INSTRUCTIE OPSTELLEN COLLEGEVERKLARING EN BIJLAGE(N)

Inleiding

Dit format collegeverklaring en de bijlagen die zijn gedownload uit ENSIA zijn vormvast. Dit betekent dat er geen ruimte is voor inhoudelijke aanvullingen en/of aanpassingen. Met deze instructie leiden wij u puntsgewijs door het format.

1. De haakjes [en]

Het format leidt u op een aantal plaatsen naar keuzes. Deze keuzes zijn met het volgende teken aangegeven: [[tekst instructie [tekst voor de collegeverklaring]]

De tekst die binnen de omsluiting van de tekens wordt aangegeven geeft:

- De mogelijkheid tot het opnemen van een keuze. U neemt een van de keuzes op. De andere keuze(s) en de vierkante haken verwijdert u.
- Tekst voor instructie. Deze verwijdert u.
- De op te nemen (vaste) tekstdelen. Deze neemt u op.

Hieronder een voorbeeld en daarna de praktische toepassing:
[[Indien in het kader van Suwinet geen sprake is van samenwerking dan opnemen: [Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersingsmaatregelen van de gemeente.]]

[[Indien wel sprake is van samenwerking bij Suwinet:[Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan [naam samenwerkingsverband[en] [en] [of] [andere gemeente].]]

Wanneer géén sprake is van samenwerking op voor het gebruik van Suwinet, wordt de tekst in de collegeverklaring:
‘Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersingsmaatregelen van de gemeente.’

Indien sprake is van samenwerking voor het gebruik van Suwinet, wordt de tekst in de collegeverklaring:
‘Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan Samenwerkingsverband Snel naar Werk.’

2. Gebruik van [kenmerk]

Op verschillende plaatsen wordt in de collegeverklaring gevraagd naar een kenmerk van een document. Dit betreft het kenmerk welk de gemeente zelf toekent aan het document. De collegeverklaring, de bijlage Suwinet en de bijlage DigiD krijgen elk een eigen kenmerk. In de bijlage DigiD wordt op één plaats gevraagd naar het kenmerk van het assurance rapport van de auditor. U kunt dit afleiden uit de tekst.

3. Gebruik tabel in de collegeverklaring bij ‘samenvattend beeld’

De tabel geeft een samenvatting van de uitwerkingen in de bijlage(n). De tabel in het format is opgesteld voor 9 aansluitingen. De regels die u niet gebruikt, omdat u over minder bestaande aansluitingen verantwoording aflegt, verwijdert u. De regels met ‘Suwinet voor SUWI-taken’, en ‘Suwinet voor niet-SUWI-taken’ verwijdert u niet. Wanneer u geen gebruik maakt van deze voorziening geeft u het antwoord ‘niet van toepassing’ in.

4. Indien verantwoording DigiD: Bijlage 1 DigiD bij collegeverklaring ENSIA

Voor elke DigiD aansluiting waarover u zich verantwoordt, neemt u een bijlage DigiD op bij de collegeverklaring. De gehele bijlage DigiD krijgt één separaat kenmerk. De verschillende bijlagen houden dezelfde titel ‘Bijlage 1 DigiD bij collegeverklaring ENSIA’. U ziet in de nummering dat per DigiD aansluiting een volgnummer is opgenomen in de titel (1), (2), etc.

Op de eerste pagina van de bijlage DigiD zijn standaard twee tabellen opgenomen. In deze tabellen geeft u de informatie op over de leveranciers en de gegevens van de TPM. De naam ‘leverancier 1’, ‘leverancier 2’, corresponderen hierna met de grote tabel waarin de uitkomsten van de zelfevaluatie zijn opgenomen. U gaat op de volgende wijze om met de tabellen:

- Bij uitbestede diensten aan één leverancier, verwijdert u de tweede tabel
- Bij uitbestede diensten aan meer dan twee leveranciers, voegt u eenzelfde tabel toe
- Indien u geen TPM ontvangt van uw leverancier, dan doet uw eigen auditor onderzoek. In dat geval kiest u bij ‘Referentie/rapportnummer’, ‘Afgiftedatum’ en ‘Naam RE-auditor’ voor ‘niet van toepassing’. En vult u bij ‘Naam serviceorganisatie’ de naam van uw leverancier of serviceorganisatie in.
- Wanneer u alles in eigen beheer uitvoert (geen leverancier), dan laat u de eerste tabel in het document staan en vult u ‘niet van toepassing in’. De tweede tabel verwijdert u.

