



Collegeverklaring ENSIA 2020 inzake informatiebeveiliging Adviesnota DigiD, Suwinet, BAG, BGT en BRO

Inleiding

In november 2013 hebben de Nederlandse gemeenten de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" aangenomen. Hieruit is het project ENSIA (Eenduidige Normatiek Single Information Audit) voortgekomen. De zogenoemde Collegeverklaring ENSIA over een aantal geselecteerde beveiligingsnormen is een jaarlijks terugkerend rapportagemiddel voor zowel de horizontale als verticale verantwoording over informatieveiligheid. Een IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op.

Dit dossier betreft de collegeverklaring en bijlagen ENSIA 2020 inzake de informatiebeveiliging van DigiD, Suwinet, Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en Basisregistratie Ondergrond (BRO).

- ☐ Wettelijke taak
- ☐ Kerntaak gekoppeld aan het werkprogramma van het college
- ☒ Onvermijdelijk
Gemaakte afspraak

Doelstelling

Kennis nemen en vaststellen van de Collegeverklaring ENSIA 2020 en alle bijlagen. Hierbij het ondertekenen en dateren van de Collegeverklaring. Dit alles met het oog op het verkrijgen van een assurance rapport van een externe IT-auditor, zodat de Gemeente Eindhoven aan haar verantwoordingsplicht kan voldoen.

Voorstel

1. Kennis nemen en vaststellen van de Collegeverklaring ENSIA 2020 en bijlagen;
2. Ondertekenen van de Collegeverklaring ENSIA 2020;
3. Door CISO gemeente Eindhoven verticale verantwoording laten uitvoeren en toestemming geven om de documenten te uploaden in de ENSIA tool.



Argumenten

Uitvoering geven aan afspraak

Het project ENSIA (Eenduidige Normatiek Single Information Audit) is een gezamenlijk project van het ministerie van Binnenlandse Zaken, gemeenten, het ministerie van SZW, het ministerie van IenW en de VNG. Het project heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). 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 basishorizont voor informatieveiligheid. Deze baseline is in 2020 opgevolgd door de Baseline Informatieveiligheid Overheid (BIO). De gemeenten hebben zich gecommitteerd aan de implementatie van de BIO in de eigen organisatie. Daarnaast informeert een college van B&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.

De ENSIA werkwijze schrijft het voor

Gemeenten voeren een zelfevaluatie informatiebeveiliging uit onder meer gericht op beveiligingsnormen van de BRP (Basisregistratie Personen), Reisdocumenten, BAG, BGT, BRO, DigiD en Suwinet. Het college van B&W rapporteert aan de gemeenteraad in een paragraaf in het jaarverslag over de informatiebeveiliging. Deze paragraaf bevat naast informatie over de informatiebeveiliging in brede zin een verwijzing naar de zogenoemde Collegeverklaring ENSIA over een aantal geselecteerde beveiligingsnormen. Een IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. De ENSIA-tooling ondersteunt het uitvoeren van de zelfevaluatie en het beschikbaar stellen van relevante informatie aan de betrokken partijen met een toezichthoudende verantwoordelijkheid.

Collegeverklaring ENSIA inzake informatiebeveiliging is verplicht

Met deze verklaring geeft het college van B&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 hiervoor de uitwerking van de Collegeverklaring ENSIA en de bijlagen bij de Collegeverklaring voor DigiD en Suwinet. De Collegeverklaring ENSIA wordt samen met het Assurance rapport DigiD en Suwinet separaat van het jaarverslag aan de gemeenteraad aangeboden.

Alle gebruikte formats zijn landelijk vastgesteld en verplicht te gebruiken.



N.B. de verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten heeft al eerder in 2021 plaats gevonden omdat voor deze verantwoording een eerdere datum gold.

Assurance rapport DigiD en Suwinet is gekoppeld aan geaccordeerde Collegeverklaring

Een bij de NOREA geregistreerde IT-auditor controleert de Collegeverklaring en stelt een Assurance rapport op. De IT-auditor verklaart in het Assurance rapport 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. De auditor geeft deze verklaring af nadat het college dit dossier heeft vastgesteld.

