032

college saneringzorginstellingen

Goedkeuring buiten reikwijdte
t art 5.1 lid 2 onder h
t art 5.1 lid 2 onder e

Type nota:

Goedkeuring	☐
(Niet) vernietigen	☐
Een-op-eenverzoek	☐
Extramuraliseren	☐
Anders, nl.: Beleidsnotitie informatiebeveiligingsbeleid CSZ versie 1.0	X

Naam opsteller nota:

[redacted]

Behandelen als:

Bespreekstuk	☐
Hamerstuk	X

B 20-28

Beleidsnotitie informatiebeveiligingsbeleid CSZ versie 1.0

Toelichting:
Het ministerie van VWS verwacht van ZBO's zoals CSZ dat zij zich committeren aan de Baseline informatiebeveiliging Overheid (BIO). Het CSZ heeft eerste stappen gezet in het opstellen en effectueren van het informatiebeveiligingsbeleid conform BIO.
Daartoe is de beleidsnotitie informatiebeveiligingsbeleid versie 1.0 (zie bijlage 1) opgesteld en een inventarisatie (zie bijlage 1a) gedaan van de reeds getroffen c.q. bestaande maatregelen op het gebied van de informatiebeveiliging bij het CSZ en de nog (in 2020) te implementeren maatregelen op grond van het verschil tussen de reeds genomen maatregelen en de noodzakelijk te nemen maatregelen (zie bijlage 1b).

De beleidsnotitie informatiebeveiligingsbeleid versie 1.0 bevat:
- de beschrijving van de toezichttaken en organisatie van het CSZ;
- de belangrijkste uitgangspunten voor het informatiebeveiligingsbeleid CSZ;
- de strategische doelen van het informatiebeveiligingsbeleid;
- de governance mbt het informatiebeveiligingsbeleid;
- de risico-analyse c.q. de signficante risico's op het gebied van de informatie-beveiliging.

De verschillen tussen de genomen maatregelen en de noodzakelijke maatregelen gelet op de significante risico's zijn opgenomen in een zogenoemde verschillen- of 'GAP'-analyse waarin tevens is aangegeven wanneer bepaalde maatregelen worden geïmplementeerd ('implementatieplan').

Een eerdere conceptversie van de beleidsnotitie informatiebeveiligingsbeleid CSZ is op verzoek van de CIO van het CSZ, de heer Sijstermans, door de manager CSZ, Wim Komrij, besproken met de CISO van VWS.
De suggesties van de CISO van VWS hebben geresulteerd in de bijgaande Beleidsnotitie informatiebeveiligingsbeleid versie 1.0. De CISO van VWS heeft aangegeven dat het van belang is om een formeel startdocument voor het informatiebeveiligingsbeleid vast te stellen en beveelt daarom aan een versie 1.0. door het CSZ vast te laten stellen.

De CISO van de NZa, [redacted] heeft op verzoek van de CIO CSZ de conceptversie van de onderhavige beleidsnotitie beoordeeld. Zijn opmerkingen zijn verwerkt.

De CIO van het CSZ die onder andere verantwoordelijk is voor het beleidskader informatiebeveiliging CSZ is akkoord met de Beleidsnotitie informatiebeveiligingsbeleid CSZ versie 1.0.

college sanering zorginstellingen

ADVIES:

Het College sanering zorginstellingen besluit:
De beleidsnotitie Informatiebevelligingsbeleid CSZ versie 1.0 vast te stellen.

Bijlagen: 3

Akk. agendering
secr. Csz
[redacted] 13/2/2020

Bijlage 5

Beleidsnotitie Informatiebeveiligingsbeleid CSZ versie 1.0

Toezichttaken en organisatie CSZ

Het CSZ Het College sanering zorginstellingen (CSZ) is een zelfstandig bestuursorgaan (ZBO) dat namens de minister van Volksgezondheid, Welzijn en Sport (VWS) een aantal taken uitvoert.

Het huidige takenpakket van het CSZ bestaat uit het toezicht op :

- Vervreemding onroerende zaken

Wanneer een zorginstelling terreinen, gebouwen of delen daarvan wil verkopen, verhuren of aan een beperkt recht onderwerpen, is de directie of de Raad van Bestuur van een instelling wettelijk verplicht dit bij het CSZ te melden. Als het CSZ besluit dat goedkeuring vereist is, vindt toezicht plaats op het verkoopproces dat moet leiden tot een marktconforme opbrengst. Doelstelling van het toezicht is om te voorkomen dat geld "weglekt" uit de zorg. Er wordt momenteel aan ca 700 casus gewerkt.

