

Rapportage Informatiebeveiliging Deurne 2018

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeente om hun processen uit te voeren. Gemeenten beschikken over een schat aan (zeer) vertrouwelijke informatie over zowel burgers als bedrijven en daarnaast zijn zij verantwoordelijk voor een betrouwbare en continue dienstverlening. Het is daarom belangrijk gemeenten op passende wijze hun informatie beveiligen.

Het begrip 'informatiebeveiliging' heeft betrekking op beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid van gegevens. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Gemeenten dienen bij hun informatiebeveiliging te voldoen aan wet- en regelgeving, zoals bijvoorbeeld voor privacy.

Het college van B&W dient jaarlijks verantwoording af te leggen over informatieveiligheid richting toezichthouders (verticale verantwoording) en richting de gemeenteraad (horizontale verantwoording). Met deze rapportage Informatiebeveiliging Deurne 2018 verantwoordt het college van de gemeente Deurne zich richting gemeenteraad over de status van informatiebeveiliging over 2018, inclusief hoe de gemeente zich heeft verantwoord richting de stelselhouders.

Voor de verantwoording richting stelselhouders betreft dit de volgende registratiesystemen en systemen met privacygevoelige informatie:

- Basisregistratie Personen (BRP).
- Paspoort en Nederlandse Identiteitskaart (PNIK).
- Digitale persoonsidentificatie (DigiD).
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).
- Basisregistratie Adressen en Gebouwen (BAG).
- Basisregistratie Grootchalige Topografie (BGT).

Alle Nederlandse gemeenten hanteren de Eenduidige Normatiek Single Information Audit (ENSIA) om zich te verantwoorden richting stelselhouders. De ENSIA bestaat uit enkele vragenlijsten waarmee bovenstaande registratiesystemen en systemen beoordeeld worden.

Deze rapportage gaat verder in op:

1. Het informatiebeveiligingsbeleid en doelstellingen.
2. Resultaat informatiebeveiliging over 2018 en vervolgstappen
 - a. per registratiesysteem;
 - b. gemeentebreed.
3. Het meerjarenperspectief.

1. Informatiebeveiligingsbeleid en doelstellingen

Informatiebeveiligingsbeleid

Een vastgestelde informatiebeveiligingsbeleid is het uitgangspunt voor de inrichting en borging van informatiebeveiliging in de gemeente.

Eind 2018 is het informatiebeveiligingsbeleid voor de gemeente Deurne opnieuw opgesteld en vastgesteld. Het is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het beleid is in lijn met het algemene beleid, de relevante landelijke en Europese wet- en regelgeving en met de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is het normenstelsel voor informatiebeveiliging waar iedere gemeente zich aan dient te houden. Overigens gaat vanaf 2020 een nieuw, maar vergelijkbaar normenkader gelden: de Baseline Informatiebeveiliging Overheid. Een gezamenlijk normenkader voor alle overheidspartijen.

De informatiebeveiligingsbeleid gaat conform de BIG in op de volgende gebieden:

- Beveiligingsbeleid.
- Organisatie van de informatiebeveiliging.
- Beheer van bedrijfsmiddelen.
- Personele beveiliging.
- Fysieke beveiliging en beveiliging van de omgeving.
- Beheer van communicatie- en bedieningsprocessen.
- Toegangsbeveiliging.
- Verwerving, ontwikkeling en onderhoud van Informatiesystemen.
- Beheer van informatiebeveiligingsincidenten.
- Bedrijfscontinuïteitsbeheer.
- Naleving.

In het beleid staan concrete doelstellingen op gebied van organisatorische, technische en fysieke beveiliging. Deze doelstellingen zijn in een beveiligingsplan verder uitgewerkt.

Doelstellingen

De gemeente Deurne stelt als doel om op het gebied van informatiebeveiliging “in control” te zijn en legt daarover jaarlijks verantwoording af. In control betekent in dit verband dat:

- de gemeente weet welke maatregelen genomen zijn;
- er een specifieke planning is van de maatregelen die nog niet genomen zijn;
- dit geheel verankerd is in de Plan Do Check Act-cyclus.

