Gemeente Deurne

Rapportage informatiebeveiliging 2020

op basis van ENSIA

Leeswijzer en inhoud

Deze rapportage is opgesteld op basis van ENSIA 2020

TERUGBLIK 2020
- Ontwikkelingen
- Resultaat bij belangrijkste doelen
- Beveiligingsincidenten en datalekken

STATUS INFORMATIEBEVEILIGING (BIO)
- Onze norm voor informatiebeveiliging samengevat (de BIO)
- Status Deurne ten opzichte van de BIO

VERANTWOORDING AAN HET RIJK
- Getoetste collegeverklaring ENSIA – DigiD
- Getoetste collegeverklaring ENSIA – Suwinet
- Status Basisregistratie Personen en Reisdocumenten
- Status GEO basisregistraties (BAG, BGT, BRO)

De BIO maatregelen zijn in deze rapportage beknopt opgenomen.

GEBRUIKTE SCHALEN:

groen:	goed	(90% - 100% van de punten)
oranje:	gaan de goede kant op	(75% - 90% van de punten)
rood:	onvoldoende	(0% - 75% van de punten)

groen:	voldaan aan een norm
rood:	niet voldaan aan een norm

TERUGBLIK 2020

Belangrijke ontwikkelingen in 2020

Deurne

- Nieuwe omgevingswet is volledig afhankelijk van gekoppelde informatiesystemen
- Datalek door online publicatie van aanvragen en besluiten. Procedures grondig aangepast
- Privacy en informatiebeveiliging belangrijk element in programma van eisen voor nieuwe website
- Sturen op basis van inzicht in risiconiveau
- Beleid voor autorisatiebeheer en DPIA's maakt verantwoordelijkheden duidelijk
- Budget voor informatievoorziening is onvoldoende om continuïteit, informatiebeveiliging en privacy op orde te brengen en te houden

Nederland en de wereld

- Online samenwerken neemt een vlucht, privacy- en informatiebeveiligingsvragen moeten snel beantwoord worden
- Explosieve stijging cybercriminaliteit vanaf eerste helft 2020
- Hackers gebruiken COVID-19 aandacht als dekmantel voor aanvallen
- PrivacyShield verdrag met USA ongeldig, persoonsgevens niet zomaar in de Cloud
- VNG-bestuur stelt Agenda Digitale Veiligheid 2020 – 2024 vast
- Gemeentelijke FG's zoeken naar rol: van advies naar toezicht
- Hof van Twente valt stil door cyber-criminelen, volledig herstel kost 2 jaar
- GGD lekt persoonsgegevens van miljoenen inwoners

Resultaat bij belangrijkste doelen 2020

- Op veel doelen is wel enig resultaat bereikt
- Capaciteitsgebrek op functies van informatisering, automatisering, privacy en security belemmert de voortgang
- Goede invulling van eigen rol door directie. College en management worden in 2021 meegenomen
- Voor DPIA's en autorisatiebeheer is beleid vastgesteld. Invoering volgt in 2021

Risico #	Doel	Resultaat
1	Opzet P&C-cyclus informatiebeveiliging (zogenaamd ISMS)	deels (capaciteit)
2	Beleggen verantwoordelijkheden (management)	deels
3	Eisen aan derde partijen bij uitbesteding	deels
18	Eisen bij aanschaf van nieuwe informatiesystemen	deels
6, 14	Autorisatiebeheer samen met in- en uitdienstproces P&O	deels (capaciteit)
8	Testen van wijzigingen in informatiesystemen	uitgesteld (capaciteit)
11, 17	Beveiligingsmaatregelen in Office365 en mobiele apparaten	uitgesteld (capaciteit)
12	Monitoren en Reageren op dreigingen en inbreuken	uitgesteld (capaciteit)
19	DPIA's: effectanalyse over het verwerken van persoonsgegevens	deels
4	Overzicht van processen, applicaties & gegevensverwerkingen (incl. eigenaar en risico-inschaling)	deels (capaciteit)
16	Richtlijnen thuis- en telewerken	gereed
7	Beheersen van veranderingen in de ICT-omgeving	deels
22	Procedures voor incidenten en datalekken	deels
--	Fysieke beveiliging en gedrag in het Huis voor de Samenleving	deels

