

## Raadsinformatiebrief

Van	Burgemeester en Wethouder/Burgemeester	Zaak nr.	755160
Aan	Gemeenteraad	RIB nr.	2021-29
Portefeuillehouder	K. Walters	Datum	31 maart 2021
Informatie bij	Jaap Huib van der Knaap (CISO) Harriët Arnolds (ENSIA coördinator)	Tel. nr.	(035) 629 2013

### Onderwerp

Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet

### Kernboodschap

In de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek is het verplicht een collegeverklaring vast te stellen. De concept collegeverklaring is op 5 maart 2021 geaudit door een externe auditor. De auditor geeft een assurance verklaring af over de collegeverklaring en de bijlagen. Die assuranceverklaring is noodzakelijk voor de continuering van de aansluitingen op DigiD en Suwinet<sup>1</sup>.

Het gaat daarbij om de DigiD aansluitingen op:

1. de gemeentelijke website
2. e-diensten voor het sociaal domein
3. e-dienstverlening voor belastingen

### Aanleiding

ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk verantwoordingsstelsel voor informatieveiligheid, gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIO. De verantwoordingsystematiek over de Basisregistratie Personen (BRP) en wet- en regelgeving Reisdocumenten (Paspoortuitvoeringsregeling Nederland (PUN) en Paspoorten en Nederlandse Identiteitskaarten (PNIK)), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is daarmee samengevoegd en gestroomlijnd.

Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan de Rijksoverheid (ministeries en uitvoeringsorganisaties) die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van 'single information single audit' toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces.

<sup>1</sup> <https://www.bkwi.nl/producten/suwinet-services/>  
Structuur Uitvoering Werk en Inkomen (SUWI)

Met het vaststellen van de collegeverklaring verklaart het College in hoeverre de Gemeente Hilversum voldoet aan de vereiste normen voor DigiD en Suwinet. Alle voorgaande jaren voldeden we aan alle normen. En ook dit jaar voldoen we voor Suwinet aan alle informatiebeveiligingsnormen.

Voor DigiD wordt dit jaar niet aan alle informatiebeveiligingsnormen voldaan. Wij krijgen jaarlijks verschillende Third Party Memoranda (TPM's) waarin een auditor ons een verklaring geeft voor de aansluitingen bij de verschillende leveranciers. Voor onze drie DigiD aansluitingen is er bij die audits vast komen te staan dat zij nog niet volledig voldoen aan de norm. Er is namelijk in 2020 een aanscherping van één norm geweest die niet alle leveranciers (op tijd) hebben gerealiseerd. Het gaat om een technische wijziging op de testaanpak waarbij de leverancier op een bepaalde manier de DigiD moet testen. Er is dus wel degelijk op die norm getest door onze leveranciers; maar ze hadden de test volgens de aangescherpte norm moeten uitvoeren. De leveranciers van onze drie DigiD aansluitingen geven bij hun auditor aan dat er een ontwikkelplan c.q. een verbeterplan uitgevoerd wordt waarbij uiterlijk 1 november 2021 aan de testaanpak voor deze norm zal worden voldaan.

Dat er niet aan deze specifieke norm voldaan wordt, geldt in Nederland voor meerdere leveranciers die een DigiD aansluiting namens een gemeente beheren. Met de toezichthouder Logius – die de DigiD aansluitingen bewaakt – is landelijk overeengekomen dat alle leveranciers tot 1 november 2021 de tijd hebben om een verbeterde Third Party Memorandum aan te leveren.

De CISO en ENSIA-coördinator van Hilversum bewaken dit het komende jaar actief voor onze drie aansluitingen. De CISO beoordeelt het risico dat we lopen – door het niet voldoen aan dit ene aspect van een van de normen - als laag.

Logius is landelijk verantwoordelijk voor DigiD aansluitingen en Bureau Keteninformatisering Werk en Inkomen (BKWI) en Uitvoeringsinstituut Werknemersverzekeringen (UWV) zijn verantwoordelijk voor Suwinet. Na vaststelling en indienen van de Collegeverklaring en het bijbehorende assurance rapport van de auditor, continueren zij de aansluitingen van de gemeente Hilversum.

Burgemeester en wethouders van Hilversum,  
de gemeentesecretaris,

de burgemeester,

D. Emmer

P.I. Broertjes

# Collegeverklaring informatiebeveiliging DigiD en Suwinet

## Gemeente Hilversum

# Collegeverklaring informatiebeveiliging DigiD en Suwinet

## Gemeente Hilversum

### Doel en achtergrond verklaring

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

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA<sup>(1)</sup> 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 755160

bijlage 2 Suwinet met kenmerk 755160

### Verklaring college

Het college verklaart dat voor DigiD en Suwinet niet aan alle normen wordt voldaan. Wij hebben een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

<sup>(1)</sup> 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 opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
Digid (1) 822008	Nee	Ja
Digid (2) 996571	Nee	Ja
Digid (3) 1003403	Nee	Ja
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Hilversum, [datum]

Burgemeester en wethouders van Hilversum,  
de gemeentesecretaris, de burgemeester,

D. Emmer

P.I. Broertjes

Naam auditfirma:	Noordbeek B.V.
Naam auditor:	Prof.dr.ir. R. Paans RE
Datum ondertekening auditor:	Handtekening of paraaf auditor

# Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Hilversum

Bijlage 2 Gebruik van Suwinet

<b>Gemeentelijk kenmerk bijlage 2 Suwinet:</b>
--

755160
--------

## Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2020 van de gemeente Hilversum. 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 [wel][niet] door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. Hilversum heeft een deel van de Suwinet taken uitbesteed aan de gemeente Gooise Meren. Als gevolg hiervan is een aantal maatregelen belegd bij de gemeente Gooise Meren. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm. De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling (TPM) van Gooise Meren.

### Leverancier 1

Naam serviceorganisatie:	Gemeente Gooise Meren
Referentie/rapportnummer:	BKBO/200817-4/TPM
Afgiftedatum:	18 maart 2021
Naam RE-auditor:	Drs.M.B.H. Ijpelaar RE CEH CISA
Ondertekend door RE-auditor:	Ja

## 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	Nee
Participatiewet (Pw) Sociale recherche Gooi en Vechtstreek	Gemeente Gooise Meren	Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	binnen de gemeente	Nee
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)	binnen de gemeente	Nee
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	binnen de gemeente	Nee

## 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)	samenwerkingsverband: Regio Gooi en Vechtstreek	Nee
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing	Nee
Adresonderzoek door Burgerzaken	binnen de gemeente	Nee

## Naleving BIO-maatregelen

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