De tabel met de uitkomsten uit de zelfevaluatie vult u met de juiste antwoorden vanuit de zelfevaluatie. Deze bestaat uit ‘voldoet’ of ‘voldoet niet’. U vult een cel grijs op wanneer de norm niet van toepassing is bij de gemeente of indien de norm niet van toepassing is op een leverancier. De laatste kolom geeft het totaal oordeel met een ‘voldoet’ of ‘voldoet niet’ antwoord. Indien bij een norm in enige cel de uitkomst 'voldoet niet' is, kan het totaal oordeel nooit tot een positief totaal oordeel leiden: het antwoord is dan altijd 'voldoet niet'.

Zie onderstaand voorbeeld:

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet		• Voldoet

In de tabel geeft u de kolommen ‘Getoetst bij leverancier’ zo vorm dat deze passen bij uw situatie: U verwijdert of neemt een extra kolom op (of verwijdert beide kolommen ‘Getoetst bij leverancier’) indien alles in eigen beheer is opgesteld). In het format is uitgegaan van 2 leveranciers.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Getoetst bij leverancier 2	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet niet	• Voldoet	• Voldoet niet

Indien een tabel op een volgende pagina doorloopt laat u, via de optie ‘Indeling’ en ‘Veldnamenrij herhalen’, de kolomhoofden terugkomen op de deze pagina.

5. Indien verantwoording Suwinet: Bijlage 2 ‘Gebruik van Suwinet’

In de bijlage Suwinet neemt u de uitkomsten van de zelfevaluatie op over het gebruik van Suwinet. In de te vullen tabellen wordt een keuze aangegeven van:

- Binnen de gemeente: Gemeentelijke organisatie (exclusief samenwerkingsverband(en))
- Samenwerkingsverband: Samenwerkingsverbanden in elke vorm, aangevuld met de naam.

Hieronder een voorbeeld en praktische toepassing:

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

Taak	Organisatie
Participatiewet	Binnen de gemeente en samenwerkingsverband Snel naar werk.

Onder de kop ‘Normnaleving’ kiest u voor de passende uitkomst. Indien uw situatie ‘Zoals in de collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2019 in opzet en bestaan aan de geselecteerde normen’ is, dan verwijdert u de beide tabellen.

Indien de uitkomst van de zelfevaluatie leidt tot ‘Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2019 in opzet en bestaan aan alle geselecteerde normen:’, dan vult u de beide tabellen aan met de gevraagde informatie.

6. Parafering en/of ondertekening auditor

De auditor ondertekent/parafeert na ondertekening van het college, de verklaring van het college, de bijlage(n) en het assurancerapport. Auditors kunnen op de site van NOREA de instructie vinden voor het juist ondertekenen/paraferen, het waarmerken en omzetten van documenten naar PDF/a formaat van de documenten.

7. Tot slot

Heeft u vragen, neem dan contact op met het ENSIA-team bij VNG Realisatie via 070-250 2400 of via ensia@vng.nl.

De instructie tekst eindigt hier. Bovenstaande tekst verwijdert u. Deze maakt geen onderdeel uit van de collegeverklaring.

Collegeverklaring ENSIA 2019

inzake informatiebeveiliging Suwinet

Gemeente <naam gemeente>

[De collegeverklaring dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de collegeverklaring begint met uw kenmerk.]

Gemeentelijk kenmerk collegeverklaring ENSIA:	

Collegeverklaring ENSIA inzake informatiebeveiliging Suwinet

Gemeente <naam gemeente>

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente <naam gemeente> voldoet aan de voor 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), wet- en regelgeving reisdocumenten, 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 en diepgang 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 het jaar 2019 voor gemeente <naam gemeente> betreft dit Suwinet.

De verklaring omvat het op 31 december 2019 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2019.

[[Indien in het kader van Suwinet geen sprake is van samenwerking dan opnemen: [Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersingsmaatregelen van de gemeente.]]

[[Indien wel sprake is van samenwerking bij Suwinet:[Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan [naam samenwerkingsverband[en] [en] [of] [andere gemeente].]]