De gemeente prioriteert op basis van risicoanalyse welke maatregelen (eerst) getroffen moeten worden en hanteert hierbij het ‘pas toe of leg uit’ principe.

2. Resultaat over 2018

Zoals eerder vermeld, dient de gemeente zich te verantwoorden richting de stelselhouders over BRP, PNIK, DigiD, Suwinet, BAG, en BGT. Dit vindt plaats door een zelfevaluatie (BRP, PNIK, BAG en BGT) of door een audit (DigiD en Suwinet). Verder toetst de gemeente haar informatieveiligheid in algemene zin via een zelfevaluatie (BIG).

De resultaten en de vervolgstappen hiervan zien er als volgt uit:

Basisregistratie Personen (BRP) en Paspoort en Nederlandse Identiteitskaarten (PNIK)

De scores voor de Basisregistratie Personen (BRP) en de Paspoort en Nederlandse Identiteitskaarten (PNIK) zijn samengesteld uit de zelfevaluatie vanuit ENSIA en uit specifieke vragenlijsten voor BRP en PNIK. In onderstaand schema is zichtbaar welke score de gemeente Deurne over 2018 heeft behaald en is een vergelijking met 2017 opgenomen:

	2017	2018
BRP	85,2%	85,3%
PNIK	87,7%	94,3%

In 2018 zijn er stappen ondernomen om de informatieveiligheid beter te borgen binnen de organisatie. Ook is de ENSIA-systematiek is verbeterd, waardoor de antwoorden op de vragen een betere weerspiegeling geven voor de domeinen BRP- en PNIK. Dit heeft geleid tot een betere score.

Gaat alles dan al goed? Nee, er is altijd ruimte voor verbetering. De verbetermaatregelen en aanbevelingen voor dit domein worden in de lijn uitgevoerd. Daar waar van toepassing zijn de maatregelen opgenomen in het informatiebeveiligingsplan. De maatregelen hebben vooral betrekking op het vaststellen van beleid en op de aanscherping van werkprocessen. Denk aan risico's van misbruik, diefstal, datalekken enz. van gevoelige informatie. Hierbij geldt dat het bewaken en borgen van informatieveiligheid een continu proces is dat in belangrijke mate bijdraagt aan de betrouwbaarheid en de kwaliteit van onze dienstverlening.

Digitale persoonsidentificatie (DigiD) en Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)

DigiD staat voor Digitale identiteit waarmee de burger kan inloggen op de websites van de overheid en in de zorg. Voor DigiD voldoet de gemeente net als in 2017 aan alle normen.

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. Voor Suwinet maakt de gemeente Deurne gebruik van Senzer, een gemeenschappelijke regeling die de Participatiewet uitvoert voor o.a. Deurne. In 2017 voldeed Senzer niet aan 10 van de 12 gestelde normen. In 2018 heeft Senzer verbeteringen uitgevoerd en voldoet Senzer, maar ook de gemeente, aan alle gestelde normen.

Het college dient formeel een collegeverklaring af te leggen over de status van DigiD en Suwinet aan de gemeenteraad en toezichthouders. Daarom is deze collegeverklaring integraal opgenomen als bijlage van deze rapportage.

Basisregistratie Adressen en Gebouwen (BAG)

BAG (Basisregistratie Adressen en Gebouwen) is onderdeel van het stelsel van basisregistraties in Nederland. Gemeenten zijn bronhouders van de BAG. Dat betekent dat de gemeente verantwoordelijk is voor het beheer en de kwaliteit van de gegevens van de adressen en gebouwen binnen de gemeentegrenzen. Deurne heeft met een zelfevaluatie de borging van de processen, tijdigheid, volledigheid en juistheid getoetst.

	2017	2018
Totaal te behalen punten:	200	205
Norm voor voldoende:	150 (75%)	153,75 (75%)
Behaald aantal punten:	200 (100%)	195 (95,1%)

De conclusie van deze zelfevaluatie is dat de kwaliteit van de BAG-registratie hoog is. Met een score van 95,1% ligt het in lijn met de vereisten van het Ministerie Infrastructuur en Milieu. Een correcte uitvoer van de wet BAG is geborgd en de tijdigheid, volledigheid en juistheid van de gegevens in de registratie is goed.

