

## **Notitie Verantwoordingsstelsel ENSIA**

Versie: 12 december 2018

### **Inleiding**

Doel van deze notitie is het bieden van een eenduidige beschrijving van het verantwoordingsstelsel Eenduidige Normatiek Single Information Audit (ENSIA) voor alle partijen en personen die betrokken zijn bij het ontwikkelen, invoeren en beheren van ENSIA.

### *Achtergrond*

Het project ENSIA (Eenduidige Normatiek Single Information Audit) is in juli 2015 gestart en in juli 2018 afgerond en heeft geresulteerd in een geïmplementeerd verantwoordingsstelsel ENSIA. Het was een gezamenlijk project van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het toenmalige ministerie van Infrastructuur & Milieu (I&M) en de Vereniging van Nederlandse Gemeenten (VNG). Het project had tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Uitgangspunt is dat aangesloten wordt op de gemeentelijke P&C-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan hier ook beter op sturen.

Het project is een resultaat van de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" die in november 2013 tijdens de Buitengewone Algemene Ledenvergadering van De VNG is aangenomen.

In deze resolutie hebben de gemeenten het belang van informatieveiligheid erkend en de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) aangenomen als hét gemeentelijk basisnormenkader voor informatieveiligheid. De gemeenten hebben zich gecommitteerd aan de implementatie van de BIG in de eigen organisatie. Daarnaast informeert een college van B en W de gemeenteraad over informatieveiligheid in het jaarverslag. In de resolutie hebben de gemeenten ook een oproep gedaan aan de rijksoverheid en ketenpartners om de verantwoordingslast over informatieveiligheid te verminderen. Dit laatste vormde de aanleiding voor de start van het project ENSIA.

### **Versie historie**

- Versie 29 juni 2016, vastgesteld in stuurgroep 12 juli 2016.
- Versie 21 november 2016, vastgesteld in de stuurgroep van 24 november 2016. Deze versie is aangepast aan voortschrijdend inzicht in de afgelopen maanden.
- Versie 16 december 2016: aangepast n.a.v. resultaten van de impactanalyse: redactieslag, aanpassing van het tijdpad, verdere uitwerking van bijlage 2 met detailafspraken over 2017 met nadere toelichting van de reikwijdte van de zelfevaluatie informatiebeveiliging, de Collegeverklaring informatiebeveiliging en de IT-audit. Besproken in de stuurgroep op 22 december 2016.
- Versie 16 maart 2017: aangepast n.a.v. herijking tijdpad en reikwijdte Collegeverklaring en IT-audit, herijkte formats Collegeverklaring (bijlage 2) en Assurancerapport (bijlage 4) na afstemming met NOREA, handreiking voor de paragraaf Informatieveiligheid in het jaarverslag (bijlage 5) toegevoegd en diverse aanpassingen op basis van voortschrijdend inzicht. Te bespreken in de stuurgroep op 23 maart.
- Versie 27 maart 2017: vastgestelde versie. Oplegger en vragen aan de stuurgroep verwijderd, procesplaat toegevoegd op pagina 2.
- Versie 29 juni 2017: n.a.v. diverse opmerkingen tekstaanpassingen ter verduidelijking doorgevoerd.

- Versie 23 oktober 2017: nadere duiding van te leveren producten in de tabel met de tijdspaden, aanpassingen in format Collegeverklaring en Assurancerapport met afzonderlijke bijlagen voor DigiD en Suwinet.
- Versie 27 november 2017: verwerken besluitvorming stuurgroep 25 oktober 2017: in bijlage 2 is de afgestemde bijlage Suwinet bij de Collegeverklaring opgenomen; verder op basis van voortschrijdend inzicht: een toelichting op de notitie Voortschrijdend inzicht, in bijlage 1 enkele technische aanpassingen in de mapping van de Suwinet-normen op de BIG en in de tabel met de reikwijdte van de zelfevaluatie.
- Versie 21 december 2017: aanpassingen in format Collegeverklaring en Assurancerapport.
- Versie 18 mei 2018: diverse aanpassingen voor het verantwoordingsjaar 2018: conform eerdere besluitvorming van de stuurgroep toevoegen van AVG en BRO, verwerken aangepaste wettelijke termijnen zelfevaluatie BRP/PUN.
- Versie 5 juli 2018: diverse aanpassingen voor het verantwoordingsjaar 2018. De volgende aanpassingen volgen nog: geactualiseerde procesplaten, geactualiseerde en vereenvoudigde formats Collegeverklaring en Assurancerapport, geactualiseerde toelichting op de paragraaf informatiebeveiliging in het jaarverslag en het verwerken van de besluitvorming van de stuurgroep over 'Waar staat je gemeente'.
- Versie 1 november 2018: diverse aanpassingen voor het verantwoordingsjaar 2018: geactualiseerde procesplaten, geactualiseerde en vereenvoudigde formats Collegeverklaring (inclusief bijlagen) en Assurancerapport, geactualiseerde toelichting op de paragraaf informatiebeveiliging in het jaarverslag en het verwerken van de besluitvorming van de stuurgroep over 'Waar staat je gemeente'. De volgende beschrijvingen volgen nog: escalatieprotocollen, herindelingsprotocol.
- Versie 12 december 2018: aanpassing datum en 'aanpassing' m.b.t. escalatie- en herindelingsprotocollen gewijzigd in 'beschrijvingen'. De volgende beschrijvingen volgen nog: escalatieprotocollen, herindelingsprotocol.

## Het verantwoordingsstelsel ENSIA

De 'ENSIA verantwoording informatiebeveiliging' gaat uit van het principe van Single Information & Single Audit (SISA). Dit betekent eenmalige informatieverstrekking en eenmalige IT-audit.

### De ENSIA werkwijze in het kort

Gemeenten voeren een zelfevaluatie informatiebeveiliging uit onder meer gericht op beveiligingsnormen van de BRP, PUN, BAG, BGT, DigiD en Suwinet. De zelfevaluatie heeft ook betrekking op een aantal aspecten van de Algemene Verordening Gegevensbescherming (AVG) en niet-informatiebeveiligingsaspecten van BRP, PUN, BAG, BGT en BRO. Het college van B&W stelt een Collegeverklaring ENSIA op over een aantal geselecteerde beveiligingsnormen. Een IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. Het college van B&W rapporteert vervolgens aan de gemeenteraad over de informatiebeveiliging. De ENSIA-tooling ondersteunt het uitvoeren van de zelfevaluatie en het beschikbaar stellen van relevante informatie aan de betrokken partijen met een toezichhoudende verantwoordelijkheid. ENSIA is in 2017 met een beperkte scope gestart. ENSIA zal de komende jaren middels een groeppad worden doorontwikkeld. Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in de Regiegroep ENSIA<sup>1</sup> daarover afspraken.



Afbeelding 1: procesplaat verantwoordingsstelsel ENSIA (horizontaal)

<sup>1</sup> Voor 2018 heeft de stuurgroep ENSIA deze afspraken gemaakt.

