Rapportage **ENSIA 2023** gemeente Duiven

Inleiding

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is 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 door ENSIA. Dat staat voor Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op verantwoording richting de gemeenteraad. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen, zoals DigiD en Suwinet en de basisregistraties BRP, Reisdocumenten, BAG, BGT, BRO en WOZ (zie de afbeelding).



De manier waarop de verantwoording richting raad gebeurt is aan het college. Met deze rapportage is geprobeerd een samenvatting te maken van de bevindingen/status van de informatiebeveiliging, net als een samenvatting van de collegeverklaring informatiebeveiliging DigiD en
Suwinet en het door de auditor opgestelde assurance- rapport van onze gemeente.

Leeswijzer

Deze rapportage is opgesteld op basis van de zelfevaluatie ENSIA 2023 en is als volgt opgebouwd:

STATUS INFORMATIEBEVEILIGING (BIO)
- Bestuurlijke uitgangspunten
- Samenvatting van 5 hoofdstukken (samenvoeging van 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)

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

Er is uitgegaan van een schaal met 3 categorieën:
Groen, oranje en rood.

 (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 deze gemeente:

- Volgt het beleid van de informatiebeveiligingsdienst gemeenten (IBD)
- Zorgt ervoor dat de juiste activiteiten voor de informatiebeveiliging door de gemeentelijke 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
- 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

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 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

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 zijn actueel en worden getest
- Incidenten worden altijd gemeld, geregistreerd en overeenkomstig het proces afgehandeld

De diensten van de gemeente worden geleverd volgens de afspraken die de gemeente daarover maakt met de burger 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 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

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 deze gemeente:

- Volgt het beleid van de IBD
- Zorgt ervoor dat de juiste informatiebeveiliging door de gemeentelijke organisatie 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 de Liemers.
In de achterliggende periode zijn een groot aantal BIO-maatregelen ingevoerd. Het accent ligt nu op de verdere implementatie van de BIO-maatregelen. Het betreft onder andere de actualisering van het ICT-continuïteitsplan in samenwerking met Openbare Orde en Veiligheid en RID de Liemers en het periodiek oefenen en testen hiervan, de verbetering van de bewustwording informatieveiligheid, de implementatie van monitoring & response, het verbeteren van Identity & Acces management (Identificatie, authenticatie en autorisatie) en de doorontwikkeling van Microsoft 365.



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



Getoetste collegeverklaring ENSIA - DIGID

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. 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. Als daar niet aan wordt voldaan, dan worden de aansluitingen afgesloten. Wanneer van toepassing krijgt de gemeente wel altijd twee maanden de tijd om de tekortkomingen te herstellen.

		Niet voldaan	voldaan
Aansluiting 1	Betreft de aansluiting voor de formulieren 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 - Suwinet

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. 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 door de gemeente zelf gebeurt. De aansluiting voor de voortijdige schoolverlaters valt onder de verantwoordingsplicht van de gemeente Arnhem. Tot slot maakt Burgerzaken incidenteel gebruik van de raadpleegmogelijkheid in Suwinet bij de uitvoering van adresonderzoeken en het Sociaal Domein bij de uitvoering van de Bijzondere Bijstand.

 Niet voldaan  voldaan

Participatiewet/IOAZ/IOAW: • Suwinet Inkijk • Suwinet Inlezen • Digitaal Klantdossier (DKD) Inlezen	Uitgevoerd door de Regionale Sociale Dienst de Liemers (RSD)		

De onafhankelijke auditor heeft vastgesteld dat de gemeente niet voldoet (deels) aan de normen voor Suwinet, zoals opgesteld door NOREA, de beroepsorganisatie van IT-Auditors. Een verbeterplan is opgesteld en inmiddels wordt er weer voldaan aan de normen. Bij de volgende audit zal dit bevestigd worden.

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). De zelfevaluatie voor informatiebeveiliging gebeurt via de ENSIA. 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 over het jaar 2023 is afgerond met een score van 1200 van maximaal 1200 zijnde 100 %	
Wet- en regelgeving voor Reisdocumenten De zelfevaluatie Reisdocumenten over het jaar 2023 is afgerond met een score van 1200 van maximaal 1200 zijnde 100 %	

Gelet op de hierboven genoemde scores blijven we de bestaande plannen en procedures kritisch monitoren. De resultaten zijn ook verwerkt in de diverse (schriftelijke) rapportages.

Status GEO-basisregistraties

Wij verantwoorden ons aan het Rijk via het ministerie van Binnenlandse Zaken/Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) over drie basisregistraties in het geografische domein. De rapportages zijn gemaakt 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 moeten de volgende score behalen voor:

- Basisregistratie Adressen en Gebouwen (BAG) 75 %
- Basisregistratie Grootschalige Topografie (BGT) 75%
- Basisregistratie Ondergrond (BRO) 60%

 Niet voldaan  voldaan

Basisregistratie Adressen en Gebouwen (BAG) De zelfevaluatie BAG over het jaar 2022 is afgerond met een score van 85%	
Basisregistratie Grootschalige Topografie (BGT) De zelfevaluatie BGT over het jaar 2022 is afgerond met een score van 100%	
Basisregistratie Ondergrond (BRO) De zelfevaluatie BGT over het jaar 2022 is afgerond met een score van 78%	

Voor de Basisregistratie Adressen en Gebouwen (BAG) hebben de ingezette verbeteracties opgeleverd dat dit jaar voor het eerst aan de norm is voldaan sinds de invoering van de ENSIA.