



Sluis_CVK_ENSIA_2020.02

Collegeverklaring Informatiebeveiliging DigiD en Suwinet Gemeente Sluis

Gemeentelijk kenmerk collegeverklaring ENSIA: Sluis_CVK_ENSIA_2020

BKBO: Concept opgesteld: 28-4-2021

College van B&W Definitief vastgesteld: 28-4-2021

Collegeverklaring informatiebeveiliging DigiD en Suwinet Gemeente Sluis

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate de gemeente Sluis voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA¹ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2020.

De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen [eventuele afwijkingen] en waar deze belegd zijn, is opgenomen in de bijlagen:

bijlage 1 DigiD met kenmerk: Sluis_DigiD1_Ensia2020_97028

bijlage 1 DigiD met kenmerk: Sluis_DigiD2_Ensia2020_1002547

bijlage 2 Suwinet met kenmerk: Sluis_SUWINET_Ensia2020

Verklaring college

Het college verklaart dat bij gemeente Sluis op 31 december 2020 de beheersingsmaatregelen (in opzet en bestaan) niet voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

¹ ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD (1) 97028	Ja	Niet van toepassing
DigiD (2) 1002547	Nee	Ja
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Sluis, 28 april 2021

College van Burgermeester en Wethouders gemeente Sluis

Naam auditfirma:

B.K.B.O. bv

Naam auditor:

Drs. M.B.H. IJpelaar

Datum: 29 april 2021



drs. M.B.H. IJpelaar RE CEH



BKBO bv 29/4/21
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37



drs. M.B.H. IJpelaar RE CEH

Gemeentelijk kenmerk bijlage 1 DigiD: Sluis_DigiD1_Ensia2020_97028

Bijlage 1 Sluis_DigiD1_Ensia2020_97028
Totaaloverzicht getoetste normen ICT-beveiligingsassessment
DigiD-aansluiting Gemeente Sluis en aansluitnummer 97028

Sluis biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Sluis voor authenticatie wordt gebruikt:

- Het genereren van aanvraagformulieren voor een uitkering
- Uittreksels van de Burgerlijke stand
- Geboorteakte
- Overlijdensacte
- Huwelijksakte
- Echtscheidingsakte
- Akte van partnerschapsregistratie
- Akte van beëindiging partnership

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- De front-office oplossingen van Visma-Roxit

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door de firma's Visma-Roxit (Frontoffice applicatie).

Deze applicatie is extern benaderbaar het volgende internetadres(sen):

<https://mijnsociaaldomein.gemeentesluis.nl>

DigiD-aansluiting Gemeente Sluis bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Hosted.nl in de vorm van Managed Hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Sluis. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Sluis heeft een deel van de DigiD web-omgeving uitbesteed aan Visma-Roxit en Hosted.nl. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier[s] van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM[s] / assurancerapportage[s] van de gemeentelijke serviceorganisatie[s]:

Leverancier 1

Naam serviceorganisatie:	Visma-Roxit
Referentie/rapportnummer:	JH/wk/20-1808 en JH/dd/21-0466
Afgiftedatum:	24 november 2020 en 4 maart 2021
Naam RE-auditor:	Ing. Jacques Herman RE RA (Deloitte Risk Advisory B.V.)
Ondertekend door RE-auditor:	Ja



BKBO bv 29/11/21
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37



drs. M.B.H. Ijpelaar RE CEH

Leverancier 2

Naam serviceorganisatie: Hosted.nl
 Referentie/rapportnummer: JH/ip/20-1817
 Afgiftedatum: 24 november 2020
 Naam RE-auditor: Ing. Jacques Herman RE RA
 (Deloitte Risk Advisory B.V.)
 Ondertekend door RE-auditor: Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM[s] / assurancerapportage[s] van onze serviceorganisatie[s] het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenoemde gedeelde norm). De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk BKBO/200818-4/AR

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij leverancier[s].

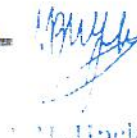
DigiD Norm	Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaal oordeel norm
B.05 Contractmanagement	Voldoet	Voldoet		Voldoet
U/TV.01 Identificatie en authenticatie	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02 Webapplicatiebeheer proces	Voldoet	Voldoet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

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

BKBO, <datum>



BKBO bv 29/11/21
 Voorstraat 20
 5251 CP Vlijmen
 073 - 211 03 37


 J. J. J. J. J.

RE CEH

Totaaloordeel norm voor alle normen uit het normenkader: Voldoet*

Getoetst bij de gemeente: Normen B05, U/TV01, U/WA02, U/WA05, U/NW06 en C08. Voldoet.