- Saneringsregeling zorginstellingen

Bij een intrekking of beperking van de toelating van een instelling houdt het CSZ toezicht op het saneringsproces. Het CSZ kan subsidie geven die (deels) voorziet in de financiële gevolgen van deze beperking of intrekking. Vrijgevestigde medische beroepsbeoefenaren kunnen subsidie krijgen om de teruggang in hun inkomen op te vangen tijdens de periode die voorafgaat aan de beperking of intrekking van de toelating. Voorwaarde voor aanmelding is een beslissing omtrent de toelating ("sluitingsbeslissing") van de minister van VWS. Hoewel de saneringsregeling nog bestaat, zijn er de afgelopen jaren geen sluitingsbeslissingen meer genomen. Het College behandelt nog lopende zaken. Het gaat op dit moment om nog één lopende casus

- Saneringsregeling ambulancehulpverlening

Bij het intrekken van een vergunning van een ambulancedienst en bij het wijzigen of opheffen van de vestigingsplaats van een Centrale Post voor het Ambulancevervoer kon het CSZ subsidie verstrekken om de financiële gevolgen geheel of gedeeltelijk op te vangen. Deze saneringsregeling is beëindigd. Lopende zaken worden door het College sanering afgehandeld. Het gaat op dit moment om nog één lopende casus

- Overige werkzaamheden

De minister of staatssecretaris van VWS kan het College sanering vragen bijzondere werkzaamheden uit te voeren of een regiefunctie te vervullen. In de afgelopen jaren is onderzoek uitgevoerd bij instellingen in financiële problemen. Ook vervolgopdrachten zijn uitgevoerd, zoals het aandragen van oplossingen of het monitoren van de situatie nadat bepaalde maatregelen zijn ingevoerd. De expertise van het CSZ heeft zich de laatste jaren steeds meer toegespitst op vastgoed. Deze expertise is beschikbaar voor het uitvoeren van onderzoeken voor het ministerie van VWS of voor andere ZBO's.

Organisatie

Het bestuur van het CSZ bestaat uit drie personen die tevens de Raad van Bestuur van de NZa vormen. Het secretariaat van het CSZ bestaat uit 7 personen die in dienst zijn van de NZa. Het CSZ maakt voor de uitvoering van de toezichttaken gebruik van zogenoemde gemachtigden die per casus

worden aangewezen en ingehuurd. De gemachtigden zijn deskundigen op het gebied van (zorg-) vastgoed. De gemachtigden adviseren het College over de onroerend goed transacties (open en transparante vervreemdingsproces en de marktconformiteit van de prijs).

De uitvoeringsorganisatie van het CSZ, de casusbehandeling is in verregaande mate gestandaardiseerd. Er is een casus en workflow-systeem.

Uitgangspunten informatiebeveiligingsbeleid CSZ

Deze beleidsnotitie is geschreven op basis van de Baseline informatiebeveiliging Overheid (BIO).

De Baseline informatiebeveiliging overheid (BIO) is bedoeld om de (significante) risico's en bedreigingen te onderkennen die schade met zich meebrengen als gevolg van het (tijdelijk) niet beschikbaar zijn van (informatie-) systemen, het niet integer zijn van informatie en het in verkeerde handen vallen van informatie. De BIO bevat tevens een overzicht van te nemen specifieke beheersmaatregelen.

De BIO is opgesteld voor generieke schades en bedreigingen bij de Rijksoverheid en de passende maatregelen hiervoor genomen kunnen worden. Het zogenoemde basis beveiligingsniveau (BBN).

Er worden 3 niveaus BBN onderscheiden. Het CSZ herkent zich in BBN niveau 2 omdat er met bedrijfsgevoelige informatie wordt gewerkt en mogelijke incidenten, mede vanwege het feit dat de Raad van bestuur de NZa het Collegebestuur vormt, tot bestuurlijke commotie kunnen leiden.

De BIO is van toepassing op de gehele Rijksdienst. De BIO is niet verplicht gesteld voor ZBO's.

Het CSZ committeert zich aan het verzoek van ministerie van VWS om de BIO toe te passen, afgestemd op het toezichtproces van het CSZ.

De strategische doelen van het informatiebeveiligingsbeleid

Het CSZ onderkent de volgende strategische doelen voor het informatiebeveiligingsbeleid.

