ASSURANCE-RAPPORT VAN DE ONAFHANKELIJK IT-AUDITOR betreffende de collegeverklaring ENSIA 2018 gemeente Langedijk
(kenmerk: AR-30000201/ENSIA2018)

Aan: het College van Burgemeester en Wethouders van gemeente Langedijk

Ons oordeel
Wij hebben de bijgevoegde collegeverklaring ENSIA 2018 inzake informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Langedijk onderzocht.

Naar ons oordeel is bijgevoegde collegeverklaring inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Langedijk, in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring (met kenmerk 19SC001935) omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en 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 inzake Suwinet voldaan.

Benadrukking aangelegenheden

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 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 DigiD en Suwinet. Doel van de collegeverklaring 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.

Verantwoordelijkheden van het college van gemeente Langedijk
Het college van burgemeester en wethouders van gemeente Langedijk is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot DigiD en 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 DigiD en 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).

Zoetermeer, 26 april 2019
Astrium Advisory B.V.

Drs. N.E. Lansbergen RA EMITA RE

Paraaf voor waarmerkingsdoeleinden:

Collegeverklaring ENSIA 2018

inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Langedijk

Behorende bij ons
assurance-rapport d.d.
26 april 2019

Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Langedijk

Gemeentelijk kenmerk collegeverklaring ENSIA:	19SC001935
Naam auditfirma:	Astrium Advisory
Naam auditor:	Drs. Niels Lansbergen RA EMITA RE
Datum:	26 ~~maart~~ april 2019

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Langedijk voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Gemeenten (BIG), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Langedijk betreft dit in 2018 DigiD en Suwinet. De verklaring omvat het op 31 december 2018 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2018.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverleners vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverleners worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverleners worden uitgevoerd, wordt door de dienstverleners verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverleners dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan Halte Werk.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD) en

Behorende bij ons assurance-rapport d.d. 26 april 2019

Suwinet (bijlage 2 Suwinet) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD) en voor Suwinet (bijlage 2 Suwinet) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Langedijk op 31 december 2018 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD.

Het college verklaart dat voor Suwinet niet aan alle geselecteerde normen wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan opgenomen, zijn belegd en worden gemonitord.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1001281	Ja	n.v.t.
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	n.v.t.	Niet van toepassing

Zuid-Scharwoude, 26 maart 2019

College van B en W gemeente Langedijk

E. Annaert, gemeentesecretaris

L.A.M. Kompier, burgemeester

Bijlage 1 DigiD

Gemeentelijk kenmerk bijlage 1 DigiD:	19SC001935
Naam auditfirma:	Astrium Advisory
Naam auditor:	Drs. N.E. Lansbergen RA EMITA RE
Datum:	26 april 2019

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Langedijk04 en aansluitnummer 1001281

Dit is een bijlage bij de Collegeverklaring ENSIA 2018. Deze bijlage wordt opgesteld voor elke individuele DigiD aansluiting waarover wij verantwoording afleggen. Het doel van deze samenvatting is om het College en Logius een totaaloverzicht te verschaffen over de resultaten van DigiD-aansluiting Langedijk04 en aansluitnummer 1001281.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. In deze bijlage zijn de resultaten opgenomen van de uitgevoerde zelfevaluatie DigiD. Deze zelfevaluatie is toegepast op dat deel van het normenkader die niet onder uitbesteding aan onze leveranciers valt. De overige normen worden afgedekt door onderstaande TPM['s] / assurancerapportage['s] van onze serviceorganisatie[s]:

Leverancier 1	
Naam serviceorganisatie:	Denit Internet Services B.V.
Referentie/rapportnummer:	JH/jg/18-2046
Afgiftedatum:	12 november 2018
Naam RE-auditor:	ing. Jacques Herman RE RA
Ondertekend door RE-auditor:	Ja

Leverancier 2	
Naam serviceorganisatie:	Green Valley B.V.
Referentie/rapportnummer:	JH/av/18-2096
Afgiftedatum:	14 november 2018
Naam RE-auditor:	ing. Jacques Herman RE RA
Ondertekend door RE-auditor:	Ja