Getoetst bij de leverancier 1 (Visma-Roxit): B.05, U/TV.01, U/WA.02, U/WA.03, U/WA.04, U/WA.05, U/PW.02, U/PW.03, U/PW.05, U/PW.07, U/NW.06, C.08, C.09. Voldoet.

Getoetst bij leverancier 2 (Hosted.NL): U/TV.01, U/PW.05, U/PW.07, U/NW.03, U/NW.04, U/NW.05, U/NW.06, C.03, C.04, C.06, C.07, C.08, C.09. Voldoet.



BKBO bv *29/4/21 M.B.H.*
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 30 *hrs. M.B.H. Hooft*

Gemeentelijk kenmerk bijlage 1 DigiD: Sluis_DigiD2_Ensia2020_1002547

Bijlage 1 Sluis_DigiD2_Ensia2020_1002547

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting "Gemeente Sluis - Mijn Sociaal Domein" en aansluitnummer 1002547

Sluis biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Sluis Mijn Sociaal Domein voor authenticatie wordt gebruikt:

- DigiD applicatie Selfservice Sociaal Domein Mijn Inkomen en Mijn Regie biedt de mogelijkheid om digitale diensten te verlenen aan de burger. De versies die door EY zijn onderzocht zijn 24 (initieel assessment) en 25 (her-assessment)

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- DigiD applicatie Selfservice Sociaal Domein Mijn Inkomen en Mijn Regie van de "Gemeente Sluis - Mijn sociaal domein" en aansluitnummer 1002547.

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door de gemeente Sluis en Centric Netherlands B.V.

Deze applicatie is extern benaderbaar via [de] volgende internetadres(sen):

<https://mijnsociaaldomein.gemeentesluis.nl>

DigiD aansluiting Sluis Mijn Sociaal Domein bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Centric Netherlands BV (Centric Managed Services) in de vorm van een Managed Services contract.

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Sluis Mijn Sociaal Domein. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Sluis heeft een deel van de DigiD web-omgeving uitbesteed aan Centric Netherlands B.V. - Centric Managed Services. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier[s] van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM[s] / assurancerapportage[s] van de gemeentelijke serviceorganisatie[s]:

Leverancier 1

Naam serviceorganisatie:	Centric Netherlands B.V.
Referentie/rapportnummer:	REQ5157460_C
Afgiftedatum:	12 februari 2021
Naam RE-auditor:	Ir. Peter Kornelisse RE CISA CIPP/e (Ernst & Young Accountants LLP)
Ondertekend door RE-auditor:	Ja



BKBO bv 29/4/21
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37 drs. M.B.H. Ijpelaar RE CEH

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM[’s] / assurancerapportage[s] van onze serviceorganisatie[s] het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenoemde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk BKBO/200818-4/AR.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

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

Totaaloordeel norm voor alle normen uit het normenkader: Voldoet niet*

Getoetst bij de gemeente: Normen B05, U/TV01, U/WA02, U/WA05, U/NW06 en C08. Voldoet.

Getoetst bij de leverancier Centric: B.05 U/TV.01 U/WA.02 U/WA.03 U/WA.04 U/WA.05 U/PW.02 U/PW.05 U/PW.07 U/NW.03 U/NW.04 U/NW.05 U/NW.06 C.03 C.04 C.06 C.07 C.08 C.09 Voldoet.

Getoetst bij leverancier Centric, maar voldoet niet : U/PW.03 voldoet niet.



BKBO bv 29/4/20
 Voorstraat 20
 5251 CP Vlijmen
 073 - 211 03 37

[Handwritten signature]

RE CEH

Gemeentelijk kenmerk bijlage 2 Suwinet: Sluis_SUWINET_Ensia2020

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2020 van de gemeente Sluis. Onderwerp van de verklaring is het gebruik van Suwinet. Deze verklaring heeft betrekking op de Verantwoordingsrichtlijn GeVS 2020 welke is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO).

Suwinet-gegevens worden ten behoeve van de dienstverlening aan onze burgers niet door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	Binnen de gemeente: Team Porthos – afd. Externe Dienstverlening	Ja/Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente: Team Porthos – afd. Externe Dienstverlening	Ja/Ja
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente: Team Porthos – afd. Externe Dienstverlening	Ja/Ja

Gebruik van Suwinet voor niet-SUWI-taken

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

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Niet van toepassing	Nee/Nee
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing	Nee/Nee
Adresonderzoek door Burgerzaken	Binnen de gemeente door Burgerzaken – afd. Externe Dienstverlening	Ja/Ja

Naleving BIO-maatregelen

Zoals in de Collegeverklaring vermeld, voldoet de gemeente Sluis aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2020 in opzet en bestaan aan de geselecteerde controls.