Deze collegeverklaring is opgesteld voor de gemeenteraad en het ministerie van Sociale Zaken en Werkgelegenheid (SZW) die toezien op de veiligheid van Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake Suwinet. In de bij deze verklaring behorende afzonderlijke bijlage Suwinet (bijlage 1 Suwinet met kenmerk [kenmerk]) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en het ministerie van Sociale Zaken en Werkgelegenheid (SZW) worden via bij deze collegeverklaring behorende afzonderlijke bijlage voor Suwinet (bijlage 1 Suwinet met kenmerk [kenmerk]) geïnformeerd over de afwijkingen van de normen.

Verklaring college

[[Indien volledig wordt voldaan aan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de normen inzake Suwinet]].

[[Bij uitzonderingen: [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 opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
Suwinet voor SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja][Nee] [Niet van toepassing]
Suwinet voor niet-SUWI-taken	[Ja][Nee] [Niet van toepassing]	[Ja][Nee] [Niet van toepassing]

[Plaatsnaam], [datum]

College van B en W gemeente <naam gemeente>

[naam/namen en functie('s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

[Hieronder start de bijlage Suwinet. De bijlage Suwinet dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de bijlage begint met uw kenmerk.]

Gemeentelijk kenmerk bijlage 1 Suwinet:	

Bijlage 1 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA 2019 van de gemeente <naam gemeente>. Deze verklaring heeft betrekking op het op 31 december 2019 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][niet] in samenwerkingsverbanden gebruikt. [[Indien 'wel': [Het gebruik van Suwinet door samenwerkingsverbanden valt binnen de reikwijdte van de verklaring.]] [[Indien niet alle Suwinet voorzieningen waar de gemeente gebruik van maakt, zijn opgenomen in de collegeverklaring: [Het college is zich ervan bewust dat de Suwinet voorziening voor [vul type SUWI-taak/niet-SUWI-taak] door [organisatie] niet is opgenomen in deze collegeverklaring.]]

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie
Participatiewet (Pw)	[binnen de gemeente] [en] [of] [samenwerkingsverband[en] [en] [of] [andere gemeente]: [[naam samenwerkingsverband[en]] [en] [[naam andere gemeente]]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)	[binnen de gemeente] [en] [of] [samenwerkingsverband[en] [en] [of] [andere gemeente]: [[naam samenwerkingsverband[en]] [en] [[naam andere gemeente]]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[binnen de gemeente] [en] [of] [samenwerkingsverband[en] [en] [of] [andere gemeente]: [[naam samenwerkingsverband[en]] [en] [[naam andere gemeente]]

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] [binnen de gemeente] [en] [samenwerkingsverband[en] [en] [andere gemeente]: [[naam samenwerkingsverband[en]] [[naam andere gemeente]]
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	[Niet van toepassing] [binnen de gemeente] [en] [samenwerkingsverband[en] [en] [andere gemeente]: [[naam samenwerkingsverband[en]] [[naam andere gemeente]]

Adresonderzoek door Burgerzaken	[Niet van toepassing] [binnen de gemeente] [en] [samenwerkingsverband[en] [en] [andere gemeente]: [[naam samenwerkingsverband[en]] [[naam andere gemeente]]

Normnaleving

[[Indien geen afwijkingen van de normen:

[Zoals in de collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2019 in opzet en bestaan aan de geselecteerde normen.]]

[[Bij afwijkingen van de normen betreffende SUWI-taken:

[Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2019 in opzet en bestaan aan alle geselecteerde normen:

Organisatie	SUWI-taak	BIG nummer en nummer SUWI norm	Applicatie
			[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]

]]

[[bij afwijkingen van de normen betreffende niet-SUWI-taken:

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

Organisatie	Niet-SUWI-taak	BIG nummer en nummer SUWI norm	Applicatie
			[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]

]]

Collegeverklaring ENSIA 2019

inzake informatiebeveiliging DigiD

Gemeente <naam gemeente>

[De collegeverklaring dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de collegeverklaring begint met uw kenmerk.]