-het managen van de risico's die gelden bij informatiebeveiliging, die betrekking hebben op: beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening

Hieronder wordt onder andere maar niet uitsluitend verstaan:

-het correct registreren, archiveren en -beveiligen van vertrouwelijke gegevens zoals persoons-/bedrijfsgevoelige gegevens van burgers, medewerkers en zorginstellingen;

-adequate bescherming van bedrijfsmiddelen;

-het waarborgen van veilige informatiesystemen;

-het beschermen van kritieke bedrijfsprocessen;

-het minimaliseren van risico's van menselijk gedrag;

-het voorkomen van ongeautoriseerde toegang c.q. het beheersen van de toegang tot informatiesystemen;

-het adequaat reageren op incidenten;

-het waarborgen van de naleving van dit beleid.

De governance mbt het informatiebeveiligingsbeleid

-Het bestuur van College is eindverantwoordelijk voor de informatiebeveiliging;

-De CIO is eindverantwoordelijk voor het informatiebeveiligingsbeleid waarmee bedoeld wordt dat er een beleidskader wordt opgesteld. Deze (door de CIO beoordeelde en door het bestuur van het College vastgestelde) notitie vormt daartoe de eerste stap. De CIO is tevens verantwoordelijk voor de onafhankelijke toetsing op de naleving van het informatiebeleid. De CIO laat zich bijstaan door de CISO van de NZa;

-De verantwoordelijkheid voor de uitvoering ligt bij de manager CSZ;

-Het informatiebeveiligingsbeleid wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, incidenten en actualisatie van risicoanalyses;

-Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.

Significante risico's

Gelet op het werkproces mbt de toezichttaken van het CSZ en het feit dat het bestuur van het CSZ uit dezelfde personen bestaat als het bestuur van de NZa onderkent het CSZ het volgende significante risico:

Het correct registreren, archiveren en beveiligen van privacy- en bedrijfsgevoelige gegevens

De belangrijkste beheersmaatregelen liggen op het terrein van:

a-De bewustwording van medewerkers mbt informatiebeveiliging;

b-De borging van de continuïteit van het casus- en workflowsysteem;

c-Het voorkomen van ongeautoriseerde toegang tot het informatiesysteem waaronder ook wordt verstaan de (fysieke) archiefruimte mbt de dossiers;

d-Het inregelen van de Plan Do Check act cyclus in termen van een uitvoeren van een periodieke risico-analyse, de verificatie van de getroffen maatregelen en de eventuele aanpassing van de getroffen maatregelen met als resultante een In Control Verklaring, waar uit moet blijken dat de in opzet' (op papier) getroffen maatregelen 'bestaan' en 'werken'.

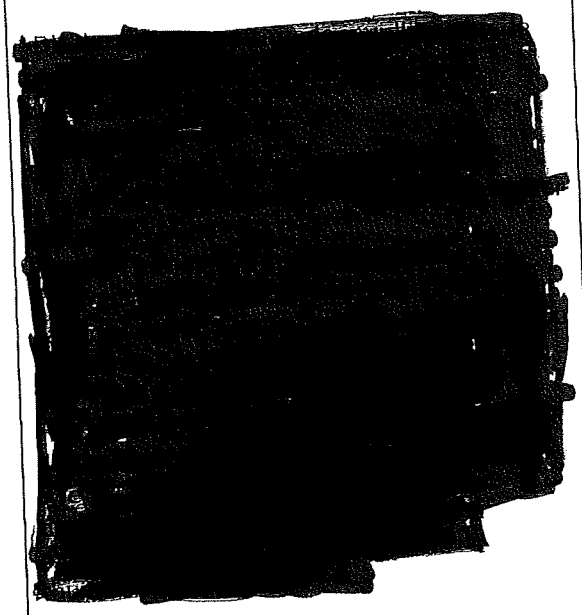
In bijlage 1a is voor het CSZ (BBN 2) weergegeven welke maatregelen genomen zijn/worden door het CSZ. Deze tabel is te beschouwen als een weergave van het beleid om, gelet op de context van het CSZ, op passende- en proportionele wijze de risico's en bedreigingen voor informatiebeveiliging af te dekken. Tevens is een overzicht opgenomen van de aandachtpunten die VWS het CSZ heeft meegegeven voor het werkprogramma 2020.

