**
   Ben je al een keer in de situatie geweest, dat je iemand binnen het gebouw tegenkwam, waar officieel geen publiek zonder begeleiding mag komen en je niet wist wie deze persoon was en wat zij daar te doen had? Spreek deze persoon aan, stel jezelf voor en vraag, wat hij of zij hier komt doen. Nieuwe collega's, uitzendkrachten of ander ingehuurd personeel stellen het op prijs om aangesproken te worden en op deze manier contacten te kunnen leggen. Echter, personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Wijs hun beleeft, maar duidelijk, de weg naar het publieke gedeelte van het gebouw en – belangrijk – begeleidt ze daar naartoe.

10. **Haast, stress, werkdrukte vs. informatiebeveiliging**
    Informatiebeveiliging krijg je niet gratis – het kost je energie en werkt vaak tegen je als je haast hebt en de werkdrukte hoog is. Echter, informatiebeveiliging is uitermate belangrijk voor je werk en hoort bij de professionele en bekwame uitvoering van het werk. Neem het daarom zeer serieus – je inwoners vertrouwen erop!

Bijlage 3. Applicaties gebruikt bij Wijzer

Onderstaand applicaties worden gebruikt binnen Wijzer. Sommige applicaties heeft de gemeente in eigen beheer, andere zijn webapplicaties. Toegang tot alle applicaties kan slechts door middel van autorisatie. Autorisaties zijn niet gelijk voor alle medewerkers.

GWS4all (Suites)
Module documenten uitvoer
Cognos
Liaan SZFraude
GBA Naarden, Muiden, Bussum
Topicus (regiesysteem Top)
Suwinet
Erow via Suwinet
UWV omgeving
UWV Sonar
UWV WBS
G Backoffice
CAK
SVB
Mesis
COA (TVS)
CreAim
Gouw kwijtschelding
Digitaal Leefplein
Jobport
Inlichtingenbureau
DUO
Corv