## Verticaal Proces ENSIA Verantwoording 2018

De vragenlijsten voor de zelfevaluatieperiode zijn te vinden op [ensia.nl](http://ensia.nl)



Afbeelding 2: procesplaat verantwoordingsstelsel ENSIA (verticaal)

### De gemeentelijke producten

- **Paragraaf Informatiebeveiliging in het jaarverslag / separate Rapportage Informatiebeveiliging**

Het college van B en W neemt in het jaarverslag in de paragraaf Bedrijfsvoering een aparte paragraaf op over informatiebeveiliging. Hierin rapporteert het college aan haar toezichthouder (de gemeenteraad) over informatiebeveiliging. Deze werkwijze hebben gemeenten in de eerder genoemde resolutie afgesproken.<sup>2</sup> In de praktijk blijken er dan wat bezwaren in relatie tot de werkzaamheden van de financial auditor in relatie tot het jaarverslag. Als alternatief adviseren we om de gemeenteraad te informeren via een aparte rapportage met daarin een beschrijving van de stand van zaken rond informatiebeveiliging. De Collegeverklaring en het Assurancerapport worden als bijlage bij deze rapportage op basis van geheimhouding aan de gemeenteraad verstrekt. Daarmee wordt verstrengeling met de werkzaamheden van de financial auditor vermeden. Door de rapportage op basis van geheimhouding (in het kader van veiligheid) te verstrekken is er een zeer beperkt risico dat de rapportage in onbevoegde handen terechtkomt. In bijlage 5 is een handreiking opgenomen voor het opstellen van de paragraaf Informatiebeveiliging en de separate rapportage. In dit geval kan in het jaarverslag kort verwezen worden naar deze separaat uitgebrachte rapportage. Een aantal gemeenten kiest nu al voor deze behandeling omdat zij verwacht een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

<sup>2</sup> Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente, BALV 29-10-2013: "Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag".

- **Collegeverklaring ENSIA inzake informatiebeveiliging**  
Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen hebben voldaan aan de voor de ENSIA verantwoording geselecteerde normen en indien aan de orde welke onderdelen daarvan zijn uitgezonderd. Ook wordt melding gemaakt van eventuele verbetermaatregelen die de gemeente gaat treffen. Zie bijlage 2 voor de uitwerking van de Collegeverklaring ENSIA en de bijlagen bij de Collegeverklaring voor DigiD en Suwinet. De Collegeverklaring ENSIA wordt inclusief de bijlagen voor DigiD en Suwinet gezamenlijk met het Assurancerapport separaat van het jaarverslag aan de gemeenteraad aangeboden.
- **Zelfevaluatie informatiebeveiliging**  
Met de ingevulde zelfevaluatievragenlijst geeft het college van B en W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van deze vragenlijst is vastgesteld waar de normen van BRP, PUN, DigiD, Suwinet, BAG en BGT aansluiten op de BIG-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIG-normen. Voor specifieke normen van BRP, PUN, DigiD, Suwinet, BAG, BGT en de AVG zijn aanvullende vragen geformuleerd (als subvraag bij een generieke BIG-vraag of separaat van de BIG-vragen). De paragraaf Informatiebeveiliging / separate Rapportage Informatiebeveiliging en de Collegeverklaring ENSIA zijn onder meer gebaseerd op de zelfevaluatie.
- **Assurancerapport**  
Een bij de NOREA geregistreerde IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. Deze werkzaamheden van de IT-auditor duiden we ook wel aan als de IT-audit. De IT-auditor verklaart in het Assurancerapport dat de Collegeverklaring een getrouw beeld geeft. Getrouw betekent dat de Collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de Collegeverklaring. Zie de uitwerking van het Assurancerapport in bijlage 3. Indien het College van B en W op basis van de IT-audit tot voortschrijdende inzichten komt betreffende de antwoorden van de zelfevaluatie, dan zal het College een notitie opstellen met per vraag een toelichting op het actuele inzicht<sup>3</sup>.

### **Informatieverstrekking met behulp van de ENSIA-tooling**

Via de ENSIA-tooling stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie, de Collegeverklaring ENSIA en het Assurancerapport aan de minister van BZK ten behoeve van het toezicht op de BRP, de PUN, DigiD, de BAG, de BGT en de BRO. Namens de minister van BZK verwerkt Logius de verantwoordingsinformatie over DigiD. Verder bieden gemeenten via ENSIA transparantie aan de beheerder van de centrale omgeving van de GeVS<sup>4</sup> (BKWI) ten behoeve van het jaarlijks opstellen van een totaaloverzicht van de beveiliging van de GeVS. Deze rapportage wordt uitgebracht aan het ketenoverleg GeVS en de minister van SZW. De Inspectie SZW houdt onafhankelijk signalerend toezicht op het functioneren van het stelsel werk en inkomen. Als de inspectie daartoe aanleiding ziet, kan de inspectie onderzoek doen naar de beveiliging van Suwinet bij gemeenten. Om de daarbij door de inspectie gevraagde informatie aan te leveren, kunnen gemeenten putten uit de via de ENSIA-tooling beschikbare verantwoordingsinformatie.

---

<sup>3</sup> De noodzaak van deze notitie is gelegen in het afronden van de zelfevaluatie per 31 december, waarna de antwoorden beschikbaar worden gesteld aan BRP, BAG en BGT en niet meer kunnen worden gewijzigd. Met de notitie Voortschrijdend inzicht is voor alle betrokkenen binnen de gemeente een eenduidige en expliciete beschrijving beschikbaar over verschillen tussen de zelfevaluatie en de Collegeverklaring. De notitie vormt derhalve de brug tussen zelfevaluatie en Collegeverklaring en bevordert daardoor dat alle geconstateerde tekortkomingen in verbeterplannen worden betrokken.

<sup>4</sup> GeVS staat voor Gezamenlijke Elektronische Voorzieningen SUWI, en wordt veelal aangeduid als Suwinet.

## **Samenwerkingsverbanden**

Bij samenwerkingsverbanden blijft het college van B en W als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan het college van B en W om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken (zie nadere informatie in bijlage 4). [Bij DigiD verantwoordt de 'Aansluithouder DigiD' zich via Logius aan de minister van BZK.](#)

## **Algemene Verordening Gegevensbescherming (AVG)**

Met ingang van het verantwoordingsjaar 2018 zijn een aantal van de AVG afgeleide vragen toegevoegd aan de zelfevaluatievragenlijst. Dit ondersteunt gemeenten bij het inregelen van privacy-maatregelen en de horizontale verantwoording hierover. Conform de AVG moeten gemeenten aan een aantal specifieke privacy-vereisten voldoen en moeten gemeenten aantonen dat persoonsgegevens op passende wijze beveiligen door middel van operationele, technische en organisatorische maatregelen. In belangrijke mate zijn die maatregelen direct herleidbaar tot BIG-maatregelen. Alhoewel de AVG-vereisten breder zijn dan de resolutie Informatieveiligheid, ondersteunt het toevoegen ervan aan ENSIA eveneens het bestuurlijk bewustzijn Informatieveiligheid.

