# Rapportage **ENSIA** voor de gemeenteraad Alblasserdam

24-05-2022

# Leeswijzer

**Deze rapportage is opgesteld op basis van de zelfevaluatie ENSIA 2021 en is als volgt opgebouwd:**

**STATUS INFORMATIEBEVEILIGING (BIO)**
- Bestuurlijke uitgangspunten
- Samenvatting van 5 hoofdstukken (consolidatie 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 beknopt 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.

# **Consolideren:** verdeling van maatregelen BIO

| BIO Hoofdstuk | | Aantal maatregelen | Consolidatie | Totaal aantal maatregelen | |
|---|---|---|---|---|---|
| H5 | Informatiebeveiligingsbeleid | 2 | **1. BELEID EN ORGANISATIE** | 23 | 155 |
| H6 | Organiseren van informatiebeveiliging | 11 | | | |
| H18 | Naleving | 10 | | | |
| H7 | Veilig personeel | 6 | **2. PERSONEEL EN TOEGANG** | 46 | |
| H9 | Toegangsbeveiliging | 27 | | | |
| H11 | Fysieke beveiliging en beveiliging van de omgeving | 13 | | | |
| H16 | Beheer van informatiebeveiligingsincidenten | 12 | **3. CONTINUÏTEIT EN INCIDENTEN** | 16 | |
| H17 | Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer | 4 | | | |
| H12 | Beveiliging bedrijfsvoering | 27 | **4. INFORMATIESYSTEMEN** | 46 | |
| H14 | Acquisitie, ontwikkeling en onderhoud van informatiesystemen | 7 | | | |
| H15 | Leveranciersrelaties | 12 | | | |
| H 8 | Beheer van bedrijfsmiddelen | 9 | **5. DATABESCHERMING** | 24 | |
| H10 | Cryptografie | 5 | | | |
| H13 | Communicatiebeveiliging | 10 | | | |

# **Bouwstenen:** 180 maatregelen

Consolidatie BIO-maatregelen

**1. BELEID EN ORGANISATIE**
(23 maatregelen)

- H5: Informatiebeveiligingsbeleid (2)
- H6: Organiseren van informatiebeveiliging (11)
- H18: Naleving (10)

**2. PERSONEEL EN TOEGANG**
(46 maatregelen)

- H7 :Veilig personeel (6)
- H9 : Toegangsbeveiliging (27)
- H11 : Fysieke beveiliging en beveiliging van de omgeving (13)

**3. CONTINUÏTEIT EN INCIDENTEN**
(16 maatregelen)

- H16: Beheer van informatiebeveiligingsincidenten (12)
- H17: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (4)

**4. INFORMATIESYSTEMEN**
(46 maatregelen)

- H12: Beveiliging bedrijfsvoering (27)
- H14: Acquisitie, ontwikkeling en onderhoud van informatiesystemen (7)
- H15: Leveranciersrelaties (12)

**5. DATABESCHERMING**
(24 maatregelen)

- H8: Beheer van bedrijfsmiddelen (9)
- H10: Cryptografie (5)
- H13: Communicatiebeveiliging (10)

# Bouwstenen

Beschrijving voor consolidatie

**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 ten aanzien van 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

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

**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

Gebleken is dat gemeente Alblasserdam over het algeheel voldoende scoort in de zelfevaluaties en verantwoording aan het Rijk.

Verbeterpunten en aandachtspunten zijn opgenomen in specifieke verbeterplannen en/of het strategische Regio Drechtsteden informatiebeveiligingsplan 2022.

**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: Voldoende

**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 en hoe: altijd werken wij veilig
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na

Voldoen aan 21/23 maatregelen

| Onderdelen | onvoldoende | voldoende | goed |
|---|---|---|---|
| H5 - Informatiebeveiligingsbeleid | | | 2/2 |
| H6 - Organiseren van informatiebeveiliging | | 9/11 | |
| H18 - Naleving | | | 10/10 |

## 2. PERSONEEL EN TOEGANG

**Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens**

Status: Voldoende

Voldoen aan 39/46 maatregelen

onvoldoende voldoende goed

| Onderdelen: | |
|---|---|
| H7 - Veilig personeel | 3/6 |
| H9 - Toegangsbeveiliging | 24/27 |
| H11 - Fysieke beveiliging en beveiliging van de omgeving | 12/13 |