BKBO bv 29/4/21
 Voorstraat 20
 5251 CP Vlijmen
 073 - 211 03 37 drs. M.B.H. Ijpelaar RE CEH

Nico Boom

Van: Marga Vermue
Verzonden: woensdag 28 april 2021 17:16
Aan: Nico Boom
CC: Samira de Kievit - Minnaert; Bestuurssecretariaat gemeente Sluis
Onderwerp: Re: Digitaal Ondertekenen Collegeverklaring Ensia 2020

Akkoord Nico.

En dank voor de telefonische uitleg want het is een ingewikkelde materie.

Met vriendelijke groeten,

mr. M.(**Marga**) M.D. Vermue
Burgemeester gemeente Sluis
Nieuwstraat 22, 4501 BD Oostburg
Postbus 27, 4500 AA Oostburg
Tel: 0117-457313
mvermue@gemeentesluis.nl
www.gemeentesluis.nl

Op 28 apr. 2021 om 17:01 heeft Nico Boom <NBoom@gemeentesluis.nl> het volgende geschreven:

Goedendag mevrouw de Burgermeester,

Beste Marga,

Naar aanleiding van de toetsing van de Collegeverklaring Ensia 2020 en de uitgevoerde audit door BKBO is er op één punt een afwijking geconstateerd.

Een van de te toetsen beveiligingspunten in Suwinet Sociaal Domein, is door BKBO op basis van de third Party mededelingen als "voldoet niet" bestempeld.

Centric is er niet op tijd in geslaagd dit op te lossen. Het 'voldoet niet' punt is genaamd U/PW.03 en heeft betrekking op het inrichten van de webserver Suwinet conform een bepaalde configuratie baseline.

Het gaat hier om een norm hoe de configuratie wordt vorm gegeven. Deze nieuwe norm had in 2020 uitgevoerd dienen te zijn. De nieuwe oplostermijn is 1-11-2021.

Daarmee is geborgd dat dit punt in de ENSIA 2021 geen herhaling kent

Graag ontvang ik van u voor de definitieve afhandeling van de Collegeverklaring uw akkoord op de verklaring.

De auditor tekent vervolgens het stuk en de ENSIA kan procesmatig afgerond worden via de daarvoor bestemde kanalen.

Volgende stap is het aanbieden van de stukken aan het College en de Raad.

Hartelijke groet
Nico Boom

Ps :

De correctie is te lezen op pagina 3 en 8!

Van: Nico Boom

Verzonden: woensdag 14 april 2021 22:31

Aan: Marga Vermue <MVermue@gemeentesluis.nl>

CC: Samira de Kievit - Minnaert <SdeKievit@gemeentesluis.nl>; Bestuurssecretariaat gemeente Sluis <Bestuurssecretariaat@gemeentesluis.nl>

Onderwerp: Digitaal Ondertekenen Collegeverklaring Ensia 2020

Goedendag mevrouw de Burgermeester,

Beste Marga

Hierbij de Collegeverklaring ENSIA 2020, welke door u ondertekend dient te worden alvorens deze wordt ondertekend door onze auditor BKBO.

Er zijn geen opmerkingen uit de zelfevaluaties DigiD m.b.t. de informatiebeveiliging conform de ENSIA vragenlijsten.

Zodra de terugkoppeling van de auditor van BKBO getekend retour komt wordt de volledige ENSIA verantwoording aan het college ter vaststelling aangeboden worden, zodat deze vervolgens aan de raad kan worden voorgelegd. (uiterlijk 1 juli 2021)

Dit jaar is er vanwege Covid 19 ruimte geboden om de collegeverklaring digitaal te ondertekenen.

Wilt u akkoord geven door deze mail te beantwoorden en aan te geven dat u akkoord gaat met de collegeverklaring ENSIA 2020.

Deze mail wordt als bijlage aan de collegeverklaring toegevoegd als 'digitale handtekening'

Aub uw reactie met naam, dagtekening en uw outlook handtekening zodat duidelijk is dat deze van u afkomstig is.

Hartelijk dank,

Nico Boom

<Collegeverklaring-ENSIA-2020v2-inzake-Informatiebeveiliging-DigiD-en-Suwinet-Sluis-20210301105656.docx>