## **Verantwoording over gemeentelijke objecten**

Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de jaarlijkse verantwoording over gemeentelijke objecten die onder de BIG vallen. Dit betreft objecten anders dan BRP, PUN, DigiD, Suwinet, BAG en BGT. Hierbij kan een gemeente een groeipad toepassen. Op termijn is denkbaar dat de verantwoordingssystematiek doorgroeit naar een collegeverklaring (in control statement) die zowel de hiervoor genoemde objecten als de overige gemeentelijke objecten omvat.

## **Transparantie en benchmarking via 'Waar staat je gemeente?'**

Via de website [Waarstaatjegemeente.nl](http://Waarstaatjegemeente.nl) kunnen Nederlandse gemeenten aan de hand van thema's op gemeenteniveau zien hoe ze op verschillende gemeentelijke onderwerpen, waaronder Informatieveiligheid, 'presteren'. Gemeenten kunnen hun eigen gegevens vergelijken met andere gemeenten. De informatie is openbaar toegankelijk. Gemeenten kunnen de data uit het dashboard meenemen in de besluitvorming, beleidsvorming, voor agendavorming, verantwoording of voor onderzoek. De ENSIA-tooling ondersteunt gemeenten met het beschikbaar stellen van gegevens over informatiebeveiliging aan 'Waar staat je gemeente'. De ENSIA-tooling voorziet in een specifiek voor 'Waar staat je gemeente' in te vullen vragenlijst en de mogelijkheid om de antwoorden in 'Waar staat je gemeente' in te lezen. Gemeenten bepalen zelf of ze 'Waar staat je gemeente' met informatie over informatieveiligheid vullen.

## **Afspraken over de ENSIA verantwoording en het groeipad**

Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in de Regiegroep ENSIA<sup>5</sup> afspraken over de inhoud van de ENSIA-verantwoording. Het betreft afspraken over te selecteren objecten, normen/vragen en over opzet/bestaan/werking, rapportageperiode, rapportagemoment en de IT-audit. In de eerste jaren zal sprake zijn van een groeipad.

---

<sup>5</sup> Voor 2017 heeft de stuurgroep deze afspraken gemaakt.

Middels het groeipad kan de ENSIA-systematiek met realistische jaarlijkse stappen doorgroeien naar een eindperspectief dat aansluit op de noodzaak en het ambitieniveau van gemeenten om het informatieveiligheidsbeleid zowel bestuurlijk als ambtelijk in de organisatie te borgen.

Uitgangspunt is dat in het eindperspectief de verantwoording over BRP, PUN, BAG, BGT en BRO<sup>6</sup> op aspecten anders dan informatiebeveiliging, op hetzelfde moment wordt afgelegd als de verantwoording over informatiebeveiliging. Daarbij wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken. Afspraken hierover kunnen onderdeel zijn van het groeipad.

### **Afspraken over het jaar 2018**

De stuurgroep ENSIA heeft besloten dat met als peildatum 31 december 2018, verantwoording wordt afgelegd over de opzet en het bestaan van beheersmaatregelen en nog niet over de werking daarvan. Verder heeft de stuurgroep ENSIA besloten dat de zelfevaluatie over 2018 betrekking heeft op BRP, PUN, DigiD, Suwinet, BAG, BGT en BRO en dat het gemeenten vrij staat om overige objecten in de zelfevaluatie te betrekken. Verder is in de stuurgroep afgesproken dat gemeenten er zorg voor dragen dat de noodzakelijke verantwoordingsinformatie via de ENSIA werkwijze wordt aangeleverd en zo invulling geven aan het single information single audit principe.

Over het verantwoordingsjaar 2018 richt de IT-audit zich op de DigiD-normen en een selectie van Suwinet normen. Een beperkt aantal normen zoals het informatiebeveiligingsbeleid en de betrokkenheid van het college van B en W bij informatiebeveiliging, hebben hierbij een generiek karakter. Met deze selectie van normen wordt in 2017 en 2018 ervaring opgedaan met het assuranceproces én is de inspanning om een goede 'guidance' te ontwikkelen relatief beperkt. Op basis van de ervaring opgedaan met de verantwoordingen over 2017 en 2018 wordt de inrichting van de IT-audit over het verantwoordingsjaar 2019 herijkt. Eén en ander is verder uitgewerkt in bijlage 1.

---

<sup>6</sup> De zelfevaluatievragen voor de Basisregistratie Ondergrond hebben geen betrekking op informatiebeveiligingsaspecten.

### Tijdpad ENSIA in 2018 en in het eindperspectief

In onderstaande tabel is weergegeven welke deadlines voor ENSIA en de kwaliteitsmonitor zullen gelden. In de kolom 'eindperspectief' is het uiteindelijk te realiseren beeld geschetst.

Stap	2018	Eindperspectief
1. Afspraken maken over de verantwoording	uiterlijk 1 april 2018	1 april
2. - Invullen van de zelfevaluatie vragenlijst - Beschikbaar stellen van de ruwe datarapportages (ingeleverde antwoorden) inzake de BIG vragen.	1 juli – 31 december 2018	1 juli – 31 december over opzet en bestaan per 31/12 en in de toekomst de werking over het kalenderjaar.
3. - Afsluiten vragenlijst met peildatum 31 december - Beschikbaar stellen van de ruwe datarapportages (ingeleverde antwoorden) inzake de domeinspecifieke vragen voor BAG, BGT en BRO. - Beschikbaar stellen van de ruwe datarapportage (ingeleverde antwoorden) inzake de BIG vragen voor BAG en BGT.	uiterlijk 31 december 2018	uiterlijk 31 december
4. - Opstellen van een Collegeverklaring inclusief bijlagen. - Uitvoeren van een IT-Audit en het daarbij opstellen van een Assurancerapport. - Opstellen van een bestuursrapportage BAG, een bestuursrapportage BGT en een bestuursrapportage BRO.	1 januari – 30 april 2019	1 januari – 30 april
5. Beschikbaar stellen van Collegeverklaring inclusief bijlagen, Assurancerapport en evt. Notitie Voortschrijdend inzicht zelfevaluatie op basis van IT-audit. - Beschikbaar stellen van de ruwe datarapportage (ingeleverde antwoorden) inzake de BIG vragen voor Suwinet. - Beschikbaar stellen van de bestuursrapportages voor BAG, BGT en BRO.	uiterlijk 30 april 2019	Uiterlijk 30 april
6. Vaststellen van de jaarstukken door de gemeenteraad, toesturen van de jaarstukken aan de minister van BZK	uiterlijk 15 juli 2019	uiterlijk 15 juli <sup>7</sup>

Toelichting op de data van het proces in 2018:



- Deze data passen binnen bestaande wettelijke kaders van de stelsels die een onderdeel uitmaken van ENSIA.