Gemeentelijk kenmerk collegeverklaring ENSIA:	

Collegeverklaring ENSIA 2019 inzake Informatiebeveiliging DigiD

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente <naam gemeente> voldoet aan de voor DigiD 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), wet- en regelgeving reisdocumenten, 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 en diepgang 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 2019 voor gemeente <naam gemeente> betreft dit DigiD. De verklaring omvat het op 31 december 2019 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2019.

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

Deze collegeverklaring is opgesteld voor de gemeenteraad en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) die toezien op de veiligheid van DigiD. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD. In de bij deze verklaring behorende afzonderlijke bijlage voor DigiD (bijlage 1 DigiD met kenmerk [kenmerk]) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) worden via bij deze collegeverklaring behorende afzonderlijke bijlage voor DigiD (bijlage 1 DigiD met kenmerk [kenmerk]) geïnformeerd over de afwijkingen van de normen.

Verklaring college

[[Indien volledig wordt voldaan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2019 de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de normen inzake DigiD]].

[[Bij uitzonderingen: [Het college verklaart dat voor DigiD 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 (1)	[Ja] [Nee]	[Ja] [Nee]
DigiD (2)	[Ja] [Nee]	[Ja] [Nee]
DigiD (3)	[Ja] [Nee]	[Ja] [Nee]
DigiD (4)	[Ja] [Nee]	[Ja] [Nee]
DigiD (5)	[Ja] [Nee]	[Ja] [Nee]
DigiD (6)	[Ja] [Nee]	[Ja] [Nee]
DigiD (7)	[Ja] [Nee]	[Ja] [Nee]
DigiD (8)	[Ja] [Nee]	[Ja] [Nee]
DigiD (9)	[Ja] [Nee]	[Ja] [Nee]

[Plaatsnaam], [datum]

College van B en W gemeente <naam gemeente>

[naam/namen en functie('s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

[Hieronder start de bijlage DigiD. De bijlage DigiD dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de bijlage begint met uw kenmerk.]

Gemeentelijk kenmerk bijlage 1 DigiD:	

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting <naam aansluiting> en aansluitnummer <aansluitnummer>

<Naam gemeente> biedt de volgende functionaliteit aan waarvoor DigiD aansluiting <naam aansluiting> voor authenticatie wordt gebruikt:

- [voeg hier (een opsomming) van de geboden functionaliteit toe bijvoorbeeld 'Het genereren van aanvraagformulieren voor een uitkering bij de snelbalie'].

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- [geef hier de naam van de applicatie op, bijvoorbeeld Snelbalie]

Deze applicatie betreft [[maak een keuze uit [geheel maatwerk] [een combinatie van maatwerk en standaard software] [een geheel standaard pakket]] en wordt onderhouden door [naam gemeente en/ of naam leverancier(s)].

Deze applicatie is extern benaderbaar via de volgende URL['s]: [neem hier de extern benaderbare website(s) op].

DigiD aansluiting <Naam aansluiting> bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door [naam gemeente en/of naam leverancier[s]] in de vorm van [neem vorm op bijvoorbeeld, fysieke hosting, IAAS, PAAS, SAAS].

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting <naam aansluiting>. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL['s] 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.

[[Alleen indien er een serviceorganisatie is, anders weglaten] <Naam gemeente> heeft een deel van de DigiD webomgeving uitbesteed aan [naam leverancier[s]]. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie[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 onze leverancier[s] valt. De overige normen worden afgedekt door onderstaande TPM['s] / assurancerapportage['s] van onze serviceorganisatie[s]:

Leverancier 1	
Naam serviceorganisatie: Referentie/rapportnummer:	 [Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor: Ondertekend door RE-auditor:	[Naam] [[maak keuze [Ja] [Nee]]

Leverancier 2	
Naam serviceorganisatie:	
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[[maak keuze [Ja] [Nee]]

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 (zogenaamde 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 [kenmerk van het assurancerapport van onze auditor].

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm [[opnemen indien van toepassing [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 niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/TV.01	Identificatie en authenticatie	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.02	Webapplicatiebeheer proces	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.03	Automatische data invoer controle	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.04	Normaliseren uitvoer	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.02	Garanderen webprotocollen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.03	Configureren webserver	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.05	Toegang tot beheermechanismen	• Voldoet	• Voldoet	• Voldoet	• Voldoet

DigiD Norm		Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaal oordeel norm
		• Voldoet niet • Grijs	• Voldoet niet • Grijs	• Voldoet niet • Grijs	• Voldoet niet • Grijs
U/PW.07	Hardening van platformen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.03	DMZ	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.04	Protectie- en detectiemechanismen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.05	Scheiding beheer- en productieomgeving	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.06	Hardening van netwerken	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.03	Vulnerability-assessments	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.04	Penetratietesten	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.06	Signaleringsfuncties	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.07	Monitoring functies	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.08	Wijzigingenbeheer	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.09	Patchmanagement	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs

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.

