D30

college Sanering zorginstellingen

Gedeeltelijk buiten reikwijdte
+ art 5.1 lid 2 onderh + art 5.1 lid 2 onder

Voortgangsoverzicht beleidsnotitie CSZ informatiebeveiliging 1.0

Type nota:

Goedkeuring	☐
(Niet) vernietigen	☐
Een-op-eenverzoek	☐
Extramuraliseren	☐
Anders, nl.: Informatiebeveiliging 1.0	X

Naam opsteller nota:

[redacted]

Behandelen als:

Bespreekstuk	X
Hamerstuk	☐

Toelichting:
Het CSZ heeft op 18 februari 2020 de beleidsnotitie informatiebeveiliging 1.0 bestuurlijk vastgesteld.

[redacted]. Via dit voortgangsoverzicht laat het CSZ zien dat het aandacht besteedt aan (ontwikkelingen op het gebied van) informatiebeveiliging.

college Sanering zorginstellingen

B 21-69

Voortgangsoverzicht beleidsnotitie CSZ informatiebeveiliging 1.0

In bijlage treft u een (activiteiten)overzicht aan van de periode 18 februari 2020-1 juni 2021.

[redacted]

In de conceptkaderbrief voor het jaarplan en de begroting CSZ 2022 (27 mei 2021 ontvangen) wordt ook aandacht gevraagd voor de informatiebeveiliging:

1. Van het CSZ wordt verwacht dat het in het kader van de informatiebeveiliging inzicht heeft in de belangrijkste processen en systemen van de organisatie en daarmee gepaard gaande risico's. Deze moeten worden aangetoond door het uitvoeren van een risicoanalyse zodat de bijbehorende beheersmaatregelen kunnen worden getroffen.
2. Het CSZ moet inzicht gegeven worden in de belangrijkste ontwikkelingen op het gebied van IV/ICT binnen de organisatie van het CSZ door middel van een overzicht op hoofdlijnen;
3. Verder wordt van het CSZ verwacht aandacht te besteden aan het CIO-stelsel Rijk.

Dit voortgangsoverzicht draagt, naast de al vastgestelde beleidsnotitie informatiebeveiliging 1.0, bij aan het gevraagde onder 2. en 3.

Wat het derde punt betreft: Het CSZ beschikt al over een CIO. De CIO van CSZ wordt geacht (on)gevraagd de CIO-Rijk en CISO-Rijk van informatie te voorzien.

ADVIES:

Het voortgangsoverzicht beleidsnotitie informatiebeveiliging CSZ 1.0 voor kennisgeving aan te nemen.

Bijlage

Akk. agendering
secr. Csz
3/6/2021

[redacted] juni 2021/csz/ctw/voortgangsoverzicht beleidsnotitie CSZ informatiebeveiliging 1.0

bijlage

Voortgangsoverzicht beleidsnotitie informatiebeveiliging CSZ 1.0

Inleiding

Het CSZ heeft op 18 februari 2020 de beleidsnotitie informatiebeveiliging 1.0 bestuurlijk vastgesteld.

[redacted]

In de concept-kaderbrief voor het jaarplan en de begroting CSZ 2022(27 mei 2021 ontvangen) wordt ook aandacht gevraagd voor de informatiebeveiliging:

1-Van het CSZ wordt verwacht dat het in het kader van de informatiebeveiliging inzicht heeft in de belangrijkste processen en systemen van de organisatie en daarmee gepaard gaande risico's. Deze moeten worden aangetoond door het uitvoeren van een risicoanalyse zodat de bijbehorende beheersmaatregelen worden getroffen;

2- Het CSZ moet inzicht gegeven worden in de belangrijkste ontwikkelingen op het gebied van IV/ICT binnen de organisatie van het CSZ door middel van een overzicht op hoofdlijnen;

3-Verder wordt van het CSZ verwacht aandacht te besteden aan het CIO-stelsel Rijk.

Dit voortgangsoverzicht draagt, naast de al vastgestelde beleidsnotitie informatiebeveiliging 1.0, bij aan het gevraagde onder 2. en 3.

Wat het derde punt betreft: Het CSZ beschikt al over een CIO. Verder wordt de CIO van CSZ geacht (on-)gevraagd de CIO-Rijk en CISO-Rijk van informatie te voorzien.

(Activiteiten-)overzicht periode 18 februari 2020-1 juni 2021.