Over het verantwoordingsjaar 2020 richt de IT-audit zich op de DigiD-normen en een selectie van Suwinet normen. Met deze selectie van normen wordt ervaring opgedaan met het assurance proces én is de inspanning om een goede 'guidance' te ontwikkelen relatief beperkt.

Suwinet op orde, twee van de vier DigiD-aansluitingen geheel, twee grotendeels

Het college verklaart dat bij gemeente Eindhoven op 31 december 2020 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake Suwinet en twee van de vier DigiD-aansluitingen.

Het college verklaart dat voor de resterende twee DigiD-aansluitingen op 31 december 2020 grotendeels aan de normen werd voldaan maar aan enkele normen niet. Naast één organisatorische norm over contract vorming (die bij onszelf ligt), zijn de oorzaken technisch van aard en liggen geheel bij de software leveranciers. Hiervoor zijn door de betrokken sectoren risicoanalyses uitgevoerd met als doel te bepalen in welke mate de continuïteit van de bedrijfsvoering bij die DigiD-aansluitingen gevaar loopt. De conclusie is dat het bedrijfsmatig risico minimaal is. De software leveranciers hebben een technische risicoanalyse uitgevoerd en concludeerden ook dat het technisch risico minimaal is. Dit is door hen gecommuniceerd met de gemeente Eindhoven. Daarbij werd aangegeven dat voor het risico afdoende tegenmaatregelen zijn genomen. De betrokken sectoren zijn op de hoogte van het risico en hebben dit geaccepteerd. De continuïteit van de bedrijfsvoering in deze wordt gemonitord door de sectoren.

De monitoring van de normen waaraan niet wordt voldaan, is opgenomen in een Verbeterplan dat deel uitmaakt van dit dossier. Tevens is er een toelichting op de collegeverklaring in het dossier opgenomen waarin wordt ingegaan op de inhoud en voortgang van het oplossen van de normen waaraan niet wordt voldaan. In reguliere overleggen met de software leveranciers wordt het oplossen van het niet voldoen aan de normen operationeel door de gemeente gemonitord. De verwachting is dat in Q3 2021 aan alle normen wordt voldaan. Met de genomen maatregelen zijn de risico's ingeperkt. Dat ze kunnen optreden is natuurlijk nooit helemaal uitgesloten.

Alles in ogenschouw nemend is er geen reden om niet in te stemmen met de collegeverklaring en de daarbij bijbehorende bijlagen.



BAG (Basisregistratie Adressen en Gebouwen) grotendeels op orde

Afgelopen jaar is veel geïnvesteerd in de BAG, in samenhang met de BGT en de WOZ. De resultaten hiervan vertalen zich in een veel beter ENSIA-score dan afgelopen jaar. De investeringen zijn voor een groot deel structureel, zodat de achterstanden die zijn weggewerkt niet opnieuw zullen ontstaan.

Op de gebieden borging proces, volledigheid en juistheid voldoen we volledig aan de eisen. Op het gebied van actualiteit scoren we nog onvoldoende.

De oorzaken hiervan zijn in beeld en er zijn beheersmaatregelen op genomen. De capaciteit is sinds begin 2020 op orde, de aansturing en daarmee bewustwording op het belang van tijdigheid is aangescherpt en afspraken met andere afdelingen zijn verder verhelderd.

Een incidentele oorzaak, de vernieuwing van de ICT, waardoor soms de productie enkele dagen stil lag, zal zich naar alle waarschijnlijkheid niet meer voordoen. De BAG-ICT is voor de komende jaren op orde.

Het komende jaar zal Eindhoven zich richten om de zaken die we op orde hebben gebracht, op orde te houden en steeds verder te verbeteren. We richten ons bij de verbeteringen vooral op de afstemming met BGT en de WOZ, waarbij we verder komen door samenwerking en dus ook bestandvergelijking tussen de registraties. Zo wordt de jaarlijkse mutatiedetectieronde samen met de BGT en WOZ verwerkt. Verder zal ook de administratieve koppeling tussen enerzijds de BAG en anderzijds de WOZ dit jaar op orde moeten worden gebracht. Zo wordt in Eindhoven ingezet op de ontwikkeling in lijn met de komst van de samenhangende objectenregistratie (de SOR).

