



Aan de gemeenteraad

Portefeuillehouder	Team	Bijlage	Datum	Onderwerp
Leo Pieter Stoel	KCC	2	31 mei 2020	Collegeverklaring Ensia-audit 2020

Geachte leden van de raad,

Hierbij bieden wij u het ter informatie aan de "Collegeverklaring Ensia-audit 2020" rondom de gegevensverwerking van de Participatiewet. Vanuit de Baseline Informatiebeveiliging Overheid (BIO) worden verplichtingen gesteld aan een juist gebruik van Suwinet en DigiD in dit proces. Als gemeenteraad bent u belast met het toezicht hierop.

Via deze collegeverklaring geven wij als college aan dat wij voldoen aan de vanuit de BIO geselecteerde beheersnormen. Voor enkele niet geselecteerde beheersnormen zijn gerichte verbeterplannen opgenomen. Dit deel van het proces wordt door gemeente Leeuwarden uitgevoerd. Onze collegeverklaring is getoetst door een onafhankelijke auditor.

Met vriendelijke groet,
Het college van burgemeester en wethouders


Leo Pieter Stoel
burgemeester


Iwan Valk
secretaris-directeur

Bijlagen

- Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging Digid en Suwinet
- Assurance-rapport van de onafhankelijke IT-auditor

Jelmeraweg 1
9162 EA
Ballum-Ameland
Tel. 0519-555555
Fax 0519-555599

Postadres:
Postbus 22
9160 AA
Hollum-Ameland

info@ameland.nl
www.ameland.nl



Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Ameland legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2020 betreft dit Suwinet. De gemeente Ameland beschikt niet over een auditplichtige DigiD aansluiting.

De verklaring omvat het op 29 april 2021 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK¹) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI² en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA³ voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2020.

De beheersingsmaatregelen rond het gebruik van Suwinet die belegd zijn bij de Dienst Sociale Zaken en Werkgelegenheid Noordwest Fryslân vallen onder de reikwijdte van deze collegeverklaring.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlage voor Suwinet (bijlage 1 Suwinet met kenmerk Suwinet Ameland) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Ameland op 29 april 2021 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake Suwinet.

Ballum, 29 april 2021

College van B en W gemeente Ameland

1 <https://www.norea.nl/download/?id=2562>

2 <https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten>

3 <https://www.ensia.nl>

Aan:

College van Burgemeester en Wethouders
van de gemeente Ameland

Ons kenmerk: SH1344/A/20

Assurance-rapport van de onafhankelijke IT-auditor

Geacht college,

Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2020 inzake Informatiebeveiliging van Suwinet (hierna: collegeverklaring), inclusief de bijlage 1 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Ameland onderzocht.

Scope

De scope van ons onderzoek bestond uit de hierna genoemde Suwinet gegevensverwerkingen:

- Participatiewet

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

Ons oordeel

Wij hebben de bijgevoegde collegeverklaring ENSIA 2020 inzake informatiebeveiliging van Suwinet (hierna: collegeverklaring), inclusief de bijlage 1 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Ameland onderzocht tussen 22 februari 2021 en 29 april 2021.

Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlage 1 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Ameland, in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring omvat het op 31 december 2020 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen voldaan. Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel

.De basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de collegeverklaring verricht in overeenstemming met Richtlijn 3000-A (Herzien) 'Assuranceopdrachten door IT-auditors'



van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

Beperking in gebruik en verspreidingskring

Dit assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen Suwinet. Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Verantwoordelijkheden van het college van gemeente Ameland

Het college van burgemeester en wethouders van gemeente Ameland is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot Suwinet, zijn naast de collegeverklaring en dit assurance-rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

- de risico's die het bereiken van de geselecteerde normen voor Suwinet in gevaar brengen, werden geïdentificeerd; en
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven,

een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

Het college is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.



Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de collegeverklaring nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance-opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de collegeverklaring en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang bevat;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen; en
- het evalueren van de toereikendheid van de assurance-informatie zoals opgenomen in de collegeverklaring en bijbehorende bijlage(n).

Alkmaar, 29 april 2021

R. Driehuis RE-CISA CIPM

ir. drs. D.J.A. Koot

certified ISO/IEC 27001 Lead Auditor

Bijlagen:

Collegeverklaring met kenmerk Z234534-2021

Bijlage Suwinet met kenmerk Z234534-2021