Toelichting op de data in het eindperspectief:

1. Uitgangspunt is dat de verantwoording over informatiebeveiliging onderdeel wordt van de jaarlijkse verantwoordingscyclus bij gemeenten. De periode waarover in het jaarverslag verantwoording wordt afgelegd betreft daarbij het kalenderjaar. Voor de opzet en het bestaan van maatregelen is 31 december een logische datum. Het afleggen van verantwoording over de werking van maatregelen betreft het kalenderjaar.
2. Het geschetste tijdpad in de derde kolom is gericht op het eindperspectief ENSIA. Hierbij geldt:
  - a. Waar nodig worden de bestaande wettelijke termijnen in lijn gebracht met het tijdpad in het eindperspectief.<sup>8</sup>
  - b. De verantwoordingssystematiek groeit in de komende jaren stapsgewijs toe naar het eindperspectief, er is sprake van een groeipad. Zo heeft de stuurgroep besloten om het eerste jaar te starten met een verantwoording over opzet en bestaan en de werking op een later moment toe te voegen. Het groeipad kan, gezien de bestaande wettelijke termijnen, ook betrekking hebben op het tijdpad.
3. De Collegeverklaring ENSIA en het Assurancerapport dienen uiterlijk 30 april beschikbaar te worden gesteld middels een upload met de ENSIA-tooling. De datum van 30 april geeft voldoende ruimte voor het opstellen van de Collegeverklaring en het Assurancerapport en ligt vóór de start van de volgende jaarcyclus waarbij per 1 juli de zelfevaluatievragenlijst wordt opengesteld.

---

<sup>7</sup> Wettelijke termijn voor het aanleveren van het jaarverslag en de jaarrekening aan de minister van BZK

<sup>8</sup> In de stuurgroep ENSIA van 24 november 2016 is besloten dat de stuurgroep BZK, I&M en SZW verzoekt in beeld te brengen op welke termijn de wet- en regelgeving met het tijdpad voor het eindperspectief in overeenstemming kan worden gebracht.

## **Bijlage 1 Detail Afspraken over de ENSIA verantwoording 2018**

### **1. Inleiding**

In deze bijlage zijn de voor het verantwoordingsjaar 2018 gemaakte afspraken over de ENSIA-verantwoording nader beschreven. Deze afspraken zijn gemaakt in de stuurgroep van het project ENSIA. Het betreft afspraken over te selecteren objecten, normen/vragen en over opzet en bestaan, rapportageperiode, rapportagemoment en de IT-audit. Na afronding van dit project gaan vertegenwoordigers van gemeenten en betrokken departementen jaarlijks in de Regiegroep ENSIA afspraken maken over de ENSIA-verantwoording.

In de eerste jaren zal sprake zijn van een groeipad. Middels het groeipad kan de ENSIA-systematiek met realistische jaarlijkse stappen doorgroeien naar een eindperspectief dat aansluit op de noodzaak en het ambitieniveau van gemeenten om het informatieveiligheidsbeleid zowel bestuurlijk als ambtelijk in de organisatie te borgen en daarbij te voldoen aan de eisen van BRP, PUN, DigiD, GeVS, BAG, BGT en BRO.

Uitgangspunt is dat in het eindperspectief de verantwoording over BRP, PUN, BAG, BGT en BRO op aspecten anders dan informatiebeveiliging, op hetzelfde moment wordt afgelegd als de verantwoording over informatiebeveiliging. Daarbij wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken. Afspraken hierover kunnen onderdeel zijn van het groeipad.

De wet Basisregistratie Ondergrond (BRO) is per 1 januari 2018 in werking getreden. Gemeenten zijn wettelijk verplicht zich te verantwoorden over de BRO. De verantwoording van de BRO richt zich op niet-informatiebeveiligingsaspecten. Voor gemeenten is het afleggen van verantwoording over de BRO via ENSIA efficiënter in vergelijking met het alternatief waarbij gemeenten separaat van ENSIA verantwoording afleggen. De toezichtparagraaf is niet helder in de wet meegenomen en wordt nog in afstemming met de achterban aangepast. Streven is dit per 1 januari 2019 of per 1 juli 2019 te hebben aangepast. BZK/DGBRW heeft met de achterban afgesproken dat 2018 voor de toepassing van de ENSIA-systematiek een proefjaar is. De bronhouders worden uitgenodigd de verantwoording over de BRO op vrijwillige basis via ENSIA in te dienen. De tijdslijnen zijn overeenkomstig aan de BAG en BGT. Voordeel van het proefjaar is dat de bronhouders zo de gelegenheid krijgen hun basisregistratie goed op orde te krijgen.

### **2. Normering**

Voor het verantwoordingsjaar 2018 zijn in de volgende documenten de van kracht zijnde normen geformuleerd voor de objecten waarover verantwoording wordt afgelegd:

- BIG: Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten, versie 1.02, juni 2016
- GeVS: Specifiek Suwinet normenkader Afnemers, versie 1.01, 3-4-2017
- Digid: Het DigiD normenkader 2017
- BAG: Wet en regelgeving BAG nieuwe vorm is vastgesteld, de ingangsdatum is waarschijnlijk 1-7-2018
- BGT: Wet en regelgeving BGT is vastgesteld en in werking getreden
- BRP: Wet en regelgeving BRP
- PUN: Wet en regelgeving PUN
- BRO: Wet en regelgeving BRO

### 3. Reikwijdte zelfevaluatie informatiebeveiliging

Met de ingevulde zelfevaluatievragenlijst geeft het college van B en W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van de zelfevaluatievragenlijst is vastgesteld waar de normen van BRP, PUN, DigiD, Suwinet, BAG en BGT aansluiten op de BIG-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIG-normen. Voor specifieke normen van BRP, PUN, DigiD, Suwinet, BAG en BGT zijn aanvullende vragen geformuleerd. De DigiD-norm kent een andere scope dan de BIG en ook een ander object van onderzoek. DigiD richt zich op de webpagina waarop zich een DigiD-snelkoppeling bevindt met een geheel eigen set van normen. Om die reden zijn de DigiD-vragen losgeweekt van de ENSIA vragenlijst. Matching met BIG-normen is daarom niet van toepassing.

Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de verantwoording in de paragraaf Informatiebeveiliging over de overige gemeentelijke objecten die onder de BIG vallen (informatie over de beveiliging in brede zin).

### 4. Reikwijdte Collegeverklaring ENSIA inzake informatiebeveiliging en IT-audit

De Collegeverklaring ENSIA en de IT-audit hebben betrekking op opzet en bestaan van de beheersingsmaatregelen per 31 december 2018 voor de gearceerde normen (controls) en objecten in de onderstaande tabellen.

