Nota Informatiebeveiligingsbeleid Wijzer 2015

1. Inleiding

Wijzer is de uitvoeringsdienst Sociaal Domein van de gemeente Naarden, Muiden en Bussum en is tot aan de herindeling een organieke afdeling van de gemeente Bussum. Wijzer voert in opdracht van de colleges van B&W van deze gemeenten wetten uit binnen het Sociaal Domein, zoals de Participatiewet, de Wet maatschappelijke ondersteuning 2015, de Jeugdwet, de Wet gemeentelijke schuldhulpverlening en andere aanverwante wetten en regelingen.

In 2011 is het informatiebeveiligingsbeleid van de gemeente Bussum vastgesteld. Hiermee is een raamwerk opgeleverd voor het verbeteren van de betrouwbaarheid van de informatievoorziening en het verkleinen van de informatiebeveiligingsrisico's. Mede in verband met de eisen van het BKWI[1] inzake de geautomatiseerde gegevensuitwisseling SUWI heeft de gemeente Bussum in 2012 het beveiligingsbeleid Sociale Zaken vastgesteld, bestaande uit een beleidsplan Informatiebeveiliging en een handboek informatiebeveiliging. In 2014 is gerapporteerd over het gebruik van Suwinet in 2013.

Inmiddels is er weer veel veranderd. Zo zijn er meer handreikingen en normenkaders bij het BKWI beschikbaar waar een adequaat beveiligingsbeleid aan moet voldoen. Daarnaast is het risicoprofiel veranderd omdat door de decentralisaties meer taken, systemen en (vertrouwelijke) persoonsgegevens naar de gemeenten zijn toegekomen. In dat verband is er veel aandacht voor de uitwisseling van gegevens, ter zake waarvan SZW met een Veegwet 2015 komt om de gegevensuitwisseling beter te reguleren of te faciliteren en is er veel aandacht voor juist gebruik van het Suwinet. Als gevolg van dat laatste zal de inspectie SZW vanaf september 2015 alle gemeenten controleren. Al met al geeft dit aanleiding om het beveiligingsbeleid Sociaal Domein te actualiseren.

Het voorliggende document bevat het geactualiseerde informatiebeveiligingsbeleid Wijzer 2015 dat ziet op de gehele Uitvoeringsdienst Sociaal Domein. Het document is een onderdeel van het Bussumse gemeentebrede informatiebeveiligingsbeleid. Uitvoering aan het beveiligingsbeleid wordt geregeld in een separaat beveiligingsplan, voorheen het handboek informatiebeveiliging, dat eveneens geactualiseerd is. Het beveiligingsplan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door de inzet van mensen en middelen.

Omdat de Uitvoeringsdienst Sociaal Domein ook taken uitvoert voor de gemeenten Naarden en Muiden, geldt het informatiebeveiligingsbeleid en het beveiligingsplan voor de uitvoering van wetten ten behoeve alle drie de gemeenten.

[1] Bureau Keteninformatisering Werk en Inkomen

2. Wijzigingen 2015

2.1 Voortkomend uit bevindingen ten opzichte van BKWI normen

Hoewel de normen zijn benoemd door het Bureau Keteninformatisering Werk en Inkomen, wordt er in dit beleid uitgegaan van een bredere wet- en regelgeving. Immers informatiebeveiliging en privacy is voor elke wet- en regelgeving van belang.

Norm 1.3 BKWI Beveiligingsplan
Deze norm luidt: de gemeente heeft een formeel vastgesteld beveiligingsbeleid en –plan. Het plan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door inzet van mensen en middelen.

Hoewel de gemeente wel beschikt over een vastgesteld beveiligingsbeleid (2012), dat bestaat uit een beleidsplan en een handboek informatiebeveiliging, is dit specifiek gericht op de wet Suwi. Sinds 1 januari 2015 is er sprake van het Sociaal Domein waarin naast de Participatiewet en aanverwante regelingen, ook de Wmo en Jeugdwet zijn ondergebracht. In verband met deze nieuwe en gewijzigde wet- en regelgeving en daarbij behorende nieuwe taken, moet het beveiligingsbeleid worden geactualiseerd. Het bestaande handboek komt te vervallen en daarvoor in de plaats komt een beveiligingsplan.

De door de gemeente nieuw uit te voeren taken hebben geleid tot de aanschaf en het gebruik van nieuwe systemen. Het gebruik van deze systemen en de daarbij behorende autorisaties moeten worden vastgelegd in het Informatiebeveiligingsplan. Welke functies krijgen toegang tot welke gegevens, hoe worden controles uitgevoerd, welke maatregelen worden genomen bij misbruik en wat zijn de spelregels rondom autorisatie van Suwinet-Inkijk.

