



Onderwerp Vaststellen Collegeverklaring ENSIA 2017	
Nummer	2018/222795
Portefeuillehouder	Spijk, J.K.N. van
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hotting, C.E.
Telefoonnummer	0235115061
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 2017 op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek. Deze verklaring luidt: Het college verklaart dat bij gemeente Haarlem op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet, met uitzondering van in de bijlagen gespecificeerde normen. De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.
Behandelveorstel voor commissie	Het college stuurt het besluit ter informatie aan de commissie Bestuur.
Relevante eerdere besluiten	n.v.t.
Besluit College d.d. 8 mei 2018	Het college van burgemeester en wethouders Besluit: 1. De Collegeverklaring ENSIA over het jaar 2017 vast te stellen; de secretaris, de burgemeester,

1. Inleiding

Informatieveiligheid en privacy hebben een belangrijke plaats op de gemeentelijke agenda, met gevolgen voor elke afdeling. Het adequaat inrichten van verantwoordingsprocessen is daarbij essentieel. Zo blijft informatieveiligheid en privacy van burgers gewaarborgd. Over 2017 verantwoorden wij ons over de kwaliteit van de informatieveiligheid van diverse informatiesystemen met een nieuwe systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA).

ENSIA is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). Of we voldoen aan deze Baseline is getoetst door middel van een zelfevaluatie. Alle gemeenten rapporteren nu op één vooraf afgesproken moment in het jaar over de status van de informatieveiligheid. Voor het jaar 2017 geldt dat de verantwoording Suwinet (aan Ministerie van SZW) en DigiD (aan Logius) wordt verantwoord door middel van een Collegeverklaring. In de toekomst zullen de overige ENSIA onderdelen (BRP, PUN, BAG en BGT) toegevoegd worden aan de jaarlijkse collegeverklaring. Deze Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie. De IT-auditor toetst (na vaststelling) de collegeverklaring en verklaart in het assurancerapport of de collegeverklaring een getrouw beeld geeft. Het gaat daarbij om opzet en bestaan van de maatregelen per 31 december 2017. Er wordt geen oordeel gegeven over de werking van de maatregelen gedurende een periode. Over het totaalbeeld en de status van informatieveiligheid van de gemeente verantwoordt de organisatie zich via het jaarverslag (met een separate rapportage informatieveiligheid) aan de raad.

2. Besluitpunten college

Het college van burgemeester en wethouders

Besluit:

1. De Collegeverklaring ENSIA over het jaar 2017 vast te stellen;

3. Beoogd resultaat

Voldoen aan de verantwoordingsplicht inzake DigiD en Suwinet middels de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek, waarbij het oordeel wordt uitgesproken dat de collegeverklaring een getrouw beeld geeft van gemeentelijke interne beheersingsmaatregelen inzake de informatiebeveiligingsnormen DigiD en Suwinet op 31 december 2017.

4. Argumenten

Het vaststellen van de collegeverklaring ENSIA is een vereiste om te voldoen aan de verantwoordingsplicht voor Suwinet en DigiD en een voorwaarde om als gemeente gebruik te kunnen blijven maken van deze voorzieningen.

De gemeente dient ieder jaar een Collegeverklaring ENSIA af te geven, waarvan voorliggende de eerste is. De Collegeverklaring gaat over een beperkt deel van de gehele ENSIA. Het betreft in dit eerste jaar alleen een verklaring over opzet en bestaan van de normen voor Suwinet en DigiD. Het ligt in de lijn der verwachting dat de scope volgend jaar wordt uitgebreid. Met de voorbereiding van de verantwoording over 2018 zal de organisatie binnenkort van start gaan.

Dit besluit heeft géén financiële consequenties.