Basisregistratie Grootchalige Topografie (BGT)

Basisregistratie Grootchalige Topografie (BGT) is een gedetailleerde digitale kaart van heel Nederland. Daarin staan onder andere gebouwen, wegen, water, spoorlijnen en groen. Door de gegevens in de BGT eenduidig op te slaan, zijn ze herbruikbaar voor alle overheidsorganisaties die deze gegevens nodig hebben. Gemeenten zijn bronhouder van deze basisregistratie en moeten er dus voor zorgen dat de gegevens van de BGT kloppen. Ook voor de BGT heeft Deurne een zelfevaluatie gedaan op het gebied van borging processen, tijdigheid, volledigheid en juistheid.

	2017	2018
Totaal te behalen punten:	150	150
Norm voor voldoende:	112,5 (75%)	112,5 (75%)
Behaald aantal punten:	130 (86,6%)	145 (96,7%)

De conclusie van deze zelfevaluatie is dat de kwaliteit van de BGT-registratie hoog is en verbeterd ten aanzien van 2017. Met een score van 96,7% ligt het in lijn met de vereisten van het Ministerie Infrastructuur en Milieu. Een correcte uitvoer van de wet BGT is geborgd en de tijdigheid, volledigheid en juistheid van de gegevens in de registratie is goed.

Informatieveiligheid gemeentebreed

Informatiebeveiliging is van belang voor meer dan alleen de voorgaande specifieke registraties en systemen. Dit geldt ook voor andere processen in de gemeente, vandaar dat binnen ENSIA ook gemeentebreed met een zelfevaluatie getoetst wordt of de gemeente voldoet aan de normen uit de Baseline Informatiebeveiliging Gemeenten (BIG).

Naar aanleiding van de verantwoording over 2017 zijn in 2018 doelen gesteld. De voornaamste punten waarbij verbetering zichtbaar is, zijn:

1. Rollen en verantwoordelijkheden ten aanzien van Informatieveiligheid duiden en vastleggen;
2. Bewustwording: kennis verhogen, houding en gedrag van medewerkers verbeteren;
3. Borging van acties in PDCA-cyclus.

Ten aanzien van informatiebeveiliging is in 2018 daarnaast het volgende bereikt:

- Fysieke werkplekken en documentatie zijn beter beveiligd;
- Privacywetgeving Algemene Verordening Gegevensbescherming (AVG) is geborgd in organisatie;
- Informatiebeveiligingsbeleid vastgesteld;
- Evaluatie en aanscherping van eisen van leveranciers;
- Beoordeling en begeleiding van informatiebeveiliging binnen projecten.

Op de volgende punten is wel verbetering geboekt, maar moet de organisatie nog stappen zetten om op conform de normen van de BIG en de toekomstige BIO-normen te kunnen opereren:

1. Autorisatiemanagement (wie mag wat waarin?) aanscherpen;
2. Proces veranderingen in ICT-omgeving beter borgen;
3. Proces afhandelen ICT-incidenten transparanter maken en verbeteren;
4. Bedrijfscontinuïteit; noodscenario's en uitwijkplannen aanscherpen.

De conclusie uit de zelfevaluatie is dat Deurne eind 2018 nog niet volledig voldoet aan haar eigen informatiebeveiligingsbeleid. Dit komt onder andere doordat niet alle maatregelen inzichtelijk waren, concreet waren gemaakt, of belegd waren. Dit komt mede doordat het informatiebeveiligingsbeleid met bijbehorende PDCA-cyclus nog niet volledig is geïmplementeerd.