Het plan beschrijft maatregelen ter bescherming van de beschikbaarheid, integriteit, vertrouwelijkheid, controleerbaarheid van het gebruik van de persoonsgegevens en informatiesystemen. Ook moet worden aangegeven welke mensen en middelen hiervoor beschikbaar worden gesteld en hoe de naleving is geregeld. Het huidige handboek voldoet gedeeltelijk aan deze eisen.

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. Niet alleen moet er via nieuwsbrieven en intranet de aandacht op worden gevestigd maar ook in de teamoverleggen moet dit een periodiek onderwerp op de agenda zijn. Vast medewerkers leggen een eed of gelofte af en inhuurkrachten moeten een integriteitsverklaring ondertekenen. Dit laatste gebeurt wel, maar moet procesmatig nog beter geborgd worden.

Norm 1.5. BKWI Actualiseren
Het beleid moet regelmatig geactualiseerd worden. Om dit te borgen is het advies dit onderdeel van de vaste Planning & Controlcyclus van de gemeente te laten worden. In elk geval zal deze nota in 2017 worden geëvalueerd en bijgesteld.

Norm 2.2 BKWI Functiescheiding
Degene die de beschikbare rapportages van BKWI/SUWI beoordeelt (applicatiebeheer Wijzer) mag niet dezelfde zijn als de Security Officer. Dit is thans wel het geval. De taken van de Security Officer moeten worden belegd bij het concern. Inmiddels is dit ambtelijk gerealiseerd maar de positionering beleidsmatig nog worden geborgd.

De huidige Security Officer is ook verantwoordelijk voor de Suwinet-accounts van de afdeling Burgerzaken. Ook dit moet belegd worden bij de Security Officer van het concern. Daarmee wordt de

afdeling Burgerzaken ook zelf verantwoordelijk zijn voor het nakomen van de verplichtingen en de jaarlijkse verantwoording aan het college.

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 (Suwinet) applicaties ligt bij de organisatie. Daarom moet de organisatie beschikken over een procedure met criteria om toegang te verlenen tot de verschillende applicaties. Het werken met autorisatieniveaus is al praktijk, maar moet ook opgenomen worden in het beleid en uitgewerkt worden in het informatiebeveiligingsplan.

Norm 13.5 BKWI Controle
Periodiek moet controle op toegangsrechten en gebruik plaatsvinden. Leg de relatie vast tussen de medewerkers waar het om gaat en hun functies/taken waarvoor het gebruik van de verschillende applicaties noodzakelijk is. Vraag rapportages op bij het BKWI (of daar waar nodig voor andere applicaties) en beoordeel deze. Dit gebeurt in praktijk, maar wordt nu ook beleidsmatig geborgd.

2.2 Voortkomend uit interne bevindingen

Reikwijdte van de informatiebeveiligingsbeleid
Het huidige informatiebeveiligingsbeleid ziet vooral op de keten Werk & inkomen en kwam voort uit 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.

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. Beschreven moet worden dat dit alleen kan waar de wet dit toestaat of waar de betrokken inwoner een ondubbelzinnige toestemmingsverklaring gegeven heeft.

Incidentregistratie
In 2015 heeft een incident plaatsgevonden waarbij een virus zich verspreidde binnen de bestanden van de uitvoeringsdienst en bestanden gijzelde. Door een adequaat backupsysteem konden schone bestanden worden teruggezet, met een dag verlies aan werk. Het is van belang om incidenten te registreren. In het beleid wordt daarom een registratieplicht opgenomen.

Inrichting beveiligingsorganisatie
De rollen, taken, bevoegdheden en verantwoordelijkheden waren onduidelijk beschreven. In de voorliggende nota zijn deze beter uitgewerkt.

3. Reikwijdte

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 voor zover de uitvoering daarvan wordt opgedragen aan Wijzer.

4. Afbakening

Het voorliggende informatiebeveiligingsbeleid geldt voor de informatiesystemen van Wijzer en omvat de uitvoering binnen de lijnverantwoordelijkheid van Wijzer. De inrichting en het onderhoud van technische en fysieke informatiebeveiligingseisen (beveiliging van servers, firewalls, virussen, alarmeringen, etc.) behoort tot de verantwoordelijkheid van de afdeling F&I). De (nadere) uitwerking van aspect regie & privacy in het Sociaal Domein maakt onderdeel uit van het regionaal uitvoeringsprogramma Sociaal Domein van de regio Gooi & Vechtstreek 2015

5. Uitgangspunten voor het informatiebeveiligingsbeleid

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.

Reikwijdte van de informatiebeveiligingsbeleid
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 en vastlegging in de notulen.