Informatiebeveiligingsincidenten en Datalekken

	2018	2019	2020
Beveiligingsincidenten	niet bekend	niet bekend	23
waarbij persoonsgegevens betrokken (datalek)	8	10	14
gemeld aan autoriteit persoonsgegevens	3	5	4
gemeld aan betrokkenen vanwege hoog risico	0	0	4

* Toename wijst op betere registratie, niet noodzakelijk op meer incidenten en datalekken.

STATUS INFORMATIEBEVEILIGING

op basis van de Baseline
Informatiebeveiliging Overheid (BIO)

DE BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO)

Alle gemeentes volgen de BIO.

- De BIO maakt onderscheid tussen een basisniveau van beveiliging dat geldt voor alle informatiesystemen (zogenaamd BBN1) en extra maatregelen voor belangrijke of gevoelige informatiesystemen (BBN2). Er bestaat ook nog een niveau BBN3. Dat geldt voor Deurne niet.
- Alle maatregelen die gelden voor een informatiesysteem zijn verplicht. Voldoen aan 75% is dus niet voldoende.
- De invoering van maatregelen prioriteren we naar wat het meeste positief effect heeft.

BIO Hoofdstuk		Normen	Consolidatie	Totaal	
5	Informatiebeveiligingsbeleid	2	1. BELEID EN ORGANISATIE	23	182
6	Organiseren van informatiebeveiliging	11			
18	Naleving	10			
7	Veilig personeel	7	2. PERSONEEL EN TOEGANG	54	
9	Toegangsbeveiliging	27			
11	Fysieke beveiliging en beveiliging van de omgeving	20			
16	Beveiligingsincidenten (Beheer van informatie..)	13	3. CONTINUÏTEIT EN INCIDENTEN	19	
17	Bedrijfscontinuïteitsbeheer (Informatiebeveiligingsaspecten van ..)	6			
12	Beveiliging bedrijfsvoering	30	4. INFORMATIESYSTEMEN	55	
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	13			
15	Leveranciersrelaties	12			
8	Beheer van bedrijfsmiddelen	14	5. DATABESCHERMING	31	
10	Cryptografie	4			
13	Communicatiebeveiliging	13			

SAMENGEVAT: WAT SCHRIJFT DE BIO VOOR

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van Deurne:

- Volgt het beleid van de informatiebeveiligingsdienst gemeenten (IBD)
- Zorgt ervoor dat de juiste activiteiten voor informatiebeveiliging door de organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

1. BELEID EN ORGANISATIE
H5 / H6 / H18

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- Informatiebeveiliging is georganiseerd
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na

Het bestuur en medewerkers zijn actief betrokken bij informatiebeveiliging. Er is een organisatiebreed beleid dat richting en sturing geeft. De organisatie is effectief ingericht, waarbij rollen, taken en bevoegdheden zijn ondergebracht. Verantwoording is structureel ingericht, zodat naleving is geborgd.

2. PERSONEEL EN TOEGANG
H7 / H9 / H11

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

Alleen de juiste personen hebben toegang tot de gebouwen, systemen en gegevens van de gemeente. Er zijn passende maatregelen, zowel in organisatie als in techniek. Dit gaat om waarborgen rondom in- en externe medewerkers, toegang tot gebouwen en omgeving en toegang tot de (digitale) informatievoorziening.

SAMENGEVAT: WAT SCHRIJFT DE BIO VOOR

3. CONTINUÏTEIT EN INCIDENTEN
H16 / H17

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen afspraken met inwoners na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

De diensten van de gemeente worden geleverd volgens de afspraken die de gemeente daarover maakt met inwoners en bedrijven. Ook bij incidenten worden de diensten geleverd volgens deze afspraken.

