1432691

DUIJNBORGH AUDIT®

Aan:

Gemeente Beemster
t.a.v. het college van burgemeester en wethouders
Rijn Middelburgstraat 1
1462 NV Middenbeemster

Duijnborgh Audit b.v.

WTC Papendorp
Papendorpseweg 100
3528 BJ Utrecht
Postbus 40270
3504 AB Utrecht

T +31 (0)88 160 1700
F +31 (0)88 160 1799
I www.dbaudit.nl

IBAN: NL03 ABNA 0547 8300 25

KVK Midden Nederland
nr. 34224905

Plaats, datum	:	Utrecht, 20 april 2018
Referentie	:	20180420 DBA GEM-BEE ENSIA 2017
Betreft	:	Assurance-rapport betreffende de Collegeverklaring ENSIA 2017

Geacht college,

Ingevolge uw opdracht hebben wij de bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen) van gemeente Beemster onderzocht.

Ons oordeel

Naar ons oordeel is bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen) van gemeente Beemster in alle van materieel belang zijnde aspecten, juist.

In de collegeverklaring is op correcte wijze aangegeven dat aan enkele normen niet wordt voldaan. Dit betreft voor DigiD-aansluitnummer 1000149: norm U/WA.05 en voor DigiD-aansluitnummer 1001541: norm U/WA.05.

De Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (hierna Collegeverklaring ENSIA 2017) omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie verantwoordingsstelsel op website ENSIA voor de selectie van normen). Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel omtrent DigiD en Suwinet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel staan beschreven in de collegeverklaring.

Benadrukking aangelegenheden

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van de collegeverklaring en dit assurance-rapport. Wij hebben wel vastgesteld dat onze assurance bij deze collegeverklaring en de assurance bij de verantwoording van de dienstverlener aan wie de beheersingsmaatregelen zijn uitbesteed tezamen de geselecteerde normen inzake DigiD afdekken.

In de collegeverklaring is vermeld dat op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op deze verbeterplannen en de belegging en monitoring hiervan.

Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

Basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de Collegeverklaring ENSIA 2017 uitgevoerd volgens Nederlands recht, waaronder de Richtlijn 3000 (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 assuranceopdracht betreffende de Collegeverklaring ENSIA 2017'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd 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 ENSIA 2017. De Collegeverklaring ENSIA 2017 is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de Collegeverklaring ENSIA 2017 is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD en Suwinet. Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Beperkingen van interne beheersingsmaatregelen

Interne beheersingsmaatregelen kunnen vanwege hun aard niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

Werking niet onderzocht

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

Verantwoordelijkheden van het college van gemeente Beemster

Het college van burgemeester en wethouders van gemeente Beemster is verantwoordelijk voor het opstellen van de Collegeverklaring ENSIA 2017. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet dienen voldoende inzicht te hebben om deze collegeverklaring,

samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang in relatie tot DigiD en Suwinet inschatten.

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 DigiD en Suwinet in gevaar brengen, werden geïdentificeerd;
- 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 ook verantwoordelijk is voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring ENSIA 2017 mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring ENSIA 2017

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 ENSIA 2017 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 ENSIA 2017 en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen. Deze werkzaamheden hebben niet als doel om een oordeel uit te spreken over de effectiviteit van de interne beheersing van de gemeente;
- het op basis van deze kennis inschatten van de risico's dat de Collegeverklaring ENSIA 2017 onjuistheden van materieel belang bevat als gevolg van fraude en fouten, het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel. Bij fraude is het risico dat een

afwijking van materieel belang niet ontdekt wordt groter dan bij fouten. Bij fraude kan sprake zijn van samenspanning, valsheid in geschrifte, het opzettelijk nalaten transacties vast te leggen, het opzettelijk verkeerd voorstellen van zaken of het doorbreken van de interne beheersing;

- 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.

Utrecht, 20 april 2018

Duijnborgh Audit BV

F. Kossen RE

Drs. M. El Aarbaoui RE

BEEMSTER

VOORSTEL
BURGEMEESTER EN WETHOUDERS

onderwerp: *Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet* **datum: 3 april 2018**	***registratienummer(s)*** **:** **1420378** *domein* : *team* : *steller* : H. Winkel, tst. 0299-452514 *e-mail* : H.Winkel@purmerend.nl

mandaat: Nee *behandelwijze: Besloten* *portefeuillehouder(s):* A.J.M. van Beek

VOORSTEL OM TE BESLISSEN

1. Het vaststellen van de bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet.
2. Het laten uitvoeren van de verplichte audit op deze verklaring door een gecertificeerd IT-auditor.
3. Het aanbieden voor 1 mei 2018 van deze verklaring en auditrapportage aan Logius en aan het ministerie van Sociale Zaken en Werkgelegenheid.
4. Het aanbieden van deze verklaring tezamen met het Jaarverslag privacy en informatieveiligheid 2017 aan de Raad ter kennisneming.

bijgevoegd: 4 bijlagen o *brief* o *(Concept)raadsvoorstel en -besluit*

Financiële consequenties:	€	*paraaf controller:*	*paraaf bestuurs-adviseur:*
Programma	1. Publieksdiensten		
Binnen beschikbare budgetten:			

paraaf teammanager:	*paraaf directeur:*	*paraaf portefeuillehouder (voorstel is besproken):*

	gemeentesecretaris Van Duivenvoorde	burgemeester Van Beek	wethouder Butter	wethouder Zeeman
Akkoord				
Bespreken				

NA BESLUIT B & W

- o Collegebesluit terug naar het domein.
- • Collegebesluit terug naar het domein, na ondertekening van de bijgevoegde brieven/stukken.
- o Het bij dit voorstel gevoegde raadsvoorstel of brief ondertekenen en verzenden aan de griffie. Het collegebesluit daarna terug naar het domein.
- o Collegebesluit terug naar het domein met het verzoek de navolgende aanpassingen door te voeren:

.....

.....

Duijnborgh Audit BV
Behorend bij de assuranceverklaring
d.d.
20 APR. 2018

CONFORM ADVIES
-3 APR 2018

Registratienummer: 1420370

BEEMSTER

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Beemster 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 Gemeenten (BIG) 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 2017 betreft dit DigID (aansluitnummers: 1000149 en 1001541) en Suwinet. De verklaring omvat het op 31 december 2017 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 BZK[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA[3] 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 2017.

De beheersingsmaatregelen inzake DigID die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring "bijlage 1 DigID" blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

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 bijlagen voor DigiD (bijlage 1 DigID met kenmerk 1420371) en Suwinet (bijlage 2 Suwinet met kenmerk 1420372) geïnformeerd over de afwijkingen van de normen.

Duijnborgh Audit BV
Behorend bij de assuranceverklaring
d.d.
20 APR. 2018

[1] https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/
[2] https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten
[3] https://www.ensia.nl/

Verklaring college

Het college verklaart dat bij gemeente Beemster op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID en Suwinet. Voor DigiD wordt niet aan alle geselecteerde normen voldaan, te weten:

- DigID-aansluitnummer 1000149: U/WA.05
- DigID-aansluitnummer 1001541: U/WA.05

De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.

Beemster, 03 april 2018

burgemeester en wethouders van Beemster

A.J.M. van Beek
burgemeester

H.C.P. van Duivenvoorde
gemeentesecretaris

Duijnborgh Audit BV
Behorend bij de assuranceverklaring
d.d.

20 APR. 2018