Collegebesluit

Collegevergadering: 20 april 2021

Zaaknummer	:	808821
Afdeling	:	Informatisering
Portefeuillehouder	:	A.C. Nienhuis
Openbaarheid	:	Actief openbaar

ONDERWERP
Vaststellen zelfevaluatie informatieveiligheid ENSIA 2020 en collegeverklaringen aan de Raad

SAMENVATTING
Jaarlijks legt het college verantwoording af over de informatieveiligheid aan de raad, ministeries en andere instanties conform ENSIA (Eenduidige Normatiek Single Information Audit). Dit betreft de informatieveiligheid gebaseerd op het normenkader van de Baseline Informatiebeveiliging Overheid (BIO) over het jaar 2020. Voor het afleggen van de verantwoording stelt het college de collegeverklaringen over DigiD en Suwinet conform het ENSIA format vast. De vastgestelde verklaringen worden bij het jaarverslag ter verantwoording over de informatieveiligheid aan de raad voorgelegd. Uit de verantwoording blijkt dat er nog verbeterpunten zijn; deze zijn uitgewerkt in de managementrapportage. Voor de basisregistraties zijn aparte verklaringen opgenomen conform de ENSIA formats.

JURIDISCH EN BESLUITKADER
Het normenkader van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO) en de zelfevaluatie over informatieveiligheid, de Eenduidige Normatiek Single Information Audit (ENSIA) zijn vastgesteld door het ministerie van BZK en zijn verplicht om uit te voeren.
Op basis van de BIO is het strategisch Informatieveiligheidsbeleid in 2020 vastgesteld door het college.

BESLUIT B&W

1. De Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet inclusief de 2 bijlagen vast te stellen;
2. De verantwoordingsrapportage 2020 over de BAG vast te stellen;
3. De verantwoordingsrapportage 2020 over de BGT vast te stellen;
4. De verantwoordingsrapportage 2020 over de BRO vast te stellen;
5. De Managementrapportage informatieveiligheid ENSIA 2020 vast te stellen;
6. Alle stukken behorende bij de beslispunten 1 tot en met 4 ter kennisname aan de raad te sturen bij het jaarverslag samen met de financiële verantwoording.

Collegebesluit

Collegevergadering: 20 april 2021

AANLEIDING
Conform de ENSIA legt het college jaarlijks verantwoording af over de status van de Informatieveiligheid aan de raad, aan ministeries en externe partijen. Voor 1 mei 2021 moet de vastgestelde collegeverklaring aan het ministerie van Binnenlandse Zaken en Koninkrijkrelaties overhandigd worden. Bij het jaarverslag en de jaarrekening wordt de raad hierover geïnformeerd. De zelfevaluatie wordt uitgevoerd op basis van de BIO. Dit normenkader bevat alle onderdelen om de informatiebeveiliging goed in te kunnen richten. Naast de algemene informatiebeveiliging kijkt de ENSIA specifiek naar de in gebruik zijnde DigiD aansluitingen, het gebruik van SUWI inkijk, en de inhoudelijke en procedurele kwaliteit van de 3 basisregistraties waar de gemeente bronhouder is.

MOTIVERING
De gemeente wil voldoen aan het gevraagde niveau voor informatieveiligheid zodat burgers en bedrijven erop kunnen vertrouwen dat gegevens die wij vastleggen veilig zijn. Daarnaast dient de dienstverlening aan burgers en bedrijven altijd beschikbaar en juist te zijn gezien vanuit de perspectieven van informatieveiligheid. Om dit te bereiken worden maatregelen vastgesteld, uitgevoerd, gecheckt en indien nodig aangepast volgens de Plan-Do-Check-Act cyclus. Hierbij hoort naast de evaluatie over de afgelopen periode, ook het afleggen van verantwoording aan raad, ministeries en andere partijen.

Doel van dit collegebesluit is het vaststellen van de zelf-evaluaties zodat deze daarna gebruikt kunnen worden voor de verantwoording aan raad en andere partijen. Hieronder volgt per beslispunt een korte toelichting over de zelf-evaluatie van 2020.

