Rapportage **Informatiebeveiliging 2021 gemeente Duiven**

Inleiding

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.
Inwoners en ondernemers verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). Dat zorgt niet alleen voor betrouwbaarheid, maar ook een goede kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen.
Iedere overheidslaag heeft in een eerder stadium besloten om de overheidsbrede norm voor informatiebeveiliging, de Baseline Informatiebeveiliging Overheid (BIO) toe te passen.
Gemeenten verantwoorden zich over informatiebeveiliging en – kwaliteit middels ENSIA. Dat staat voor Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op verantwoording richting het college van burgemeester en wethouders en de gemeenteraad. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen, zoals de diverse basisregistraties BRP, BAG, BGT, BRO, WOZ en DigiD en Suwinet (zie de afbeelding).



De wijze waarop de verantwoording richting raad plaatsvindt is aan het college. Met deze rapportage is getracht een samenvatting te maken van de bevindingen/status van de informatiebeveiliging, alsmede een samenvatting van de collegeverklaring en het door de auditor opgestelde assurance-rapport van onze gemeente.

Leeswijzer

Deze rapportage is opgesteld op basis van ENSIA 2021
De samenvatting is als volgt opgebouwd:

STATUS INFORMATIEBEVEILIGING (BIO)
- Bestuurlijke uitgangspunten
- Samenvatting van 5 hoofdstukken (consolidatie van de 18 BIO-hoofdstukken)

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

De maatregelen zijn beknopt opgenomen. Voor de exacte strekking raadpleegt u ENSIA (zelfevaluatie BIO) of de BIO.

Er is uitgegaan van een schaal met 3 categorieën:

 (goed),  (voldoende) en (onvoldoende).

Bij de samengevatte 5 hoofdstukken zijn twee teksten met toelichting opgenomen:
a. Puntsgewijze toelichting
b. Uitgeschreven toelichting
Er zijn bestuurlijke uitgangspunten opgenomen in de overzichtspagina. Deze kennen geen score.

Bouwstenen

Beschrijving van de vijf hoofdstukken bestaande uit achttien geconsolideerde BIO-hoofdstukken

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van onze gemeente:

- Volgt het beleid van de Informatiebeveiligingsdienst Gemeenten (IBD)
- Zorgt ervoor dat de juiste activiteiten ten aanzien van informatiebeveiliging door de gemeentelijke organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

1. BELEID EN ORGANISATIE
H5 / H6 / H18 uit de BIO

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- De informatiebeveiligingsorganisatie is geregeld
- Waar, wanneer houden we ons aan onze afspraken en leven we 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 uit de BIO

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is de toegang 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 organisatorische en technische maatregelen getroffen. Dit gaat om waarborgen rondom in- en externe medewerkers, toegang tot gebouwen en omgeving en toegang tot de (digitale) informatievoorziening.

Bouwstenen

Beschrijving voor consolidatie

3. CONTINUÏTEIT EN INCIDENTEN
H16 / H17 uit de BIO

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen onze afspraken met de burger na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen worden geactualiseerd en na vaststelling ook getest
- Incidenten worden gemeld, geregistreerd en overeenkomstig het proces afgehandeld

4. INFORMATIESYSTEMEN
H12 / H14 / H15 uit de BIO

Veilige omgang met informatiesystemen en afspraken hierover met onze 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 uit de BIO

Veilige omgang met data in onze software

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

Status informatiebeveiliging BIO Duiven

BESTUURLIJKE UITGANGSPUNTEN
Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van onze gemeente:

- Volgt het beleid van de IBD
- Zorgt ervoor dat de juiste informatiebeveiliging door de gemeentelijke organisatie en de samenwerkingspartners wordt uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

De samenvatting van deze status van informatiebeveiliging geeft een weergave van de gehele organisatie en onze belangrijkste samenwerkingspartner, de RID.
In de achterliggende periode zijn een groot aantal BIO-maatregelen ingevoerd, waarbij gelet op de omvang van het aantal maatregelen prioriteit is gegeven aan de meest risicovolle processen. Dit jaar ligt het accent op de verdere implementatie van de BIO-maatregelen en o.a. de actualisering van het ICT-continuïteitsplan, actualisering van het logisch en fysiek toegangsbeheer, de verbetering van de bewustwording informatieveiligheid, monitoring en response en goede procesbeschrijvingen/werkinstructies.