#### Het DigiD normkader 2.0

Als eerste is er de DigiD-norm met een andere scope dan de BIG en ook met een ander object van onderzoek. DigiD richt zich op de webpagina waarop zich een DigiD-snelkoppeling bevindt met een geheel eigen set van normen. Daarnaast moet een gemeente de DigiD-audit laten uitvoeren per aansluiting. Daarnaast is een deel van de DigiD-norm soms van toepassing op de gemeente en soms op een leverancier en soms op beiden. Om die reden zijn de DigiD-vragen losgeweekt van de ENSIA vragenlijst. Matching met BIG-normen is daarom niet meer van toepassing.

Nr	Beschrijving van de beveiligingsrichtlijn
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 is 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

Nr	Beschrijving van de beveiligingsrichtlijn
	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 hardeningsrichtlijn 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.

In de zelfevaluatie is het vernieuwde DigiD normenkader zoals dat geldt vanaf 2017 verwerkt. Vanuit de zelfevaluatie wordt aan Logius in een voor hen verwerkbaar format per DigiD aansluiting informatie door de gemeente verstrekt. De in samenwerking met NOREA uitgewerkte guidance DigiD is uitgangspunt voor het uitvoeren van werkzaamheden door de gemeenten en de auditors.

### Het Suwinet normenkader voor afnemers 1.01

Als tweede is er de Suwinet-norm. Deze richt zich net zoals de BIG (generiek) op de bedrijfsvoering, met als focus de sociale keten binnen de gemeente, omdat de Suwinet-norm maar eenmalig hoeft te worden uitgevraagd en omdat ze gematchd zijn op de BIG controls, zijn de Suwinet-vragen in de ENSIA-vragenlijst verweven met de BIG vragen.

BIG	Suwinet
<b>Generieke controls met specifieke objectgerichte aanvullingen</b>	
5.1.1 Beleidsdocument voor informatiebeveiliging	x (B01)
5.1.2 Beoordeling van het informatiebeleid	X (C01)
6.1.1 Betrokkenheid van het college van B en W bij informatiebeveiliging	X (B01, C01)
6.1.2 Coördineren van informatiebeveiliging	x (B04)
6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging	x (B05)
<b>Objectgerichte controls</b>	
8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	x
10.1.3 Functiescheiding	x (B05)
10.10.1 Aanmaken auditlogbestanden	x (C05)
10.10.2 Controle van het systeemgebruik	x (C06, C07)
11.2.1 Registratie van gebruikers	x (U02, U03)
11.2.4 Beoordeling van toegangsrechten van gebruikers	x (U03, C04)
11.5.2 Gebruikersidentificatie en -authenticatie	x (U03)
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen	x (U11)

Bij de Suwinet-normen zijn tussen haakjes verwijzingen naar het Suwinet specifieke normenkader afnemers opgenomen. Dit normenkader omvat nadere toelichting op de Suwinet-normen.

Betreffende Suwinet gelden voor gemeenten alle van kracht zijnde aan de beveiliging van Suwinet gestelde normen van de BIG en het specifieke Suwinet normenkader afnemers.

De Inspectie SZW en de AP hebben in de afgelopen jaren ten behoeve van hun onderzoek de volgende onderwerpen geselecteerd:

1. Het informatiebeveiligingsbeleid en het beveiligingsplan Suwinet;
2. De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur en de rol van de security officer daarbij;
3. Het logische toegangsbeheer;
4. De aansluiting van niet-Suwi partijen en de toepassing van Suwinet-inlezen daarbij.

De 7 normen die de inspectie voor haar onderzoeken heeft geselecteerd, vormen een uitwerking van de eerste 3 onderwerpen. Voor 2017 en daarop volgende jaren is van belang dat het bereikte niveau van beveiliging wordt vastgehouden. De Suwinet beveiligingsnormen voor afnemers zijn het afgelopen jaar herijkt en daarbij is het Specifiek Suwinet normenkader Afnemers opgesteld. In de tabel hiervoor zijn de verwijzingen naar dit normenkader opgenomen.

Verder is van belang dat invulling wordt gegeven aan de toezeggingen die UWV aan de AP heeft gedaan betreffende de controle op het gebruik van via Suwinet-Inlezen geleverde gegevens. UWV heeft aan de AP toegezegd medio 2016 van SNG, Amsterdam, Den Haag en Rotterdam een jaarrapportage te ontvangen over de uitgevoerde controles op het gebruik van Suwinet-Inlezen. Met ingang van het verantwoordingsjaar 2017 wordt deze rapportage via ENSIA ingevuld. Conform het Suwinet specifieke normenkader afnemers betekent dit dat de eisen betreffende logging over het gegevensgebruik op medewerkersniveau, het opstellen van gebruiksrapportages en het op basis daarvan controleren van het gebruik op alle gemeentelijke applicaties van toepassing zijn waarin via Suwinet-Inlezen of DKD-Inlezen ingelezen gegevens worden verwerkt.

<b>BIG</b>	<b>Inleesapplicatie<sup>9</sup></b>
10.10.1 Aanmaken auditlogbestanden	x (C05)
10.10.2 Controle van het systeemgebruik	x (C06)

Verder is, gezien het belang ervan, een norm toegevoegd voor het versleutelen van netwerkverbindingen.

---

<sup>9</sup> De inleesapplicatie is de gemeentelijke bedrijfsapplicatie waarin gegevens via Suwinet- of DKD-Inlezen worden ingelezen.

## **Bijlage 2 Format Collegeverklaring ENSIA en bijlagen DigiD en Suwinet**

Deze bijlage bevat het format voor de Collegeverklaring Ensia en de bijlagen DigiD en Suwinet. Het format voor de Collegeverklaring is uitgewerkt in drie verschijningsvormen:

- Format Collegeverklaring voor gebruik van DigiD en Suwinet
- Format Collegeverklaring voor gebruik van uitsluitend DigiD
- Format Collegeverklaring voor gebruik van uitsluitend Suwinet

### **Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging DigiD en Suwinet**

#### ***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), Paspoortuitvoeringsregeling Nederland (PUN), 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).

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 <naam gemeente> 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 dienstverlener(s) vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met 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) 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 bijlagen voor DigiD (bijlage 1 DigiD met kenmerk <...>) en Suwinet (bijlage 2 Suwinet met 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 <...>) en voor Suwinet (bijlage 2 Suwinet met 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 2018 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet>. <Bij uitzonderingen: Het college verklaart dat voor <DigiD> <en/of> <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 <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
Suwinet voor SUWI-taken	<Ja, Neen, n.v.t.>	<Ja, Neen, n.v.t.>
Suwinet voor niet-SUWI-taken	<Ja, Neen, n.v.t.>	<Ja, Neen, n.v.t.>

[Plaats, datum]

[College van B en W gemeente]

## **Collegeverklaring ENSIA 2018 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), Paspoortuitvoeringsregeling Nederland (PUN), 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).

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 het jaar 2018 voor gemeente <naam gemeente> betreft dit DigiD. De verklaring omvat het op 31 december 2018 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 2018.