Collegeverklaring zelf-evaluatie ENSIA 2020 over DigiD en Suwinet
Voor DigiD en inzien van Suwinet worden een beperkt aantal maatregelen uit de BIO door het ministerie van Sociale Zaken en door Logius (beheerdienst van de DigiD) als verplichte maatregelen gesteld. DigiD wordt gebruikt bij digitale producten van burgerzaken, voor parkeervergunningen en voor een aantal producten bij GBKZ. Inzien van Suwinet wordt gebruikt bij het samenwerkingsverband IASZ voor onder andere de participatiewet en bij burgerzaken voor adresonderzoek.
Voor de DigiD aansluitingen voor parkeervergunningen en voor GBKZ wordt aan een paar maatregelen niet voldaan.

- DigiD voor parkeervergunningen

  De gemeente voldoet aan alle 6 de maatregelen waar de gemeente voor verantwoordelijk is. De oplossing voor parkeervergunningen is een zogeheten SAAS-oplossing waarbij de leverancier de applicatie via internet aanbiedt en het gehele technische beheer doet. Hierdoor moet de leverancier aan 19 normen voldoen. Aan één technische norm is niet voldaan.
- DigiD voor Burgerzaken

  De gemeente voldoet aan alle 6 de maatregelen waar de gemeente voor verantwoordelijk is.

Voor Suwinet is bij beide aansluitingen op alle punten voldaan aan de maatregelen.

Zelf-evaluatie 2020 over de BAG
Voor de Basisregistratie Adressen en Gebouwen (BAG) heeft het ministerie de kwaliteit bepaald op het niveau ‘gelegitimeerde werkelijkheid’. Dit houdt in dat alle verleende vergunningen moeten terugkomen in de registratie, daarbij moet de gemeente maatregelen nemen om ervoor te zorgen dat de registratie zo nauw mogelijk aansluit op de feitelijke werkelijkheid.
De gemeente Heemstede heeft met de vragenlijst vanuit de ENSIA-Portaal 205 punten gescoord, op een totaalscore van 205 punten. Dit komt neer op een percentage van 100%. De conclusie van deze zelfevaluatie is dat de kwaliteit van de BAG-registratie hoog is, met een score van 100% ligt het ruim in lijn met de vereisten van het ministerie. Een correcte uitvoer van de wet BAG is geborgd en de tijdigheid, volledigheid en juistheid van de gegevens in de registratie is goed.

Zelf-evaluatie 2020 over de BGT
De Basisregistratie Grootschalige Topografie (BGT) is een gedetailleerde (in vaktaal: grootschalige) digitale kaart van heel Nederland. Daarin worden alle objecten als gebouwen, wegen, water, spoorlijnen en groen op een eenduidige manier vastgelegd.
De resultaten van de zelfcontrole laten een kleine verbetering zien ten opzichte van het jaar 2019. In 2019 werd er 140 punten gescoord van de 150 (93%). In 2020 zijn er 150 punten gescoord op een totaal van 150 (100%). 2020 is het eerste jaar dat de gemeente een totaalscore van 100% weet te behalen. Een correcte uitvoer van de wet BGT is geborgd en de tijdigheid, volledigheid en juistheid van de gegevens in de registratie is goed.

Zelf-evaluatie 2020 over de BRO
De Basisregistratie Ondergrond (BRO) bevat gegevens over geologische en bodemkundige opbouw van de Nederlandse ondergrond. In de komende jaren wordt de BRO stapsgewijs voltooid. Per stap bevat de BRO steeds meer gegevens over de diepe en ondiepe ondergrond. Deze worden geordend op basis van zogeheten ‘registratieobjecten’. In totaal gaat het om ca. 26 registratieobjecten. De inhoud is voor een deel vastgesteld en voor een deel nog bespreekbaar.
De resultaten van de zelfcontrole laten een kleine verbetering zien ten opzichte van het jaar 2019. In 2019 zijn er 110 punten gescoord op een totaal van 120 (91,7%). In 2020 zijn er 120 punten gescoord op een totaal van 120 (100%). 2020 is het eerste jaar dat de gemeente een totaalscore van 100% weet te behalen

Managementrapportage informatieveiligheid ENSIA 2020
De managementrapportage is vastgesteld op basis van het invullen van de zelfaudit in de ENSIA omgeving. Daarnaast is een fysieke inspectie van de gebouwen en werkomgeving gehouden en zijn bevindingen van de medewerkers die een rol hebben in de beveiliging verwerkt. Onderstaand de uitkomst uit de zelfevaluatie.