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.

Collegeverklaring ENSIA 2019

inzake informatiebeveiliging DigiD en Suwinet

Gemeente <naam gemeente>

[De collegeverklaring dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de collegeverklaring begint met uw kenmerk.]

Gemeentelijk kenmerk collegeverklaring ENSIA:	

Collegeverklaring ENSIA 2019 inzake informatiebeveiliging DigiD en Suwinet

Gemeente <naam gemeente>

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente <naam gemeente> 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), wet- en regelgeving reisdocumenten, 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 en diepgang 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 <naam gemeente> betreft dit in 2019 DigiD en Suwinet.

De verklaring omvat het op 31 december 2019 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 2019.

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

[[Indien in het kader van Suwinet geen sprake is van samenwerking dan opnemen: [Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersingsmaatregelen van de gemeente.]]

[[Indien wel sprake is van samenwerking bij Suwinet:[Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan [naam samenwerkingsverband[en] [en] [of] [andere gemeente].]]

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 bijlage voor DigiD (bijlage 1 DigiD met kenmerk [kenmerk]) en Suwinet (bijlage 2 Suwinet met kenmerk [kenmerk]) 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 met kenmerk [kenmerk]) en voor Suwinet (bijlage 2 Suwinet met kenmerk [kenmerk]) geïnformeerd over de afwijkingen van de normen.

Verklaring college

[[Indien volledig wordt voldaan aan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.]]

[[Bij uitzonderingen: [Het college verklaart dat voor [DigiD] [en] [Suwinet] niet aan alle geselecteerde normen wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in [een] verbeterplan[nen] 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 (1)	[Ja] [Nee]	[Ja] [Nee]
DigiD (2)	[Ja] [Nee]	[Ja] [Nee]
DigiD (3)	[Ja] [Nee]	[Ja] [Nee]
DigiD (4)	[Ja] [Nee]	[Ja] [Nee]
DigiD (5)	[Ja] [Nee]	[Ja] [Nee]
DigiD (6)	[Ja] [Nee]	[Ja] [Nee]
DigiD (7)	[Ja] [Nee]	[Ja] [Nee]
DigiD (8)	[Ja] [Nee]	[Ja] [Nee]
DigiD (9)	[Ja] [Nee]	[Ja] [Nee]
Suwinet voor SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]
Suwinet voor niet-SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]

[Plaatsnaam], [datum]

College van B en W gemeente <naam gemeente>

[naam/namen en functie('s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

[Hieronder start de bijlage DigiD. De bijlage DigiD dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de bijlage begint met uw kenmerk.]

Gemeentelijk kenmerk bijlage 1 DigiD:	

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting <naam aansluiting> en aansluitnummer <aansluitnummer>

<Naam gemeente> biedt de volgende functionaliteit aan waarvoor DigiD aansluiting <naam aansluiting> voor authenticatie wordt gebruikt:

- [voeg hier (een opsomming) van de geboden functionaliteit toe bijvoorbeeld 'Het genereren van aanvraagformulieren voor een uitkering bij de snelbalie'].

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- [geef hier de naam van de applicatie op, bijvoorbeeld Snelbalie]

Deze applicatie betreft [[maak een keuze uit [geheel maatwerk] [een combinatie van maatwerk en standaard software] [een geheel standaard pakket]] en wordt onderhouden door [naam gemeente en/ of naam leverancier(s)].

Deze applicatie is extern benaderbaar via de volgende URL['s]: [neem hier de extern benaderbare website(s) op].

DigiD aansluiting <Naam aansluiting> bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door [naam gemeente en/of naam leverancier[s]] in de vorm van [neem vorm op bijvoorbeeld, fysieke hosting, IAAS, PAAS, SAAS].

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting <naam aansluiting>. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL['s] 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.