3. Volgende stappen

In 2020 gaan alle overheidsinstellingen over op een zelfde informatiebeveiligingsnorm: de Baseline Informatiebeveiliging Overheid (BIO). In 2019 zijn en worden acties opgezet die ervoor zorgen dat:

- de gemeente beter inzicht heeft in de status van informatiebeveiliging;
- de gemeente beter inzicht heeft in de benodigde maatregelen en bijbehorende planning en middelen;
- leiding beter kan sturen op informatiebeveiliging binnen hun eigen afdelingen en processen.

Hiermee bereikt de gemeente dat informatiebeveiliging dichter bij de lijnorganisatie komt te liggen en dat de BIO wordt geïmplementeerd.

Focus maatregelen 2019-2020

De verbeterpunten op basis van de risicoanalyse kunnen niet allemaal gelijktijdig worden opgelost. De komende periode ligt de focus op onderstaande punten:

1. Autorisatiemanagement (wie mag wat waarin?) aanscherpen;
2. Proces veranderingen in ICT-omgeving beter borgen;
3. Proces afhandelen ICT-incidenten transparanter maken en verbeteren;
4. Bedrijfscontinuïteit; noodscenario's en uitwijkplannen aanscherpen.
5. Rapportage en sturing op informatiebeveiliging

4. Meerjarenperspectief

De gemeente richt zich de komende jaren op het structureel verbeteren en borgen van informatieveiligheid in de organisatie. De coördinerende rol hiervoor ligt bij de CISO, de doorgevoerde maatregelen worden geborgd in de betreffende vakafdeling. Vakafdelingen zijn verantwoordelijk voor het alle aspecten van hun werkproces en daar is informatiebeveiliging onderdeel van. De basis hiervoor vormen de BIO-normen en de informatiebeveiligingsaspecten van de audits en zelfevaluaties (waaronder ENSIA). Op basis van risico, impact en beschikbare capaciteit en middelen worden maatregelen ingepland over meerdere jaren. Daar waar mogelijk of noodzakelijk worden maatregelen in 2019 al getroffen. Om efficiënt met middelen en capaciteit om

te gaan wordt zoveel mogelijk aangesloten bij lopende projecten. Ieder jaar wordt een overzicht van genomen maatregelen en nog te nemen maatregelen meegenomen in het verantwoordingsproces.

Tot slot

Bij informatie is het van belang dat deze op een passende wijze wordt beveiligd. Zoals in de inleiding gesteld: hoe waardevoller en gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. 100% beveiliging bestaat echter niet; dagelijks worden er nieuwe kwetsbaarheden ontdekt in software, maken mensen regelmatig bewust of onbewust fouten in hun handelen of ontwikkelen criminelen nieuwe manieren om in te breken. Bedreigingen en risico's blijven zich door ontwikkelen, te treffen beveiligingsmaatregelen worden daarop continu aangepast. Daarnaast is het belangrijk dat de werkomgeving voor de medewerkers van de gemeente Deurne ook werkbaar blijft, zowel fysiek als digitaal. Je plaatst immers niet 10 sloten op de voordeur.

Kortom: bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen en werkbaarheid. Het is hierbij van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen maatregelen.

Bijlage 1: Collegeverklaring ENSIA over informatiebeveiliging DigiD en Suwinet

Hier vindt u de collegeverklaring (exclusief bijlagen) van de gemeente Deurne over DigiD en Suwinet. Een onafhankelijke auditor heeft deze verklaring getoetst.

Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Deurne

Gemeentelijk kenmerk collegeverklaring ENSIA:
001078402

Naam auditfirma:

BKBO

Naam auditor:

René Ijpelaar

Datum: 20 maart 2019

Handtekening of paraaf auditor

drs. M.B.H. Ijpelaar RE CEH

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Deurne 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 Deurne 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 001070632) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener[s] worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener worden uitgevoerd, wordt door de dienstverlener verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener[s] dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan Senzer.

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 001070632) en Suwinet (bijlage 2 Suwinet met kenmerk 001070639) 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 001070632) en voor Suwinet (bijlage 2 Suwinet met kenmerk 001070639) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Deurne op 31 december 2018 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

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 1002181	Ja	Neen
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Niet van toepassing	Niet van toepassing

Deurne, 12-03-2019

College van B en W gemeente Deurne

