D31

college saneringzorginstellingen

Gedeeltelijk buiten reikwijdte
+ art 5.1 lid 2 onder h
+ art 5.1 lid 2 onder e

Voortgangsoverzicht beleidsnotitie CSZ informatiebeveiliging 1.0 stand 1 maart 2022

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 (naar de stand van 1 maart 2022) laat het CSZ zien dat het voortdurend aandacht besteedt aan (ontwikkelingen op het gebied van) informatiebeveiliging.

B 22-39

Voortgangsoverzicht beleidsnotitie CSZ informatiebeveiliging 1.0 stand 1 maart 2022

In bijlage treft u een update van het (activiteiten)overzicht aan van de periode 1 juni 2021-1 maart 2022.

In de kaderbrief voor het jaarplan en de begroting CSZ 2022 wordt door het Ministerie van VWS 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.

De update van dit voortgangsoverzicht draagt, naast de al vastgestelde beleidsnotitie informatiebeveiliging 1.0, bij aan het gevraagde onder 1. en 2.

In de periode 1 juni 2021 - 1 maart 2022 heeft het CSZ de volgende stappen gezet voor een IC-verklaring dan wel een informatiebeveiligingsbeeld:

1. Het invulling geven aan de PDCA-cyclus, waarin de brede risicoanalyse, de genomen maatregelen en de monitoring van de werking is opgenomen.
2. Het opzetten van een incidentenregistratie.
3. Het creëren van een digitale map met daarin opgenomen de (bewijs-)stukken die aantonen dat het CSZ voortdurend aandacht heeft voor informatiebeveiligings-aangelegenheden.
4. Het introduceren van 2Factor-authenitficatie en het maken van afspraken met de ICT-leverancier over data-restore-tests.

ADVIES:

Het voortgangsoverzicht beleidsnotitie informatiebeveiliging CSZ 1.0 naar de stand van 1 maart 2022 voor kennisgeving aan te nemen.

Bijlage

Akk. agendering secr. Csz
[redacted] 9/3/2022

bijlage

Voortgangsoverzicht beleidsnotitie informatiebeveiliging CSZ 1.0 update periode 1 juni 2021-1 maart 2022

Inleiding

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

Van het CSZ wordt verwacht dat het toewerkt naar een zogenoemde InControl-verklaring (IC-verklaring) voor de informatiebeveiliging dan wel, zo is de laatste ontwikkeling op dit gebied, naar een informatiebeveiligingsbeleid-beeld. Het CSZ heeft hiervoor reeds stappen zetten.

De IC-verklaring of het informatiebeveiligings-beeld kan mogelijk de vorm aannemen van een statusoverzicht waaruit blijkt welke zaken op het gebied van de informatiebeveiliging, gelet op de aanwezige risico's, reeds geregeld zijn en welke zaken in dit kader nog opgepakt moeten worden of in behandeling zijn.

In de 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;

Dit voortgangsoverzicht draagt, naast de al vastgestelde beleidsnotitie informatiebeveiliging 1.0, bij aan het gevraagde onder 1. en 2. Daarnaast beoogt dit doorlopend voortgangsoverzicht een beeld te verschaffen van de risico's en (eventuele) incidenten die zich hebben voorgedaan en welke maatregelen het CSZ getroffen heeft en fungeert daarmee als periodieke (update van de) risico-analyse. Daarmee wordt ook aangetoond dat het CSZ voortdurende aandacht heeft voor het onderwerp informatiebeveiliging.

Update (Activiteiten-)overzicht periode 1 juni 2021-1 maart 2022.

In deze periode heeft tweemaal overleg plaatsgehad met de ICT-leverancier.

[redacted]

Wij hebben besloten tot 2Factor-authentificatie, een extra maatregelen in het kader van de toegangsbeveiliging, die op 25 januari 2022 is geimplementeerd.

[redacted]

[redacted]

In januari 2022 hebben wij een incidentenregistratie opgezet waarin de incidenten met ingang van 1 januari 2021 zijn opgenomen.

[redacted]

Verder heeft het CSZ in december 2021 een start gemaakt met het verzamelen van achterliggende stukken die van belang zijn voor de aantoonbare (continue) aandacht voor informatiebeveiliging:

1-Informatiebeveiligingsbeleid 1.0. inclusief getroffen maatregelen in het kader van BIO en de GAP-analyse;

[redacted]

4-De incidentenregistratie en de afdoening hiervan;

5-Het contract met de ICT-leverancier en de ISO en AVG-certificaten waarover de ICT-leverancier beschikt;

[redacted]

Verder is bij de evaluatiegesprekken 2021 en de planningsgesprekken 2022 de informatiebeveiliging expliciet aan de orde geweest. Daar zijn geen bijzonderheden uit naar voren gekomen.

In het werkoverleg van het CSZ wordt in voorkomende gevallen (aspecten van) de informatiebeveiliging besproken.

[redacted]

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 maart 2022:

In de periode 1 juni 2021- 1maart 2022 heeft zich een beperkt aantal incidenten voorgedaan die adequaat zijn opgepakt door de ICT-leverancie. Verder is 2F-authentificatie als extra toegangsbeveiliging ingevoerd.

[redacted]

Besloten is dat als PlanDoCheckAct-cyclus dient:

1-De periodieke update/risicoanalyse inzake de informatiebeveiligingssituatie van het CSZ waarbij de overleggen met de ICT-leverancier en de incidenten input vormen;

2-De daaruit voortvloeiende maatregelen die genomen worden (in afstemming met de CIO, CISO en de ICT-leverancier). Voorbeelden hiervan zijn de 2F authentificatie en de restore tests;

3-De monitoring van de blijvend goede werking van het informatiebeveiligingsbeleid gebeurt door de manager van het CSZ in afstemming met de CIO en CISO van het CSZ en de ICT-leverancier. Over de monitoring wordt verslag gedaan in dit voortgangsoverzicht.

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

Stand van zaken 1 maart 2022: In de periode 1 juni 2021 tot 1 maart 2022 zijn de volgende bijzonderheden te melden:

De dienstverlening van de ICT-leverancier is uitgebreid met 2 Factor authentificatie en restoretests op data.

3-(Externe) toets op opzet, bestaan en werking van de informatiebeveiliging.

Stand van zaken 1 maart 2022:

In de periode 1 juni 2021 tot 1 maart 2022 heeft de volgende ontwikkeling zich voorgedaan:

Er word overgeschakeld van een IC verklaring naar het periodiek tonen van het informatiebeveiligingsbeeld, waarbij van belang is dat een ZBO kan aantonen dat sprake is van:

-Een periodieke brede risicoanalyse;

-Een Incidentenregistratie;

-Aandacht voor de oplossing van (bestaande) knelpunten

In de periode 1 juni 2021- 1 maart 2022 heeft het CSZ de volgende stappen gezet voor een IC-verklaring dan wel een informatiebeveiligingsbeeld:

1-Het invulling geven aan de PDCA-cyclus, waarin de brede risicoanalyse, de genomen maatregelen en de monitoring van de werking is opgenomen;

2-Het opzetten van een incidentenregistratie;

3-Het creëren van een digitale map met daarin opgenomen de (bewijs-)stukken die aantonen dat het CSZ voortdurend aandacht heeft voor informatiebeveiligingsaangelegenheden;

4-Het introduceren van 2Factor-authentificatie en het maken van afspraken met de ICT-leverancier over data-restore tests.

[redacted]