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 <...>) 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 <...>) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) die toezien op de veiligheid van DigiD worden via bij deze collegeverklaring behorende afzonderlijke bijlage voor DigiD (bijlage 1 DigiD met 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 2018 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 opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>
DigiD <aansluitnummer>	<Ja, Neen>	<Ja, Neen>

[Plaats, datum]

[College van B en W gemeente]

## **Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging Suwinet**

### ***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), Paspoortuitvoeringsregeling Nederland (PUN), 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).

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 het jaar 2018 voor gemeente <naam gemeente> betreft dit Suwinet. De verklaring omvat het op 31 december 2018 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 2018.

<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) 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 <...>) zijn de eventuele afwijkingen van de normen opgenomen. De gemeenteraad en het ministerie van Sociale Zaken en Werkgelegenheid (SZW) die toezien op de veiligheid van Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlage voor Suwinet (bijlage 1 Suwinet met 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 2018 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, Neen, n.v.t.>	<Ja, Neen>
Suwinet voor niet-SUWI-taken	<Ja, Neen, n.v.t. >	<Ja, Neen>

[Plaats, datum]

[College van B en W gemeente]

## Bijlage DigiD (bijlage 1 bij Collegeverklaring Ensia)

### Bijlage 1 Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting <Aansluitnaam> en <Aansluitnummer>

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 <aansluitnummer> en <aansluitnaam>.

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:	
Referentie/rapportnummer:	
Afgiftedatum:	
Naam RE-auditor:	
Ondertekend door RE-auditor:	

#### Leverancier 2

Naam serviceorganisatie:	
Referentie/rapportnummer:	
Afgiftedatum:	
Naam RE-auditor:	
Ondertekend door RE-auditor:	

De uitkomsten uit de zelfevaluatie zijn getoetst door een RE-gecertificeerde IT-auditor. Deze heeft tevens getoetst of de zelfevaluatie en de TPM(s)/assurancerapportage(s) van onze serviceorganisaties het gehele normenkader afdekken. De uitkomsten van de auditor zijn opgenomen in het assurancerapport met kenmerk <kenmerk>.

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).

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

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

DigiD Norm	
<b>B.05</b>	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.
<b>U/TV.01</b>	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.
<b>U/WA.02</b>	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
<b>U/WA.03</b>	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
<b>U/WA.04</b>	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
<b>U/WA.05</b>	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
<b>U/PW.02</b>	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
<b>U/PW.03</b>	De webserver is ingericht volgens een configuratie-baseline.
<b>U/PW.05</b>	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
<b>U/PW.07</b>	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.
<b>U/NW.03</b>	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.
<b>U/NW.04</b>	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.
<b>U/NW.05</b>	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
<b>U/NW.06</b>	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.
<b>C.03</b>	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
<b>C.04</b>	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
<b>C.06</b>	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
<b>C.07</b>	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.
<b>C.08</b>	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
<b>C.09</b>	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

## **Bijlage Suwinet (bijlage 2 bij Collegeverklaring Ensia)**

### **Bijlage 2 Gebruik van Suwinet**

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2018 van de gemeente <naam gemeente>. 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/niet> in samenwerkingsverbanden gebruikt. <Indien 'wel': 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/of> <samenwerkingsverband(en): ...>
...	

#### **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)	N.v.t. <of> <binnen de gemeente>
Loonbeslag door Gemeentelijke Belastingdeurwaarders	N.v.t. <of> <binnen de gemeente> <en/of> <samenwerkingsverband(en): ...>
Bijhouden BRP door Burgerzaken	N.v.t. <of> <binnen de gemeente> <en/of> <samenwerkingsverband(en): ...>

## Normnaleving

<indien geen afwijkingen van de normen:

Zoals in de Collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2018 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 2018 in opzet en bestaan aan alle geselecteerde normen:

SUWI-taak	Organisatie	BIG-nummer en SUWI-nummer	Applicatie
		...	<Suwinet-Inkijk> of <Suwinet-Inlezen / DKD-Inlezen in combinatie 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:

Niet-SUWI-taak	Organisatie	BIG-nummer en SUWI-nummer	Applicatie
...		...	<Suwinet-Inkijk> of <Suwinet-Inlezen / DKD-Inlezen in combinatie met naam inleesapplicatie>

>



### **Bijlage 3 Format Assurance-rapport**

Deze bijlage bevat het format voor het Assurance rapport. Het format voor het Assurance rapport is uitgewerkt in drie verschijningsvormen:

- Format Assurancerapport voor gebruik van DigiD en Suwinet
- Format Assurancerapport voor gebruik van uitsluitend DigiD
- Format Assurancerapport voor gebruik van uitsluitend Suwinet

## **Assurance-rapport van de onafhankelijke IT-auditor**

### **(Bij gebruik DigiD en Suwinet)**

Aan: <Opdrachtgever>

#### ***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 <naam gemeente> onderzocht.

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

De collegeverklaring 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.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake DigiD en/of Suwinet voldaan>.

<Alleen bij uitzonderingen >

#### ***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 (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 is 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 assurancerapport 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 assurancerapport 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 <naam gemeente>***

Het college van burgemeester en wethouders van gemeente <naam gemeente> 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).

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT Auditor RE)

# Assurance-rapport van de onafhankelijke IT-auditor

## (Bij gebruik van uitsluitend DigiD)

Aan: <Opdrachtgever>

### **Ons oordeel**

Wij hebben de bijgevoegde collegeverklaring ENSIA 2018 inzake informatiebeveiliging van DigiD (hierna: collegeverklaring), inclusief de bijlage 1 DigiD waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlage 1 DigiD waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>, in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de normen voor DigiD. Wij benadrukken dat het specifieke normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake DigiD voldaan>.

<Alleen bij uitzonderingen >

### **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 (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 is 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 assurancerapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor het departementen dat toeziet op de veiligheid van DigiD. Doel van de collegeverklaring is om de gemeenteraad en de het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) die toezien op de veiligheid van DigiD te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD. Ons assurancerapport is derhalve uitsluitend bestemd voor de

gemeenteraad en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) die toezien op de veiligheid van DigiD en dient niet te worden verspreid aan of te worden gebruikt door anderen.

### **Verantwoordelijkheden van het college van gemeente <naam gemeente>**

Het college van burgemeester en wethouders van gemeente <naam gemeente> 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, 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 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).

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT Auditor RE)

# Assurance-rapport van de onafhankelijke IT-auditor

## (Bij gebruik van uitsluitend Suwinet)

Aan: <Opdrachtgever>

### **Ons oordeel**

Wij hebben de bijgevoegde collegeverklaring ENSIA 2018 inzake informatiebeveiliging van Suwinet (hierna: collegeverklaring), inclusief de bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>, in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor Suwinet<sup>1</sup>. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake Suwinet voldaan>.

