

Onderwerp Vaststellen Collegeverklaring ENSIA 2018	
Nummer	2019/341565
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hotting, E.
Telefoonnummer	023-5115061
Email	ehotting@haarlem.nl
Kernboodschap	Het college van burgemeester en wethouders van de gemeente Haarlem legt met de Collegeverklaring ENSIA verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet voor het jaar 2018 op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek. Naast de Collegeverklaring worden met dit besluit ook de zelfevaluaties over de basisregistraties BAG, BGT en BRO vastgesteld. De Collegeverklaring over DigiD en Suwinet en de zelfevaluaties BAG, BGT en BRO zullen aan de respectievelijke toezichhouders worden toegestuurd.
Behandelveorstel voor commissie	Het college stuurt het besluit ter kennisname aan de commissie Bestuur.
Relevante eerdere besluiten	Vaststellen Collegeverklaring ENSIA 2017 (2018/222795)
Besluit College d.d. 14 mei 2019	Het college van burgemeester en wethouders Besluit: 1. De Collegeverklaring ENSIA over het jaar 2018 vast te stellen 2. De vastgestelde Collegeverklaring voor te leggen aan de IT Auditor voor het verkrijgen van een assurancerapport 3. De zelfevaluaties m.b.t. de basisregistraties BAG, BGT en BRO over het jaar 2018 vast te stellen de secretaris, de burgemeester,

1. Inleiding

Voor de tweede keer verantwoorden wij ons over de kwaliteit van de informatieveiligheid van diverse informatiesystemen met behulp van de Eenduidige Normatiek Single Information Audit (ENSIA).

Alle gemeenten rapporteren nu op één vooraf afgesproken moment in het jaar over de status van de informatieveiligheid. Voor het jaar 2018 geldt net als in 2017 dat de verantwoording Suwinet (aan Ministerie van SZW) en DigiD (aan Logius) wordt verantwoord door middel van een Collegeverklaring.

Met de voorliggende ENSIA-collegeverklaring geeft het college aan in hoeverre de beheersingsmaatregelen voldoen aan de normen die gelden voor DigiD en Suwinet en op welke onderdelen verbeteringen noodzakelijk zijn. De collegeverklaring is opgesteld aan de hand van de uitkomsten van de zelfevaluaties die door de lijnverantwoordelijken zijn uitgevoerd, onder coördinatie van de CISO. Een gecertificeerde IT-auditor controleert de collegeverklaring. Na vaststelling van de collegeverklaring zal de auditor zijn hij naar verwachting een assurance rapport afgeven. De IT-auditor verklaart hierin dat de collegeverklaring een getrouw beeld geeft. De collegeverklaring wordt gezamenlijk met het assurance rapport aangeboden aan de gemeenteraad.

Daarnaast zijn dit jaar nieuwe ENSIA onderdelen (BRP, PUN, BAG en BGT) toegevoegd. Deze vallen buiten de scope van de Collegeverklaring (waarover door een auditor een assuranceverklaring wordt afgegeven), maar ze worden wel los vastgesteld door het college.

Uit de zelfevaluatie blijkt dat de Gemeente Haarlem op peildatum 31 december 2018 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet, met uitzondering van de in het verbeterplan geadresseerde normen. Er zijn inmiddels maatregelen getroffen om de afwijkingen van normen inzake DigiD te verhelpen. Hiermee voldoen de beheersingsmaatregelen inmiddels aan de normen, ofwel is de te treffen maatregel op korte termijn gereed. Hiermee is gemeente Haarlem 'in control' voor wat betreft de DigiD normen. De te treffen maatregelen inzake Suwinet vergen grotere aanpassingen en de verbetermaatregelen hebben in 2018 te weinig prioriteit gekregen. Daarnaast is het, net als rond DigiD, in het algemeen noodzakelijk dat de verantwoording over de informatieveiligheid een zaak wordt van de betrokken lijnmanagers en deze verantwoordelijkheid ook zo gevoeld wordt. Dit jaar krijgt dit punt de nodige aandacht onder regie van de Concerncontroller, FG en CISO. De planning is om de afwijkingen inzake Suwinet dit jaar te verhelpen.

Het verbeterplan beschrijft welke opvolging (correctieve maatregelen) er door Gemeente Haarlem worden getroffen en welke verbetertermijn wordt gehanteerd. De externe toezichthouder kan oordelen dat bepaalde verbetermaatregelen sneller getroffen dienen te worden dan gepland.