Gemiddelde score voldoen aan maatregelen BIO in 2020 is 60%
Dit is in harde cijfers een achteruitgang ten opzicht van 2019, daar voldeden we gemiddeld voor 70% aan de maatregelen. Verklaring van deze achteruitgang zit in de volgende 3 zaken:

In de BIO zijn 47 nieuwe maatregelen opgenomen.
In 2020 voldeden we nog steeds aan alle normen waar we ook in 2019 aan voldeden. Daarnaast zijn er bestaande maatregelen vanuit de BIG aangescherpt. Hierdoor is het gemiddelde percentage van voldoen gezakt.
Outsourcing ICT zorgt voor een scheef beeld
In 2020 is de outsourcing van de ICT aan OGD gerealiseerd. Hiermee zijn ongeveer 20% van de normen nu een verantwoordelijkheid voor OGD. Omdat we in 2020 nog in de eindfase en afronding van het project zaten, was het nog niet mogelijk om deze normen bij OGD goed te toetsen. Volgens het contract moet de omgeving voldoen aan de BIO normen maar bij een zelfaudit moet dat wel vastgesteld worden. Doordat het niet vastgesteld is, is de score negatief. We verwachten dat bij de zelfaudit medio 2021 deze cijfers weer goed zijn.
Invoering BIO in 2020 voor een deel naar achteren geschoven
Door de extra werkdruk door de coronamaatregelen was er onvoldoende capaciteit om dit project goed op te pakken.
We zijn wel in control blijkt uit de GAP analyse
Uit de GAP analyse blijkt dat we voor het grootste gedeelte,70%, wel in control zijn. Zoals hierboven al genoemd is OGD als onze outsourcepartij voor 20% van de maatregelen verantwoordelijk. Contractueel gezien moeten zij voldoen maar zekerheid hebben we niet, dat verklaart voor een belangrijk deel waarom we nog niet volledig in control zijn. Dit is wel een actiepunt waar we in 2021 verandering in willen brengen aangezien bij veel technische maatregelen wel directe bedreigingen kunnen liggen.

Advies voor een actieplan informatiebeveiliging 2021 opgenomen in de managementrapportage.
Dit advies is voortgekomen uit de GAP analyse en een risicoanalyse. Hierin zijn 19 actiepunten opgenomen, in een aantal actiepunten zijn missende maatregelen gecombineerd die met elkaar samenhangen.

FINANCIËN
Voor het uitvoeren van de verbeteringen uit de managementrapportage zijn geen extra financiële middelen nodig. Indien extra middelen nodig zijn is in het verleden al rekening gehouden in de begroting met kosten. De meeste verbeteringen betreffen organisatorische en procedurele aanpassingen. Dit kan worden opgepakt binnen de bestaande werkzaamheden.

PLANNING/UITVOERING
Deze verantwoording wordt bij het jaarverslag en de jaarrekening aan de raad voorgelegd. Na vaststelling door het college moeten de rapportages over de BAG, de BRO, de BGT, DigiD en Suwinet voor 1 mei 2021aan de diverse ministeries worden gestuurd. De rapportage over DigiD moet ook naar Logius worden gestuurd.

PARTICIPATIE EN COMMUNICATIE
Participatie is niet van toepassing op dit onderwerp.
De communicatie naar de inwoners en bedrijven vindt plaats door het publiceren van het collegebesluit op de website met de bijbehorende openbare stukken.

DUURZAAMHEID
Niet van Toepassing

BIJLAGEN

1. De Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet;
2. Bijlage 1 DigiD bij De Collegeverklaring ENSIA 2020;
3. Bijlage 2 Suwinet bij De Collegeverklaring ENSIA 2020;
4. De verantwoordingsrapportage 2020 over de BAG;
5. De verantwoordingsrapportage 2020 over de BGT;
6. De verantwoordingsrapportage 2020 over de BRO;
7. Managementrapportage Informatieveiligheid ENSIA 2020 (Niet Openbaar).