<Alleen bij uitzonderingen >

### **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 (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 is 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 assurancerapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor het ministerie van Sociale Zaken en Werkgelegenheid (SZW) die toezien op de veiligheid van Suwinet. Doel van de collegeverklaring is om de gemeenteraad en het ministerie van Sociale Zaken en Werkgelegenheid (SZW) die toezien op de veiligheid van Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor Suwinet. Ons assurancerapport is

derhalve uitsluitend bestemd voor de gemeenteraad en het departement dat toeziet op de veiligheid van Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

***Verantwoordelijkheden van het college van gemeente <naam gemeente>***

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

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT Auditor RE)

## **Bijlage 4. De invulling van verantwoordelijkheden in samenwerkingsverbanden**

### **Wat is de aanleiding?**

Eind 2013 is in de BALV de resolutie 'Informatieveiligheid randvoorwaarde voor een professionele gemeente aangenomen. In de resolutie hebben gemeenten afgesproken de BIG (Baseline Informatie veiligheid Gemeenten) te hanteren als gezamenlijk normenkader. Gemeenten zullen zich in het jaarverslag gaan verantwoorden over informatieveiligheid aan de eigen toezichthouder (horizontale verantwoording). Gemeenten hebben gevraagd aan Min BZK om de bestaande verantwoordingen op het vlak van informatieveiligheid te stroomlijnen. In de huidige situatie hebben gemeenten te maken met minimaal vijf verantwoordingen op het vlak informatieveiligheid. Deze verschillen qua diepgang, timing en gevraagde assurance, terwijl zij steeds hetzelfde thema belichten.

Min BZK heeft in samenwerking met betrokken departementen en VNG het project ENSIA gestart en (Eenduidige Normatiek Single Information Audit) heeft tot doel om het horizontale verantwoordingsproces rond informatieveiligheid bij gemeenten in te richten op basis van een zelfevaluatie (met als basis de BIG). De betrokken departementen vervolgens krijgen vanuit dit proces de voor hen relevante informatie. De zelfevaluatie leidt tot een gemeentelijke collegeverklaring informatiebeveiliging die door een IT auditor wordt onderzocht. De departementen 'steunen' als het ware op de resultaten van dit verantwoordingsproces.

Kern van het geheel is de eigen verantwoordelijkheid van het gemeentebestuur voor de inrichting van deze informatieveiligheid. Die verantwoordelijkheid is eenduidig zolang de diverse relevante processen zich binnen de gemeentelijke organisatie afspelen. De praktijk is echter dat gemeenten voor een aantal taken de samenwerking opzoekt. En natuurlijk geldt ook in die situatie dat uiteindelijk de gemeentelijk bestuurder verantwoordelijkheid kent voor de processen die in die samenwerking worden afgehandeld. De vraag ligt voor hoe aan die verantwoordelijkheid invulling te geven en hoe dat vervolgens moet landen in de ENSIA verantwoording.

### **De WGR en informatieveiligheid**

(Inter) gemeentelijke samenwerkingen zijn geënt op Wet Gemeenschappelijke regelingen (WGR). De wet beschrijft een aantal mogelijke juridische mogelijkheden om samenwerkingen vorm te geven. En beschrijft daarbij op de hoofdlijn de wijze waarop per constructie verantwoording moet/kan worden afgelegd. De wet gaat bij geen enkele beschreven samenwerking in op het thema informatieveiligheid en laat de invulling daarvan over aan de samenwerkende partijen die daarover al dan niet afspraken (wensen te) maken. De wijze waarop die verantwoording vorm krijgt, is ook afhankelijk van de specifieke juridische constructie van het samenwerkingsverband. Een openbaar lichaam (als zelfstandig rechtspersoon) heeft daartoe andere mogelijkheden dan bijvoorbeeld een BV of stichting. Een centrumgemeenteconstructie kent ook weer zijn eigen beperkingen in het afleggen van verantwoording. De wet geeft verder weinig kapstokken om aan die verantwoordelijkheid invulling te geven.

### **Handreiking Informatieveiligheid en intergemeentelijke samenwerking**

In deze handreiking is al het volgende opgenomen:

- *Een portefeuillehouder binnen het college van B en W is verantwoordelijk voor de (prioritering van) beveiliging van informatie binnen de bedrijfs(werk)processen. Deze verantwoordelijkheid wijzigt niet op het moment dat de gemeente besluit om een bepaalde dienst of taak uit te besteden of samen met andere gemeenten (intergemeentelijk) uit te voeren. De gemeente blijft als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan de portefeuillehouder om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken. In de handreiking informatieveiligheid en intergemeentelijke samenwerking worden aanzetten gegeven hoe die verantwoording invulling te geven. [https://vng.nl/files/vng/publicaties/2015/20150731\\_informatieveiligheid-en-intergemeentelijke.pdf](https://vng.nl/files/vng/publicaties/2015/20150731_informatieveiligheid-en-intergemeentelijke.pdf). In dit rapport wordt ingegaan op publiekrechtelijke samenwerkingsvormen (openbaar lichaam, centrumgemeente), privaatrechtelijke samenwerkingsvormen en ketens. In het rapport wordt het volgende al behandeld: afspraken over de BIG, aanvullende afspraken tov de BIG, afleggen van verantwoording en audits. Er is*

*dus al het een en ander verwoord als het gaat over de gemeentelijke verantwoordelijkheid bij samenwerking.*

Om invulling te geven aan de specifieke verantwoordelijkheid rond (intergemeentelijke) informatieveiligheid suggereren de bij ENSIA betrokken auditors de volgende aanvulling op deze handreiking:

- *Bij publiekrechtelijke en privaatrechtelijke samenwerkingsvormen is het uitgangspunt dat de gemeente voor de bij de samenwerkingsvorm ondergebrachte activiteiten verantwoordelijk blijft voor het aantoonbaar voldoen aan de BIG (c.q. de beveiligingsafspraken). De verantwoording van de gemeente over het voldoen aan de BIG omvat derhalve ook de activiteiten van de samenwerkingsvormen voor de gemeente. De gemeente laat zich door de samenwerkingsvorm informeren over het voldoen van de ondergebrachte activiteiten aan de BIG (c.q. beveiligingsafspraken) en de gemeente stelt de juistheid en volledigheid van de ontvangen verantwoording van de samenwerkingsvorm vast. De gemeente kan dit zelf doen of de samenwerkingsvorm vragen hiervoor een auditor in te schakelen.*

Kern van deze aanvulling is dat de gemeenten binnen het samenwerkingsverband afspreken hoe zij zich wil laten informeren over de gerealiseerde informatieveiligheid en op welke wijze deze informatie landt in de zelfevaluatie. De ontwikkelde tool biedt daarvoor beperkte functionaliteit. Als met het samenwerkingsverband een vorm van gebruik van TPM's is ingericht, kunnen gemeenten daar (desgewenst) uiteraard op steunen.