Norm 1.5 BKWI Actualiseren
Het beleid moet regelmatig geactualiseerd worden. Voor de eerste maal uiterlijk 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 lig bij de organisatie. Er moet een procedure beschikbaar zijn waarin de criteria staan vermeld om toegang te verlenen tot de applicaties. De autorisatieniveaus moeten worden opgenomen in het beveiligingsplan.

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 gegevensverlies, bijvoorbeeld door virussen, moet een adequaat backupsysteem aanwezig zijn. Incidenten moeten worden geregistreerd.

Inrichting beveiligingsorganisatie
De rollen, taken, bevoegdheden en verantwoordelijkheden moeten duidelijk zijn beschreven.

5.1 Privacy

Bescherming van de privacy heeft de volgende uitgangspunten:

- Het uitwisselen of hergebruik van gegevens binnen Wijzer of door andere partijen dan Wijzer is uitsluitend toegestaan op wettelijke basis, of op grond van een ondubbelzinnige toestemmingsverklaring van persoon die het betreft.
- Beheer en toegang tot gegevensverzamelingen en applicaties is alleen mogelijk als iemand daarvoor geautoriseerd is.
- Suwinet is een besloten netwerk dat technisch adequaat van het publieke internet is afgescheiden. Daardoor zijn de ook de Suwi- berichten beveiligd tegen onbevoegd inzien en wijzigen.
- Inwoners kunnen op verzoek inzage krijgen en correcties laten doorvoeren in hun eigen (elektronische) dossier.
- (Elektronische) dossiers worden op basis van BSN aangemaakt. Er zijn geen familiedossiers.
- Het college van burgemeester en wethouders heeft een privacy protocol vastgesteld.

5.2 Algemeen

De informatievoorziening is een lijnverantwoordelijkheid en maakt een geïntegreerd onderdeel uit van het bedrijfsproces. De volgende uitgangspunten liggen hieraan ten grondslag:

- Beveiligingsmaatregelen mogen niet ten koste gaan van de veiligheid van het personeel en van derden.
- 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.
- De beveiligingsmaatregelen betreffen de gegevensuitwisseling tussen Wijzer, de overige SUWI partners en de derden.
- De betrouwbaarheid van het informatiesysteem dat gegevens uitwisselt met derden moet gewaarborgd zijn.
- Informatiebeveiliging is een essentieel onderdeel van de dagelijks bedrijfsvoering.
- Informatiebeveiliging is van toepassing op het hele proces van zowel de geautomatiseerde als niet-geautomatiseerde systemen ongeacht de soort informatie en opslagwijze.
- Het afdelingshoofd Wijzer is verantwoordelijk voor de gegevensbescherming en gegevensuitwisseling met derden maar ook voor wat betreft de interne uitwisseling.
- Al het netwerkverkeer (zowel eigen als andere netwerken) moet verlopen via één logische netwerkingang (de filterende netwerkkoppeling). Dat wil zeggen dat pas als men is ingelogd de applicaties waarvoor men geautoriseerd is toegankelijk zijn.
- Als bij (geautomatiseerde) gegevensuitwisseling tussen Wijzer en andere instanties gebruik wordt gemaakt van intern opgeslagen gegevens, moet schriftelijk worden vastgelegd wie hiervoor verantwoordelijk is, aan welke kwaliteiten de uitwisseling moet voldoen en welke maatregelen er moeten worden getroffen.
- Wijzer autoriseert en registreert de toegang die gebruikers hebben tot haar (Suwinet)applicaties op basis van een formele procedure (norm 13.1 BKWI).
- Er vindt meerdere malen controle plaats op verleende toegangsrechten van applicaties van Wijzer alsmede analyse van BKWI-gebruikersinformatie inzake Suwinet (norm 13.5 BKWI).

6. Toezicht en evaluatie

6.1 Beveiligingsorganisatie

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 beveiligings-procedures 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 informatie-beveiliging 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.

6.2 Incidentregistratie

- 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.

6.3 Beveiligingsplan

Ter uitvoering van deze beleidsnota wordt jaarlijks een beveiligingsplan opgesteld, dat vastgesteld wordt door het uitvoerende college van burgemeester en wethouders en kenbaar gemaakt wordt aan alle werknemers en relevante externe partijen. Het beveiligingsplan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door de inzet van mensen en middelen (norm 1.3 BKWI). Het beveiligingsplan wordt actief binnen Wijzer uitgedragen (norm 1.4 BKWI).

6.4 Beleidscyclus

Deze beleidsnota wordt uiterlijk in 2017 geëvalueerd en bijgesteld. Het beveiligingsplan wordt jaarlijks geëvalueerd en verbeterd conform een PDCA-cyclus (norm 1.5 BKWI).