Het CSZ kenmerkt zich als een stabiele organisatie wat de geautomatiseerde omgeving en informatiebeveiliging betreft. Er hebben zich in de periode van 18 februari tot 1 juni 2021 geen ICT/Cyber/AVG- incidenten voorgedaan c.q. wij hebben geen signalen van onze ICT leverancier ontvangen over knelpunten in de werking van ons systeem.

De CSZ medewerkers hebben in oktober 2020 de beschikking gekregen over een zakelijke CSZ laptop ivm het thuiswerken als gevolg van de Covid-situatie. De zakelijk laptop geeft alleen toegang tot de CSZ-werkomgeving. Het betreft een door de ICT leverancier van het CSZ, ICT Teamwork, gemanagede laptop, met eenzelfde beveiligingsniveau als de desktops ten kantore van het CSZ.

In verband met de verbouwingswerkzaamheden in het pand waar het CSZ gehuisvest is, heeft het CSZ vanaf 1 maart 2021 een afgesloten ruimte op de 3e etage van het pand aan de Pythagoras-laan. De ruimte voldoet aan de gescheiden informatie-huishouding ten opzichte van de NZa:

a-het betreft een afgesloten ruimte met toegangsbeveiliging op de deuren; alleen CSZ medewerkers [redacted] hebben toegang;

b)-Het archief van het CSZ bevindt zich in de afgesloten ruimte;

[redacted]

Op 21 januari 2021 heeft een overleg plaatsgehad met de ICT leverancier van het CSZ, ICT teamwork, in het bijzijn van de CIO van het CSZ. De doelstelling van dat overleg was om een duidelijker beeld te krijgen van de ondersteunende werkzaamheden van ICT teamwork voor de informatiebeveiliging van het CSZ:

1-Afgesproken is dat halfjaarlijkse afstemming plaatsvindt met ICT Teamwork. ICT teamwork geeft aan de hand van een zogenoemd full service rapport en de ingeregelde toegangsrechten een terugkoppeling van de prestaties van het ICT-systeem. Van het overleg tussen CSZ en ICT Teamwork wordt een verslag gemaakt.

2-ICT Teamwork verricht de noodzakelijke werkzaamheden voor het geautomatiseerde systeem van het CSZ;

-in het kader van het Vulnerability en Patchmanagement;

-het voorkomen van hackpogingen;

-het testen van het systeem door middel van PEN-tests en dergelijke;

[redacted]

ICT Teamwork heeft een AVG-certificaat. Het certificaat dat ICT Teamwork voert (de dataprocode) is door de Autoriteit Persoonsgegevens onderschreven. In die zin heeft het volgens ICT teamwork zelfs de juridische status dat je er van uit mag gaan dat een partij die een dergelijk certificaat houdt ook werkelijk zijn zaakjes voor elkaar heeft en ook afdoende handelt volgens de wet.

Het ISO27001 certificaat met de daarop beschreven scope geeft volgens ICT teamwork afdoende zekerheid dat ICT teamwork als ICT-leverancier de informatiebeveiliging serieus neemt.

ICT teamwork heeft ons de beide certificaten doen toekomen.

Gap-analyse bij de beleidsnotitie informatiebeveiliging CSZ 1.0

Bij de beleidsnotitie informatiebeveiliging CSZ 2.0 is een zogenoemde GAP-analyse opgenomen, een overzicht van de noodzakelijk nog op te pakken zaken.

1-Het betreft het inregelen van een PlanDoCheckAct-cyclus met een periodieke risico-analyse;

Stand van zaken 1 juni 2021:-Er hebben zich geen incidenten voorgedaan c.q. er zijn geen (afwijkende) signalen ontvangen van de ICT-leverancier van het CSZ over de werking van het geautomatiseerde gegevensverwerkende systeem . Er zijn adequate maatregelen getroffen voor het thuiswerken ivm COVID (gemanagede laptops) en de nieuwe tijdelijke huisvestingssituatie van het CSZ voldoet aan vereisten van een gescheiden informatie-huishouding ten opzichte van de NZa;

2-De afstemming met de ICT-leverancier over de reikwijdte van de dienstverlening;

Stand van zaken 1 juni 2021-De reikwijdte van de dienstverlening van ICT-teamwork is afgestemd. ICT-teamwork verzorgt op een adequate wijze het patch- en vulnerability management, het onderscheppen van hack-pogingen en uitvoeren van PEN-tests. ICT teamwork beschikt over een kwaliteitscertificaat voor het voldoen aan de AVG en voor informatiebeveiliging.

[redacted]