- *Bij ketens heeft iedere deelnemer een zelfstandige verantwoordelijkheid. Iedere deelnemer van de keten legt verantwoording af over het voldoen aan de BIG en laat deze verantwoording **desgewenst** van zekerheid voorzien door een auditor. De ketenpartners/ ketenregisseur stelt vast dat er niets tussen de wal en het schip valt en dat de verantwoordingen de gehele keten afdekken.*

Kern van deze aanvulling is dat aanvullend op de reguliere verantwoording van een ketenpartner wordt bewaakt dat alle in de keten betrokken partijen voldoen aan de gemaakte afspraken. Concreet betekent dit dat binnen de keten in ieder geval de afspraak moet bestaan dat voldaan wordt aan BIG (of vergelijkbare baseline).

Binnen ENSIA is voorsnog de afspraak dat minimaal BRP, PUN, BAG, BGT SUWI en DigiD in de zelfevaluatie betrokken zijn. De evaluatie betreft het voldoen aan de volle breedte van de BIG op dit vlak. De audit in 2017 spitst zich toe op een beperkt aantal normen.

De verantwoordelijkheid van gemeenten betreft uiteraard alle vormen van samenwerking. Voorstelbaar is dat de focus voor gemeenten allereerst ligt bij die samenwerkingsverbanden die binnen de scope van ENSIA vallen.

## **Bijlage 5. Handreiking Paragraaf Informatiebeveiliging in het jaarverslag van gemeenten / separate Rapportage Informatiebeveiliging**

Met de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' van november 2013 hebben gemeenten afgesproken om de informatiebeveiliging op orde te krijgen en te houden. In deze resolutie is onder meer afgesproken dat de gemeente in het jaarverslag een aparte paragraaf opneemt over informatiebeveiliging. Met deze paragraaf verantwoordt een college van B en W zich aan de gemeenteraad over informatiebeveiliging in brede zin ('horizontale verantwoording'). Dit betreft onder meer gemeentelijke doelstellingen en afspraken over informatiebeveiliging. Daaronder zijn de afspraken die gemaakt zijn voor de ENSIA verantwoording informatiebeveiliging ('verticale verantwoording'). Over (het nakomen van) de ENSIA afspraken doet de gemeente ook een specifieke uitspraak in de 'Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet'<sup>10</sup>. De IT-auditor doet een uitspraak over de juistheid en volledigheid van de Collegeverklaring ENSIA.

De (sub-)paragraaf Informatiebeveiliging wordt opgenomen in de paragraaf Bedrijfsvoering van het jaarverslag (als onderdeel van de jaarstukken, naast de jaarrekening). Om gemeenten te faciliteren de paragraaf Informatiebeveiliging op eenduidige wijze op te stellen, volgt hierna een format met de ingrediënten daarvan.

Gemeenten kunnen ervoor kiezen om een separate Rapportage Informatiebeveiliging aan de Raad te verstrekken. Deze rapportage omvat zowel de informatie over informatiebeveiliging in brede zin als de Collegeverklaring ENSIA. Een aantal gemeenten kiest nu al voor deze behandeling omdat zij verwacht een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. In dat geval kan in het jaarverslag kort verwezen worden naar deze separaat uitgebrachte rapportage. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

---

<sup>10</sup> Over het verantwoordingsjaar 2018 richt de IT-audit zich op de DigiD-normen en een selectie van Suwinet-normen (zie bijlage 1). Hierbij is een groeipad voorzien.

## Paragraaf Informatiebeveiliging in het jaarverslag óf separate Rapportage Informatiebeveiliging

<p><b>IB beleid, doelstellingen en afspraken</b></p> <p>Bestuurlijke beschrijving van de belangrijkste gemeentelijke doelstellingen van het informatiebeveiligingsbeleid, waaronder onder meer: "zorgvuldig omgaan met informatie", "betrouwbare en continue dienstverlening", "voldoen aan wet- en regelgeving (privacy)" en "beheersen van risico's" (Governance, Risk en Compliance).</p> <p>Beschrijf hier ook specifieke doelstellingen zoals:</p> <ul style="list-style-type: none"><li>• de ambities om te voldoen aan de BIG als basisnormenkader voor de IB maatregelen.</li><li>• het nakomen van de afspraken over de 'ENSIA verantwoording'.</li></ul>
<p><b>Algemeen beeld en resultaten afgelopen periode</b></p> <p>Beschrijving van de (belangrijkste) activiteiten / resultaten die in het afgelopen jaar hebben bijgedragen aan het behalen van de doelstellingen. "In 2018 heeft de gemeente .."</p>
<p><b>"Disclaimer"</b></p> <p>Wellicht verstandig om iets op te nemen over de illusie van 100% veiligheid.</p>
<p><b>Beheersmaatregelen IB</b></p> <p>Geef een overzicht van de belangrijkste maatregelen die bijdragen aan het realiseren van de IB doelstellingen:</p> <ul style="list-style-type: none"><li>• Organisatie en TBV's, awareness</li><li>• Organisatorische en technische maatregelen</li><li>• Information Security Management System (ISMS) / PDCA</li></ul>
<p><b>Realisatie doelstelling IB Beleid (effectiviteit beheersmaatregelen en risico's)</b></p> <p>Geef aan in welke mate de afgesproken doelstellingen voor 2018 zijn gerealiseerd (in hoeverre beheersmaatregelen effectief zijn in relatie tot realiseren van het IB Beleid en welke (*specifieke) doelstellingen en risico's nog aandacht behoeven (en waarvoor nog maatregelen getroffen moeten worden). Let wel, hier wel omzichtig zijn met wat je naar buiten brengt.</p> <p>Geef aan hoe dit is getoetst. Onder meer met de ('brede') Zelfevaluatie Informatiebeveiliging en eventueel andere instrumenten (ISMS). Geef ook aan wat de reikwijdte is van de Zelfevaluatie Informatiebeveiliging.</p>
<p><b>Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet</b></p> <p>Bij een paragraaf Informatiebeveiliging in het Jaarverslag wordt hier een verwijzing naar een separate Collegeverklaring ENSIA opgenomen. Bij een separate Rapportage Informatiebeveiliging wordt hier de Collegeverklaring ENSIA exclusief de bijlagen opgenomen.</p>
<p><b>Incidenten</b></p> <p>Rapportage (privacy) incidenten / datalekken en de afhandeling daarvan.</p>
<p><b>Meerjaren perspectief</b></p> <p>Beschrijving van aandachtspunten, doelstellingen en resultaatafspraken (planning) volgende periode.</p> <p>De stappen en het tijdspad voor het implementeren van de BIG. Beschrijf per stap de reikwijdte (systemen en ICT-beheerprocessen<sup>11</sup>).</p>

### *Toelichting:*

Bij een paragraaf Informatiebeveiliging in het jaarverslag worden de afzonderlijke bijlagen 1 DigiD en 2 Suwinet bij de Collegeverklaring met het jaarverslag aan de gemeenteraad verstrekt.

---

<sup>11</sup> Bijvoorbeeld Logische Toegangsbeveiliging (LTB).

Bij een separate Rapportage Informatiebeveiliging worden de afzonderlijke bijlagen 1 DigiD en 2 Suwinet bij de Collegeverklaring als onderdelen van de Rapportage Informatiebeveiliging aan de gemeenteraad verstrekt.