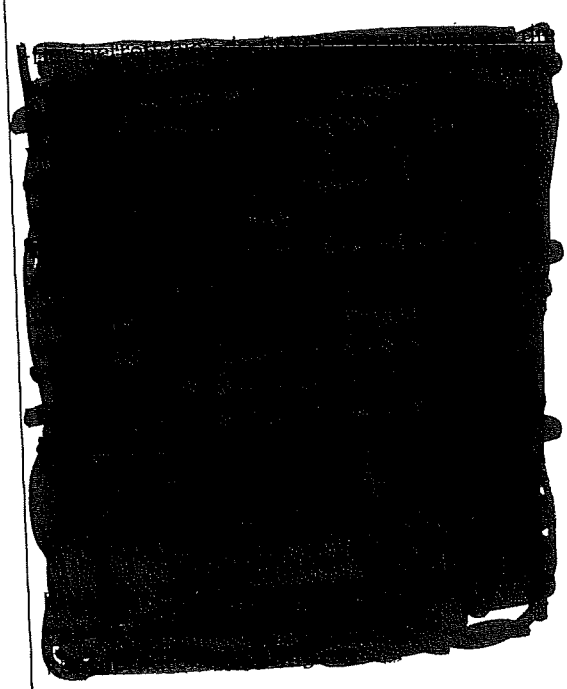
In bijlage 1b is een zogenoemde GAP-analyse opgenomen, het verschil tussen de op grond van BIO te nemen maatregelen en de door CSZ getroffen maatregelen (zoals weergegeven in bijlage 1) en wijze waarop de nog te nemen maatregelen worden geïmplementeerd, het implementatieplan.

Bijlage 1a

Bijlage 1a Getroffen maatregelen in het kader van BIO

Onderwerp	Getroffen maatregelen
Informatiebeveiligingsbeleid	-Conceptversie 1.0 opgesteld waarin opgenomen de taken van het CSZ, de organisatie van het CSZ, de uitgangspunten en strategische doelen, de governance en de significante risico's.
Organisatie beveiliging -Functiescheiding bedrijfsmiddelen	[redacted]
-Autorisatie toegang tot middelen	[redacted]
-Organisatie contact met overheidsinstanties over incidenten, calamiteiten	-Via Functionaris Gegevensbescherming voor persoonsgegevens/datalekken-> AP -In voorkomende gevallen zal het CSZ advies inwinnen bij het meldpunt informatiebeveiliging van de NZa en het handelen (waar CSZ verantwoordelijk voor is) daarop afstemmen.
-Beleid voor mobiele apparatuur	[redacted]
Veilig personeel -VOG bij indiensttreding	-Ja, dit geldt voor medewerkers en inhuurkrachten die toegang hebben tot (bedrijfs-)vertrouwelijke gegevens.

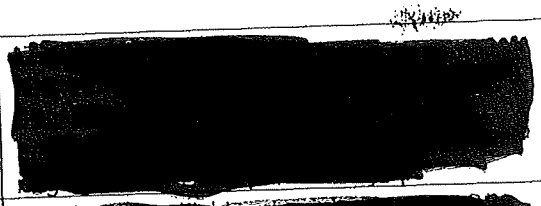
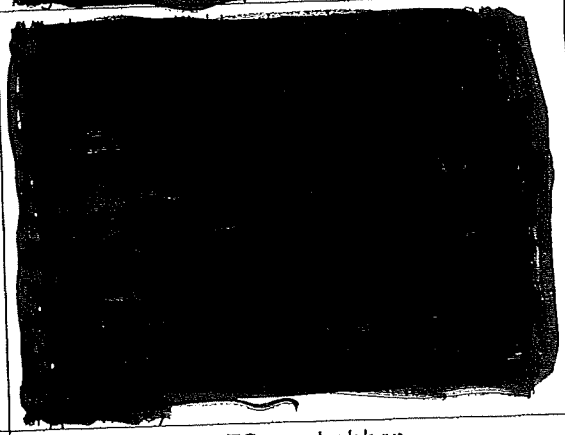
-Instructies informatiebevelliging	Daarnaast wordt de ambtenaren-eed afgelegd bij indiensttreding en wordt een geheimhoudingsverklaring verlangd -Als medewerkers in dienst komen dan krijgen zij een intake gesprek 'beveiliging en privacy' om hen aan de hand van leidraad te informeren over informatiebeveiliging. Daarnaast wordt in elk geval in het planningsgesprek en het functioneringsgesprek aandacht besteed aan het onderwerp informatiebeveiliging. 
Beheer bedrijfsmiddelen -Inventarisatie /eigendom bedrijfsmiddelen die samenhangen met informatie/informatieverwerking -Gedragsregels digitale werkomgeving	 
Informatie classificatie -Informatie moet geclassificeerd en gelabeld worden	-We onderscheiden de volgende type gegevens: 1-Salaris-/personeelsvertrouwelijke gegevens. Deze bevatten persoonsvertrouwelijke gegevens. De (digitale/fysieke)toegang tot deze gegevens is beperkt tot de salarisverwerker/boekhouder, de financieel beleidsmedewerker en de manager.