4. INFORMATIESYSTEMEN
H12 / H14 / H15

Veilige omgang met informatiesystemen en afspraken hierover met leveranciers

- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

Informatiesystemen zijn een keten van mensen, processen en middelen. Hierin zijn procedures en maatregelen beschikbaar ter bescherming van de omgeving. Het gaat hierbij om zowel de interne als de externe informatiesystemen (uitbesteding, leveranciers en Cloud- toepassingen).

5. DATABESCHERMING
H8 / H10 / H13

Veilige omgang met data in onze applicaties

- Data wordt op de juiste manier beschermd
- De gegevens van de burgers worden veilig opgeslagen en gecommuniceerd. Binnen en buiten de gemeente

STATUS DEURNE TEN OPZICHT VAN DE BIO

Deurne is in 2020 gestart met werken volgens de BIO.
Op veel punten wordt nog niet aan de norm voldaan. Hierdoor lopen we risico's.
De eerste aandacht moet gaan naar twee gebieden:

- taken en verantwoordelijkheden duidelijk beleggen en vervolgens sturen en controleren op het naleven van beleid voor privacy en informatiebeveiliging,
- voorbereiden voor wanneer het ernstig mis gaat en bijvoorbeeld systemen uitvallen of Deurne slachtoffer wordt van cybercriminelen.

onvoldoende
60%

0% - 75% 75% - 90% 90% - 100%

1. BELEID EN ORGANISATIE Actueel beleid en organisatie van informatiebeveiliging en controle op naleving	48%
2. PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	76%
3. CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten	21%
4. INFORMATIESYSTEMEN Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers	62%
5. DATABESCHERMING Veilige omgang met data in onze software	62%

1. BELEID EN ORGANISATIE

onvoldoende

48%

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is.
- Informatiebeveiliging is georganiseerd.
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na.

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H5 / Informatiebeveiligingsbeleid	0%
H6 / Organiseren van informatiebeveiliging	64%
H18 / Naleving	40%

Bevindingen en verbeteracties

- *Beleid voor informatiebeveiliging vernieuwen en/of beschrijven waar het nog ontbreekt*
- *Toewijzen van taken en verantwoordelijkheden in de organisatie en hulp bieden om deze uit te voeren*
- *Overzicht van de relevante wetgeving en dit vertalen naar maatregelen voor privacy en informatiebeveiliging*
- *Controles uitvoeren op naleven van richtlijnen voor privacy en informatiebeveiliging*
- *Structureel onderzoek doen naar aanwezigheid van technische kwetsbaarheden in informatiesystemen*

Risico’s

- *Er kan niet worden gestuurd op privacy en informatiebeveiliging*
- *Afspraken over gebruik van (persoons)gegevens worden niet nagekomen, wet- en regelgeving worden overtreden*
- *De organisatie kent de risico's en zwakke plekken niet. Dit kan ernstige gevolgen hebben voor continuïteit*

2. PERSONEEL EN TOEGANG

voldoende

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

76%

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H7 / Veilig personeel	100%
H9 / Toegangsbeveiliging	67%
H11 / Fysieke beveiliging en beveiliging van de omgeving	80%

Bevindingen en verbeteracties

- *Beleid voor toegang tot informatiesystemen is vastgesteld. Nu invoeren en borgen met controles*
- *Fysieke beveiliging van gebouwen (bijv. nieuwe gemeentehuis) moet worden geborgd met beleid en controles*

Risico's

- *Vertrouwelijke informatie en persoonsgegevens zijn in te zien door medewerkers die dit niet nodig hebben*
- *Gemeentehuis houdt na het verbouwen zwaktes in de beveiliging. Personen, goederen en informatie lopen risico*