1. BELEID EN ORGANISATIE
Actueel beleid en organisatie van informatiebeveiliging en controle op naleving



2. PERSONEEL EN TOEGANG
Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens



3. CONTINUÏTEIT EN INCIDENTEN
Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten



4. INFORMATIESYSTEMEN
Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers



5. DATABESCHERMING
Veilige omgang met data in onze software

1. BELEID EN ORGANISATIE

Status:
goed



Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

Onderdelen:

H5 / Informatiebeveiligingsbeleid	
H6 / Organiseren van informatiebeveiliging	
H 18 / Naleving	

Voor dit onderdeel kunnen we op basis van de zelfevaluatie concluderen dat we in het algemeen voldoende scoren voor wat betreft de BIO-eisen. Echter: het is nog niet perfect en op een beperkt aantal onderdelen is zeker nog verbetering noodzakelijk.

Met name het implementeren van een ISMS (Information Security Management System) is een verbeterpunt. Dit ISMS is inmiddels aangeschaft en wordt nu ingericht. Met dit instrument kunnen we onder andere de veiligheidsrisico's beter in kaart brengen, het beleid beheersen en opstellen en de taken en verantwoordelijkheden verdelen. Dit leidt tot een manier van werken met als basis een systematisch verbeterproces, met als uiteindelijk resultaat een steeds betere informatiebeveiliging.

2. PERSONEEL EN TOEGANG

Status: voldoende



Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

Onderdelen:

H7 / Veilig personeel	
H9 / Toegangsbeveiliging	
H11 / Fysieke beveiliging en beveiliging van de omgeving	

We voldoen over het algemeen voldoende aan BIO-eisen voor veilig personeel en toegangsbeveiliging (digitaal en fysiek), maar er zijn verbeterpunten, zoals het systematisch instrueren (via een bewustwordingsprogramma) van de medewerkers over verantwoordelijkheden rond informatiebeveiliging en een goede borging van het logisch en fysiek toegangsbeheer. Het beleid op dit terrein wordt geactualiseerd.

3. CONTINUÏTEIT EN INCIDENTEN

Zorgen voor de continuïteit van onze dienstverlening en het opvolgen van incidenten

Status: voldoende



Onderdelen:

H16 / Beheer van beveiligingsincidenten	
H17 / Bedrijfscontinuïteitsbeheer & informatiebeveiliging	

De continuïteit is in het algemeen goed geregeld, maar er is verbetering mogelijk rond het ICT-continuïteitsplan, de back-up en restore procedures en met name ook het periodiek testen en oefenen ervan.

4. INFORMATIESYSTEMEN

Veilige omgang met informatiesystemen en afspraken hierover maken met onze leveranciers

Status: voldoende



Onderdelen:

H12 / Beveiliging van de bedrijfsvoering	
H14 / Acquisitie, ontwikkeling en onderhoud van informatie systemen	
H16 / Beheer van informatiebeveiligingsincidenten	

Een van de aandachtspunten uit de brief van de VNG inzake voorkomen van een ransomware-aanval is om te zorgen voor het up-to-date houden van de hard- en software. Om dit mogelijk te maken zijn extra middelen beschikbaar gesteld.

5. DATABESCHERMING

Veilige omgang met data in onze software

Status: voldoende



Onderdelen:

H8 / Beheer van bedrijfsmiddelen	
H10 / Cryptografie	
H13 / Communicatiebeveiliging	

Ook bij dit onderdeel is het beeld gemengd: verbetering is mogelijk o.a. door het hanteren van een strikte netwerksegmentatie. Dit is ook een van de aanbevelingen uit de brief van de VNG inzake de toename van de dreiging van een ransomware-aanval.

Getoetste collegeverklaring ENSIA

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 (nog niet op werking). Voor DigiD worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder Logius/BZK. Voor Suwinet worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder BKWI/SZW.

DigiD

DigiD is een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening. Voor de verantwoording van de DigiD aansluitingen op naam van de gemeente moet verantwoording worden afgelegd via ENSIA. Voor de aansluitingen moet worden voldaan aan landelijk normenkader. Indien daar niet aan wordt voldaan, dan worden de aansluitingen afgesloten. Indien van toepassing krijgt de gemeente wel altijd twee maanden de tijd om de tekortkomingen te herstellen.