Daarbij is het ook belangrijk te realiseren dat de toezichthouder algemeen geldende principes hanteert waaraan volgens de toezichthouder voldaan moet zijn bij de bescherming van gegevens. Die principes ondersteunen de oordeelsvorming. Normen kunnen het vertrekpunt zijn van die oordeelsvorming, maar niet het eindpunt. Te vaak is gebleken dat het voldoen aan normen een losse koppeling onderhoudt met daadwerkelijke veiligheid.

Naast het adresseren van de afwijkingen van de normen, zal er middels het jaarverslag aan de raad over het totaalbeeld en de status van informatieveiligheid van de gemeente verantwoording afgelegd. Door in het vervolg de ENSIA verantwoording te betrekken in het jaarverslag krijgt het gemeentebestuur meer zicht op de informatieveiligheid in de juiste context en is ze beter in staat om keuzes te maken in het informatieveiligheidsbeleid van de gemeente. Hiermee wordt aangesloten bij de gemeentelijke P&C-cyclus en wordt het leervermogen van de organisatie vergroot.

2. Besluitpunten college

Het college van burgemeester en wethouders

Besluit:

1. De Collegeverklaring ENSIA over het jaar 2018 vast te stellen
2. De vastgestelde Collegeverklaring voor te leggen aan de IT Auditor voor het verkrijgen van een assurancerapport
3. De zelfevaluaties m.b.t. de basisregistraties BAG, BGT en BRO over het jaar 2018 vast te stellen

3. Beoogd resultaat

Met dit Collegebesluit wordt het jaarlijkse ENSIA verantwoordingsproces een stap verder gebracht. Beoogd wordt te voldoen aan de verantwoordingsplicht inzake DigiD, Suwinet, BAG, BGT en BRO middels de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek. Daarbij wordt het oordeel uitgesproken dat de collegeverklaring een getrouw beeld geeft van gemeentelijke interne beheersingsmaatregelen inzake de informatiebeveiligingsnormen DigiD en Suwinet op 31 december 2018.

4. Argumenten

1. Juridische verplichting

Het vaststellen van de collegeverklaring ENSIA is een vereiste om te voldoen aan de verantwoordingsplicht voor Suwinet en DigiD. De vastgestelde collegeverklaring dient samen met het

assurancerapport van de IT-auditor voor 1 mei 2019 te worden aangeleverd aan de respectievelijke toezichthouders (BKWI namens Ministerie van SZW en Logius namens Ministerie van BZK). Het vaststellen van de overige zelfevaluaties is een vereiste om te voldoen aan de verantwoordingsplicht voor BAG, BGT en BRO binnen ENSIA. De vastgestelde zelfevaluaties worden aangeleverd aan de toezichthouder. Voor alle aanleveringen richting de toezichthouders is uitstel gevraagd in verband met de niet gehaalde deadline van 1 mei.

2.Financiën

Dit besluit heeft géén financiële consequenties. Wel kan het zo zijn dat de toezichthouders naar aanleiding van de rapportage mogelijk instructies geeft voor het versneld oplossen van tekortkomingen. Het sneller moeten oplossen van deze tekortkomingen dan de voorgestelde planning in het verbeterplan, heeft mogelijke financiële gevolgen van enkele tienduizenden euro's.

5. Risico's en kanttekeningen

In de bijlagen van de verklaring is per DigiD aansluiting en per Suwinet voorziening aangegeven op welke specifieke punten niet voldaan wordt aan het geldende normenkader. Naast de risico's die mogelijk voortvloeien uit het niet voldoen aan het normenkader, bestaat er bij het niet-oplossen van de verbeterpunten nog het risico dat de landelijke toezichthouder de gemeente niet meer gebruik laat maken van deze voorzieningen. Dit heeft verregaande gevolgen voor de dienstverlening van de gemeente aan burgers en bedrijven.

6. Uitvoering

Na besluitvorming wordt de collegeverklaring, inclusief alle bijlagen, ter kennisgeving aan de raad aangeboden.

7. Bijlagen

- 1.Collegeverklaring ENSIA 2018
 - 1.1 Bijlage Digid
 - 1.2 Bijlage Suwinet
 - 1.3 Verbeterplan ENSIA 2018
- 2. Verantwoordingsrapportage BAG 2018
- 3. Verantwoordingsrapportage BGT 2018
- 4. Verantwoordingsrapportage BRO 2018