[[Alleen indien er een serviceorganisatie is, anders weglaten] <Naam gemeente> heeft een deel van de DigiD webomgeving uitbesteed aan [naam leverancier[s]]. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie[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 onze leverancier[s] valt. De overige normen worden afgedekt door onderstaande TPM['s] / assurancerapportage['s] van onze serviceorganisatie[s]:

Leverancier 1	
Naam serviceorganisatie:	
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]

Leverancier 1	
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[[maak keuze [Ja] [Nee]]

Leverancier 2	
Naam serviceorganisatie:	
Referentie/rapportnummer:	[Nummer]
Afgiftedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[[maak keuze [Ja] [Nee]]

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 (zogenaamde 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 [kenmerk van het assurancerapport van onze auditor].

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm [[opnemen indien van toepassing [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 niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/TV.01	Identificatie en authenticatie	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.02	Webapplicatiebeheer proces	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.03	Automatische data invoer controle	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.04	Normaliseren uitvoer	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.02	Garanderen webprotocollen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs

DigiD Norm		Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaal oordeel norm
U/PW.03	Configureren webserver	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.05	Toegang tot beheermechanismen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.07	Hardening van platformen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.03	DMZ	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.04	Protectie- en detectiemechanismen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.05	Scheiding beheer- en productieomgeving	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.06	Hardening van netwerken	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.03	Vulnerability-assessments	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.04	Penetratietesten	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.06	Signaleringsfuncties	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.07	Monitoring functies	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.08	Wijzigingenbeheer	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.09	Patchmanagement	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs

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.

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.

[Hieronder start de bijlage Suwinet. De bijlage Suwinet dient te worden van voorzien van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de bijlage begint met uw kenmerk.]

Gemeentelijk kenmerk bijlage 2 Suwinet:	

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA 2019 van de gemeente <naam gemeente>. Deze verklaring heeft betrekking op het op 31 december 2019 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][niet] in samenwerkingsverbanden gebruikt. [[Indien 'wel': [Het gebruik van Suwinet door samenwerkingsverbanden valt binnen de reikwijdte van de verklaring.]] [[Indien niet alle Suwinet voorzieningen waar de gemeente gebruik van maakt, zijn opgenomen in de collegeverklaring: [Het college is zich ervan bewust dat de Suwinet voorziening voor [vul type SUWI-taak/niet-SUWI-taak] door [organisatie] niet is opgenomen in deze collegeverklaring.]]

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie
Participatiewet (Pw)	[binnen de gemeente] [en] [of] [samenwerkingsverband[en] [en] [of] [andere gemeente]: [[naam samenwerkingsverband[en]] [en] [[naam andere gemeente]]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)	[binnen de gemeente] [en] [of] [samenwerkingsverband[en] [en] [of] [andere gemeente]: [[naam samenwerkingsverband[en]] [en] [[naam andere gemeente]]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[binnen de gemeente] [en] [of] [samenwerkingsverband[en] [en] [of] [andere gemeente]: [[naam samenwerkingsverband[en]] [en] [[naam andere gemeente]]

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] [binnen de gemeente] [en] [samenwerkingsverband[en] [en] [andere gemeente]: [[naam samenwerkingsverband[en]] [[naam andere gemeente]]

Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	[Niet van toepassing] [binnen de gemeente] [en] [samenwerkingsverband[en] [en] [andere gemeente]: [[naam samenwerkingsverband[en]] [[naam andere gemeente]]
Adresonderzoek door Burgerzaken	[Niet van toepassing] [binnen de gemeente] [en] [samenwerkingsverband[en] [en] [andere gemeente]: [[naam samenwerkingsverband[en]] [[naam andere gemeente]]

Normnaleving

[[Indien geen afwijkingen van de normen:

[Zoals in de collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2019 in opzet en bestaan aan de geselecteerde normen.]]

[[Bij afwijkingen van de normen betreffende SUWI-taken:

[Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2019 in opzet en bestaan aan alle geselecteerde normen:

Organisatie	SUWI-taak	BIG nummer en nummer SUWI norm	Applicatie
			[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]

]]

[[bij afwijkingen van de normen betreffende niet-SUWI-taken:

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

Organisatie	Niet-SUWI-taak	BIG nummer en nummer SUWI norm	Applicatie
			[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]

]]