3. CONTINUÏTEIT EN INCIDENTEN

onvoldoende

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen afspraken met inwoners na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

21%

Onderdelen:

0% - 75% 75% - 90% 90% - 100%

H16 / Beheer van beveiligingsincidenten	31%
H17 / Bedrijfscontinuïteitsbeheer & informatiebeveiliging	0%

Bevindingen en verbeteracties

- *Opstellen en oefenen van een responsplan voor incidenten en calamiteiten in die onze informatievoorziening*
- *Opstellen en oefenen van plannen om continuïteit van de dienstverlening overeind te houden tijdens een calamiteit*

Risico's

- *Bij onjuist reageren groeit een incident uit tot calamiteit met politieke, maatschappelijke en financiële schade*
- *De dienstverlening aan inwoners komt na een ernstig incident of gerichte cyber-aanval langdurig stil te liggen*

4. INFORMATIESYSTEMEN

onvoldoende

62%

Veilige omgang met informatiesystemen en afspraken hierover met leveranciers

- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

Onderdelen: 0% - 75% | 75% - 90% | 90% - 100%

H12 / Beveiliging van de bedrijfsvoering	43%
H14 / Acquisitie, ontwikkeling en onderhoud van informatie systemen	85%
H15 / Leveranciersrelaties	83%

Bevindingen en verbeteracties

- *Back-ups maken, testen en beschermen op een manier die past bij het belang van de informatie*
- *Nieuwe en aangepaste applicaties gecontroleerd en (liefst) zonder persoonsgegevens testen buiten productie*
- *Strakke afspraken over informatiebeveiliging met leveranciers en partners*
- *Beter contractbeheer en controle op naleven van afspraken door leveranciers en partners*
- *Logbestanden automatisch controleren om cyber-dreigingen te kunnen opmerken*

Risico's

- *Informatie die niet goed geback-upt is gaat verloren door een ongeluk of cyber-aanval*
- *De dienstverlening wordt gehinderd door fouten in een nieuwe of aangepaste applicatie*
- *Persoonsgegevens worden onrechtmatig verwerkt bij het testen van applicaties*
- *Wanneer de gemeente uitbesteedt of samenwerkt wordt ons beveiligingsbeleid geschonden*
- *Hackers zijn al binnen zonder dat het wordt opgemerkt. Gevolg: dienstverlening ligt weken stil (zie Hof van Twente)*

5. DATABESCHERMING

onvoldoende

62%

Veilige omgang met data in onze applicaties
- Data wordt op de juiste manier beschermd
- De gegevens van de burgers worden veilig opgeslagen en gecommuniceerd.
- Binnen en buiten de gemeente

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H8 / Beheer van bedrijfsmiddelen	64%
H10 / Cryptografie	0%
H13 / Communicatiebeveiliging	77%

Bevindingen en verbeteracties
- *Informatie passend beveiligen en beschermen door het eerst te classificeren zodat eisen en risico's duidelijk worden*
- *Technisch beter beschermen van (gemeentelijke) informatie bij thuis- en mobiel werken*
- *Computernetwerk van het gemeentehuis veiliger inrichten met afgescheiden "kamers" (segmenten) en zorgen dat aanvallen en verdachte bewegingen kunnen worden opgemerkt en gestopt*

Risico's
- *Informatie wordt niet goed beveiligd en beschermd met politieke, organisatie- of persoonlijke schade als gevolg*
- *Informatie wordt onveilig en/of onrechtmatig verwerkt op mobiele apparaten die ook privé eigendom kunnen zijn*
- *Een aanvaller (cyber-crimineel) die in ons netwerk binnen is kan ongehinderd alle "kamers" doorzoeken*

ENSIA VERANTWOORDING AAN HET RIJK

Getoetste collegeverklaring ENSIA - DIGID

voldaan

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor DigiD worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder Logius/BZK.

DigiD:
DigiD is een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening.