	De gegevens over het functioneren en beoordelen van medewerkers zijn alleen toegankelijk voor de manager en de hogere leidinggevende. De betreffende (fysieke) informatie wordt bewaard in een afgesloten kast (die zich in een werkruimte bevindt die toegangsbeveiliging kent). 2-Casusgegevens. Dit betreft bedrijfsgevoelige gegevens. Deze gegevens zijn slechts (digitaal/fysiek) toegankelijk voor degenen die aangewezen zijn om werkzaamheden voor het CSZ te verrichten. Dit betreft alle CSZ-medewerkers. De lopende fysieke casusdossiers bevinden zich in een (afsluitbare) archiefruimte.  3-De besluiten die gepubliceerd worden op de website. De besluiten worden geanonimiseerd. Persoonlijke gegevens van individuele kopers/huurders worden niet gepubliceerd.
Behandelen media -Fysieke media die informatie bevatten moeten beschermd worden tegen onbevoegde toegang, corruptie	
Toegangsbeveiliging	

-Beleid en beheer van toegangsrechten Toegangsbeveiliging van systeem en wachtwoordbeheer	[redacted]
Cryptografie	[redacted]
Fysieke beveiliging -Toegang tot ruimte -Clean desk	[redacted]
Beveiliging bedrijfsvoering -Gedocumenteerde bedieningsprocedure -Wijzigingsbeheer -Capaciteitsbeheer -Scheiding van ontwikkel, test en productieomgeving -Bescherming tegen malware -Backup van informatie	[redacted]

-Verslaglegging en monitoren van gebeurtenissen -Audit informatie systeem	[redacted]
Leveranciersrelatie -Bij offerte uitvragen (eisen tav informatiebeveiliging/beheersbare afhankelijkheid van leverancier)	-De ondersteuning van de kantoorautomatisering is ondergebracht bij ICT Teamwork. Dit biedt goede waarborgen voor continue ondersteuning. De service-overeenkomst met ICT Teamwork en de periodieke bespreking van knelpunten en incidenten bevat voldoende waarborgen voor de informatiebeveiliging.
-Bij verwerking van persoonsgegevens: verwerkersovereenkomsten	-Er zijn verwerkersovereenkomsten ICT-leverancier, salarisverwerker/boekhouder) Met de gemachtigde is er een raamovereenkomst (art 7.1. verplichting tot geheimhouding van bedrijfsgevoelige informatie. [redacted]
-Monitoring prestaties leverancier	[redacted]
-Meldpunt incidenten, bij vertrouwelijke gegevens melding binnen 72 uur bij CISO	-Belegd bij de FG
-Analyse- en leerpunten mbt Incidenten	-Belegd bij de FG
Bedrijfscontinuiteit -Welke maatregelen bij rampen?	[redacted]

Naleving wettelijke en contractuele eisen -Inzichtelijk welke bewaartermijnen -In kader AVG is er een FG -Interne controle op naleving privacy	 -Ja, Selectielijsten aanwezig -Ja -Check op te publiceren Collegebesluiten
Jaarlijkse ICV, in control verklaring over de informatiebeveiliging	

VWS uitwerking speerpunten informatiebeveiliging. Onderwerpen	Uitwerking
-VWS heeft aan ons gevraagd om de CIO functie in te vullen en aan te geven op welke wijze dit organisatorisch op een onafhankelijke wijze is geborgd.	-Het CSZ heeft miv 1 augustus 2019 een CIO benoemd.
-Inspanningen om op basis van risico management de BIR in te voeren	
-Het dreigingsbeeld van uw organisatie met daarin de belangrijkste dreigingen op het gebied van cybersecurity	
-Uw inspanningen voor het in control zijn op het gebied van privacy wetgeving	-We hebben een FG, we hebben verwerkersovereenkomsten en we besteden regelmatig aandacht aan het onderwerp privacy tijdens het werkoverleg. De medewerkers hebben de module e-learning ingevuld

-De wijze waarop aandacht wordt gegeven aan het gedrag van medewerkers in relatie tot informatiebeveiliging en de omgang met persoonsgegevens (waaronder alertheid op datalekken)	-Dit beleidsdocument beoogt mede het bewustzijn te verhogen -Regelmatige bespreking van het onderwerp informatiebeveiliging tijdens het werkoverleg in het bijzijn van de CIO/CISO.

Bijlage 1b

Bijlage 2: GAP-analyse. Noodzakelijke maatregelen die nog ingeregeld moeten worden	Implementatie-plan
[redacted]	[redacted]