5. Risico's en kanttekeningen

Alle gemeenten verantwoorden op dit moment over de kwaliteit van de informatieveiligheid van diverse informatiesystemen met een nieuwe systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). De nieuwe werkwijze heeft voordelen. Omdat alle gemeenten nu op dezelfde manier verantwoorden kan bijvoorbeeld meer eenvoudig relevante kennis worden uitgewisseld en kunnen toezichthouders beter uit de voeten met de documenten die gemeenten produceren.

Tegelijk is het ook wennen voor zowel de gemeenten, die in een vaste planning en systematiek worden gedwongen, als voor de toezichthouders die hebben gepoogd zo goed mogelijk de voor hen relevante vragen in een gezamenlijk format te voegen. Op basis van deze eerste verantwoording zullen de nodige evaluaties worden uitgevoerd en verbeteringen worden doorgevoerd, zowel in het proces binnen onze organisatie als bij het opstellen van de ENSIA vragenlijsten.

Een belofte van de ENSIA methodiek is dat deze de totale hoeveelheid werk rond audits fors zou reduceren. Dit is in de praktijk niet het geval gebleken voor deze eerste ronde. Hoewel er een uniformering van werkwijze richting de zelfevaluatie heeft plaatsgevonden, is tegelijkertijd de scope fors uitgebreid. De gehele ENSIA zelfevaluatie betreft honderden vragen waarmee verantwoording wordt afgelegd over de Baseline Informatieveiligheid Gemeenten, normen geldend voor verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

De ENSIA zelfevaluaties zijn door een projectgroep uitgevoerd in 2017, met het zwaartepunt in kwartaal drie en vier. Alle vragenlijsten zijn ingediend via ensia.nl voor de gestelde deadline van 31 december 2017.

De deadline van 1 mei voor het indienen van de documenten richting de toezichthouders is niet gehaald door een planningsfout. Het is mogelijk dat hierover een brief van de toezichthouders aan de gemeenteraad volgt. Zo spoedig mogelijk na vaststelling worden de gevraagde documenten alsnog aan de toezichthouders gestuurd waardoor naar verwachting eventuele escalaties worden voorkomen.

De Collegeverklaring en de bijlagen die daarbij ingediend moeten worden hebben een grotendeels voorgeschreven format. Gelet op de doelgroep, namelijk de toezichthouders in de verticale verantwoordingslijn, betreft het documenten van technische aard met daarin exact

de informatie die nodig is voor beoordeling van de zelfevaluaties. Dit brengt met zich mee dat de documenten minder goed leesbaar zijn, en bovendien eenvoudig kunnen leiden tot een foutieve interpretatie. In de bijlagen is daarom op elk van de punten waarop nog niet aan de normen wordt voldaan een korte toelichting opgenomen. Het is daarbij relevant te weten dat elk van de normen pas “voldoet” wanneer we op alle aspecten ervan tevreden zijn, en dat het de situatie in 2017 betrof.

De bijlagen vermelden op welke punten verbetering noodzakelijk is om volledig compliant te worden. Op hoofdlijnen kan worden gesteld dat om volledig compliant te worden, meer inzet nodig is op borging en verantwoording. Een aantal bevindingen laat zien dat een veilige praktijk wordt gehanteerd maar dat niet kan worden aangetoond op welke manier men is gekomen tot die veilige praktijk. Dit leerpunt wordt meegenomen in de door te voeren verbeteringen.

6. Uitvoering

Na besluitvorming wordt de collegeverklaring inclusief de bijlagen ter informatie aan de commissie Bestuur aangeboden. Daarnaast zal de IT auditor over de Collegeverklaring inclusief bijlagen een assurancerapport opstellen. Vervolgens wordt de Collegeverklaring inclusief de bijlagen en de assuranceverklaring toegezonden aan de respectievelijke toezichthouders.

7. Bijlagen

1. Collegeverklaring ENSIA 2017, reg.nr 2018/222822
2. Bijlage afwijkingen DigiD, reg.nr. 2018/222836
3. Bijlage afwijkingen Suwinet, reg.nr. 2018/222840