Niet voldaan voldaan

Website deurne.nl	Aanvragen van diensten van de gemeente	Geen risico’s	
iBurgerzaken	Aanvragen van diensten van Burgerzaken (BRP en reisdocumenten)	Geen risico’s	

Voor DigiD aansluitingen voldoet Deurne op alle punten aan de norm. Daarom zijn geen verbetermaatregelen gepland.

Getoetste collegeverklaring ENSIA - Suwinet

niet voldaan

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor Suwinet worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder BKWI/SZW.

SUWI (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen):
Suwinet is een digitale infrastructuur die is ontwikkeld door de Suwipartijen (UWV, SVB en gemeenten) om ervoor te zorgen dat zij gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld waar een wettelijke grondslag voor is. Wij gebruiken Suwinet voor de uitvoering van de Participatiewet, de uitvoering van de IOAZ en IOAW, raadplegen van adresgegevens bij Burgerzaken en het raadplegen van gegevens door gemeentelijk gerechtsdeurwaarders wanneer er een getekend dwangbevel is.

Niet voldaan voldaan

Participatiewet/IOAZ/IOAW - Suwinet Inkijk	Gebruik Suwinet door Senzer	Oud informatiebeveiligingsbeleid (Deurne) Controle toegangsrechten onvoldoende (Senzer)

Door Senzer zijn per direct aanvullende controles ingevoerd op toegangsrechten van gebruikers. Hierdoor wordt inmiddels wel voldaan aan de norm. Het college laat in de eerste helft van 2021 het informatiebeveiligingsbeleid vernieuwen.

Status Basisregistratie Personen en Reisdocumenten

goed

Van onze zelfevaluatie ENSIA wordt de verantwoording over de Basisregistratie Personen (BRP) en de wet- en regelgeving voor de Reisdocumenten (paspoorten en ID-kaarten) afgeleid. De uitkomsten worden verzonden aan de Rijksdienst voor de Identiteitsgegevens (RvIG). De zelfevaluatie voor informatiebeveiliging vindt via de ENSIA systematiek plaats. De verantwoording over de kwaliteit van de registraties komt voort uit de zelfevaluatie in de Kwaliteitsmonitor.

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen:

- BRP: 90%
- Reisdocumenten: 90%

0% - 75% 75% - 90% 90% - 100%

Basisregistratie Personen (BRP)
De zelfevaluatie BRP over het jaar 2020 is afgerond met 1879 van maximaal 2000 zijnde 94%

Wet- en regelgeving voor Reisdocumenten
De zelfevaluatie BAG over het jaar 2020 is afgerond met 1945 van maximaal 2000 zijnde 97%

De belangrijkste verbetermaatregelen die de gemeente zich voorneemt zijn het vernieuwen van het informatiebeveiligingsbeleid en het verstevigen van de controle op naleven van privacy-regelgeving (de AVG).

Status GEO-basisregistraties

goed

Wij verantwoorden ons aan het ministerie van BZK/Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) over drie basisregistraties in het geografische domein. De rapportages zijn tot stand gekomen op basis van door ons uitgevoerde zelfevaluaties. De zelfevaluaties betreffen de kwaliteit van de registraties (geen informatiebeveiliging).

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen:

- BAG 75 %
- BGT 75%
- BRO 75 %

0% - 75% 75% - 90% 90% - 100%

Basisregistratie Adressen en Gebouwen (BAG)
De zelfevaluatie BAG over het jaar 2020 is afgerond met 175 van maximaal 205 punten zijnde 85%

Basisregistratie Grootschalige Topografie (BGT)
De zelfevaluatie BGT over het jaar 2020 is afgerond met 150 van maximaal 150 punten zijnde 100%

Basisregistratie Ondergrond (BRO)
De zelfevaluatie BGT over het jaar 2020 is afgerond met 110 van maximaal 120 zijnde 92%

Deurne voldoet op alle punten aan de norm. Daarom zijn geen verbetermaatregelen gepland.