Voor wat betreft de BAG kan worden gemeld dat we in control zijn ten aanzien van de benodigde fte's en de genomen maatregelen.

Daarentegen hebben we voor de WOZ nog een hoog risico met een hoge impact op het onvoldoende kunnen innen van belastingopbrengsten. In eerste instantie wordt er voor gekozen om de oplossingen te zoeken binnen een separaat traject. Dat betekent dat wij dit proces actief blijven volgen, want als de maatregelen onvoldoende resultaat geven dan is dit negatief van invloed op een volgende ENSIA audit.

BGT (Basisregistratie Grootchalige Topografie) opnieuw volledig op orde

De BGT is een belangrijk onderdeel van het stelsel van Basisregistraties. In enkele jaren tijd is de registratie uitgegroeid tot de meest betrouwbare digitale kaart van heel Nederland. De gemeente Eindhoven speelt een voortrekkersrol bij de totstandkoming en inbedding van deze registratie door voorzitterschap van het landelijk Bronhoudersoverleg en actieve participatie in het doorontwikkelingstraject van de geo-standaarden. De inrichting van de processen rond de BGT is geborgd bij afdeling RU/GDK (Geo-informatie, Data en Kwaliteit).

De gemeente voldoet volledig aan de gestelde wettelijke kwaliteitseisen voor de BGT en de in ENSIA getoetste criteria. Op alle indicatoren wordt de maximale score gehaald. De ingezette verbeteringen uit eerdere jaren worden gecontinueerd. Deze betreffen het nog beter beschrijven van de processen (wat voortdurende aandacht heeft), en het uitvoeren van een jaarlijkse mutatiedetectieronde, nadrukkelijk in samenhang met (en afgestemd op de werkprocessen van) de BAG. Deze is voor het eerst uitgevoerd in 2020 en zal in 2021 opnieuw worden uitgevoerd.



BRO (Basisregistratie Ondergrond) in ontwikkeling o.b.v. implementatieplan

De Basisregistratie Ondergrond (BRO) wordt stapsgewijs opgebouwd. Voor de gemeente Eindhoven betekent het dat vanaf 1 januari 2018 alle grondwatermonitoringsputten ("peilbuizen") en sonderingen in de BRO geregistreerd moeten worden. Dat is nog niet het geval. In 2020 is gestart met het wegwerken van de achterstand. De grondwatermonitoringsputten zijn nu geregistreerd, op enkele uitzonderingen na.

Vanaf 1 oktober 2020 is een BRO-coördinator binnen de gemeente Eindhoven aangesteld. Deze heeft een implementatieplan gemaakt waarin beschreven is hoe en wanneer:

- De achterstand in wettelijk verplichte registraties wordt weggewerkt;
- De afspraken over het actueel houden van de BRO worden geborgd;
- De voorbereiding op de volgende uitbreiding van de BRO gebeurt.

De inschatting is dat uiterlijk medio 2021 de activiteiten uit dit implementatieplan zijn gerealiseerd. Vanaf dat moment zal de BRO actueel zijn en zijn de afspraken die nodig zijn om de BRO actueel te houden gemaakt gecommuniceerd.

Kanttelingen

Niet van toepassing

Personele consequenties

Niet van toepassing

Kosten

Niet van toepassing

Communicatie

Na instemming en ondertekening zal verantwoording plaatsvinden via de voorgeschreven ENSIA tool. Na ontvangst van het assurance rapport van de auditor vindt de verantwoording richting de raad kan plaats via een raadsinformatiebrief.

Planning en uitvoering

De (verticale) verantwoording dient te geschieden voor 01 mei 2021.

Evaluatie

Niet van toepassing


Chief Information Officer (CIO)

Paraaf: 