 Niet voldaan  voldaan

Aansluiting 1	Betreft een aansluiting voor de website van Duiven		
Aansluiting 2	Betreft de aansluiting voor de eDiensten van Burgerzaken		

De onafhankelijke auditor heeft vastgesteld dat de gemeente voldoet aan de normen voor DigiD, zoals opgesteld door NOREA, de beroepsorganisatie van IT-Auditors. Inmiddels heeft ook Logius bevestigd, dat onze gemeente heeft voldaan aan alle voorwaarden en de DigiD-dienstverlening voor deze twee aansluitingen zal voortzetten.

Getoetste collegeverklaring ENSIA - vervolg

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. De participatiewet/ IOAZ/IOAW wordt door de Regionale Sociale Dienst uitgevoerd. Maar het ministerie heeft aangegeven dat ongeacht of je taken hebt gemandateerd of gedelegeerd de verantwoording dient plaats te vinden door de gemeente zelf. De aansluiting voor de voortijdige schoolverlaters valt onder de verantwoordingsplicht van de gemeente Nijmegen. Tot slot maakt Burgerzaken incidenteel gebruik van de raadpleegmogelijkheid in Suwinet bij de uitvoering van adresonderzoeken.

☹ Niet voldaan ☺ voldaan

Participatiewet/IOAZ/IOAW - Suwinet Inkijk - Suwinet Inlezen - DKD Inlezen	Uitgevoerd door de Regionale Sociale Dienst de Liemers (RSD)	Voldaan	☺ ☺ ☺

Vastgesteld door de onafhankelijke auditor.

Status Basisregistratie Personen en Reisdocumenten

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) en Autoriteit Persoonsgegevens(AP). 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.

Basisregistratie Personen (BRP)
De zelfevaluatie BRP (ENSIA) over het jaar 2021 is afgerond met een score van 1090 van maximaal 1200 zijnde 90 %



Wet- en regelgeving voor Reisdocumenten
De zelfevaluatie Reisdocumenten (ENISA) over het jaar 2021 is afgerond met een score van 1075 van maximaal 1200 zijnde 89%



Gelet op de hierboven genoemde scores worden de bestaande plannen en procedures geactualiseerd en de resultaten ook verwerkt in de diverse (schriftelijke) rapportages.

Status GEO-basisregistraties

Wij verantwoorden ons aan het Rijk via het directoraat-generaal Bestuur, Ruimte en Wonen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties over drie geobasisregistraties. De rapportages zijn tot stand gekomen op basis van door ons uitgevoerde zelfevaluaties via de ENSIA systematiek. De beantwoording van de vragen worden uiteindelijk omgezet naar een score voor de gegevenskwaliteit en een score voor het proces en organisatie. In deze rapportage is de totaalscore opgenomen.

De gemeente wordt geacht de volgende score (norm) te behalen voor:

- BAG 75 %
- BGT 75 %
- BRO 60 %

Basisregistratie Adressen en Gebouwen (BAG) De zelfevaluatie BAG over het jaar 2021 is afgerond met een score van 64%	
Basisregistratie Grootschalige Topografie (BGT) De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 95%	
Basisregistratie Ondergrond (BRO) over het 2021 is afgerond met een score van 61%	

Voor de Basisregistratie Adressen en Gebouwen (BAG) wordt een plan van aanpak opgesteld met als doel om komend jaar wel aan de norm te voldoen. De behalen norm voor de BRO ligt op dit moment een stuk lager. Dit heeft te maken met het feit dat dit een basisregistratie in opbouw is.

Status basisregistratie WOZ

Wij verantwoorden ons aan de Waarderingskamer en het ministerie van Financiën over de basisregistratie WOZ. De rapportage is tot stand gekomen op basis van door ons uitgevoerde zelfevaluatie (de beantwoording van de vragenlijst). In 2021 is de WOZ-zelfevaluatie voor de eerste keer toegevoegd aan de ENSIA. De WOZ-vragenlijst beperkt zicht tot de onderdelen informatiebeveiliging en de informatie-architectuur.

Basisregistratie Waardering Onroerende Zaken (WOZ)



Voor de WOZ zijn een aantal maatregelen in gang gezet. Onder andere door de implementatie van het ISMS komt ook voor de WOZ de gewenste managementinformatie voor bijvoorbeeld de onderwerpen autorisatiebeheer en het change management proces beschikbaar. Voor de WOZ is nog geen normering beschikbaar. Op basis van de resultaten van de zelfevaluatie concluderen we dat het resultaat voldoende is.