De uitkomsten uit de zelfevaluatie zijn getoetst door een RE-gecertificeerde IT-auditor. Deze heeft tevens getoetst of de zelfevaluatie en de TPM's van onze serviceorganisaties het gehele normenkader afdekken. De uitkomsten van de auditor zijn opgenomen in het assurancerapport met kenmerk AR-30000201/ENSIA2018. Onderstaande tabel toont de resultaten van de normen die zijn getoetst bij de serviceorganisatie én de bij ons getoetste normen. Het kan voorkomen dat een norm deels bij een leverancier getoetst is en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).

Behorende bij ons
assurance-rapport d.d.
26 april 2019

DigiD Norm		Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet		• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet		• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle	• Voldoet		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer	• Voldoet		• Voldoet	• Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet		• Voldoet	• Voldoet
U/PW.02	Garanderen webprotocollen	• Voldoet		• Voldoet	• Voldoet
U/PW.03	Configureren webserver	• Voldoet		• Voldoet	• Voldoet
U/PW.05	Toegang tot beheermechanismen	• Voldoet	• Voldoet	• Voldoet	• Voldoet
U/PW.07	Hardening van platformen	• Voldoet	• Voldoet	• Voldoet	• Voldoet
U/NW.03	DMZ	• Voldoet	• Voldoet		• Voldoet
U/NW.04	Protectie- en detectiemechanismen	• Voldoet	• Voldoet		• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	• Voldoet	• Voldoet		• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments	• Voldoet	• Voldoet		• Voldoet
C.04	Penetratietesten	• Voldoet	• Voldoet		• Voldoet
C.06	Signaleringsfuncties	• Voldoet	• Voldoet		• Voldoet
C.07	Monitoring functies	• Voldoet		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement	• Voldoet	• Voldoet	• Voldoet	• Voldoet

Hoeft volgens de gemeente en volgens hoofdstuk "verantwoordelijkheden gebruikersorganisatie" van de TPM van de serviceorganisatie niet bij de gemeente getoetst te worden.

Behorende bij ons assurance-rapport d.d. 26 april 2019

DigiD Norm	
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

Behorende bij ons
assurance-rapport d.d.
26 april 2019

Bijlage 2 Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging Suwinet

Gemeentelijk kenmerk bijlage 2 Suwinet:	19SC001935
Naam auditfirma:	Astrium Advisory
Naam auditor:	Drs. Niels Lansbergen RA EMITA RE
Datum:	26 april 2019

Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2018 van de gemeente Langedijk. Deze verklaring heeft betrekking op het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie Verantwoordingsstelsel ENSIA). Deze bijlage is opgesteld voor de gemeenteraad en het Ministerie van Sociale Zaken en Werkgelegenheid.

Onderwerp van de verklaring is het gebruik van Suwinet. Suwinet wordt wel in samenwerkingsverbanden gebruikt. Het gebruik van Suwinet door samenwerkingsverbanden valt binnen de reikwijdte van de verklaring.

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	**Organisatie**
Participatiewet/IOAW/IOAZ	Binnen de gemeente en samenwerkingsverband: Halte Werk

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	**Organisatie**
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Niet van toepassing
Loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing
Bijhouden BRP door Burgerzaken	Niet van toepassing

Normnaleving

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2018 in opzet en bestaan aan alle geselecteerde normen:

Behorende bij ons assurance-rapport d.d. 26 april 2019

SUWI-taak	Organisatie	BIG-nummer en SUWI-nummer	Applicatie
Participatiewet/IOAW/IOAZ	Halte Werk	B.01	DKD-Inlezen met Centric Snelbalie
Participatiewet/IOAW/IOAZ	Halte Werk	C.01	DKD-Inlezen met Centric Snelbalie
Participatiewet/IOAW/IOAZ	Halte Werk	C.05	DKD-Inlezen met Centric Snelbalie
Participatiewet/IOAW/IOAZ	Halte Werk	C.06	DKD-Inlezen met Centric Snelbalie