## 3. CONTINUÏTEIT EN INCIDENTEN

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

Status: Voldoende

Voldoen aan 15/16 maatregelen

Onderdelen:

onvoldoende voldoende goed

| | |
|---|---|
| H16 - Beheer van beveiligingsincidenten | 11/12 |
| H17 - Bedrijfscontinuïteitsbeheer & informatiebeveiliging | 4/4 |

## 4. INFORMATIESYSTEMEN

**Veilige omgang met informatiesystemen en afspraken hierover maken met onze leveranciers**

Status: Voldoende

Voldoen aan 34/46 maatregelen

Onderdelen:

onvoldoende voldoende goed

| | |
|---|---|
| H12 - Beveiliging van de bedrijfsvoering | 20/27 |
| H14 - Acquisitie, ontwikkeling en onderhoud van informatie systemen | 5/7 |
| H15 - Leveranciersrelaties | 9/12 |

## 5. DATABESCHERMING

**Veilige omgang met data in onze software**

Status: voldoende

Voldoen aan 19/24 maatregelen

Onderdelen:

onvoldoende voldoende goed

| | |
|---|---|
| H8 - Beheer van bedrijfsmiddelen | 9/9 |
| H10 - Cryptografie | 1/5 |
| H13 - Communicatiebeveiliging | 9/10 |

Cryptografie betreft een aandachtspunt. Dit is belegd bij het SGD, hierbij is een voorstel onder handen om tot verbeteringen te komen.

# 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.

☹ Niet voldaan ☺ voldaan

| | | | |
|---|---|---|---|
| DigiD Loket 1002829 | Alblasserdam heeft één DigiD-aansluiting voor authenticatie bij het genereren van aanvraagformulieren voor de gemeentelijke dienstverlening. | Niet voldaan | ☹ |
| DigiD eDiensten 1003441 | Ablasserdam heeft één DigiD-aansluiting voor authenticatie bij e-Diensten, digitale dienstverlening, voor Burgerzaken. | Voldaan | ☺ |

Er wordt over het jaar 2021 niet voldaan in opzet en bestaan aan alle geselecteerde normen.
De bevindingen zijn opgenomen in een verbeterplan. De zelfevaluatie is getoetst door een IT-auditor.

# 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, 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<br>- Suwinet Inkijk<br>- Suwinet Inlezen<br>- DKD Inlezen | Participatiewet/IOAW/IOAZ (samenwerkingsverband: Sociale Dienst Drechtsteden) | DKD: niet voldaan | ☺<br>☹ |
| Burgerzaken | Adresonderzoek door Burgerzaken (Gemeente Dordrecht: Dienstverlening Drechtsteden) | Niet voldaan | ☹ |
| Gerechtsdeurwaarders | Loonbeslag door Gemeentelijke Belastingdeurwaarders (samenwerkingsverband: Samenwerkingsverband Vastgoedinformatie Heffing en Waardebepaling (SVHW)) | Voldaan | ☺ |

DKD: Er wordt over het jaar 2021 niet voldaan in opzet en bestaan aan alle geselecteerde normen en is getoetst door een IT-auditor. Het betreft een nieuwe aansluiting. De bevindingen zijn opgenomen in een verbeterplan. Na uitvoering verbeterplan in Q3 is de verwachting dat we weer voldoen.

Burgerzaken: Er wordt over het jaar 2021 niet voldaan in opzet en bestaan aan alle geselecteerde normen.
De bevindingen zijn opgenomen in een verbeterplan. De zelfevaluatie is getoetst door een IT-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). 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 binnen ENSIA geacht de volgende score te behalen voor:

- BRP 1200 punten = 100%
- Reisdocumenten 1200 punten = 100%

**Basisregistratie Personen (BRP)**
De zelfevaluatie BRP over het jaar 2021 is afgerond met een score van 1160 van maximaal 1200 zijnde 96.0%

**Wet- en regelgeving voor Reisdocumenten**
De zelfevaluatie Reisdocumenten over het jaar 2021 is afgerond met een score van 1185 van maximaal 1200 zijnde 98.75%

## Status GEO-basisregistraties

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 voor:

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

**Basisregistratie Adressen en Gebouwen (BAG)**
De zelfevaluatie BAG over het jaar 2021 is afgerond met een score van 109.2 van maximaal 140 zijnde 78.0%

**Basisregistratie Grootschalige Topografie (BGT)**
De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 110 van maximaal 110 zijnde 100.0%

**Basisregistratie Ondergrond (BRO)**
De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 84.5 van maximaal 90 zijnde 94.0%

# Resultaten en vervolg

Gebleken is dat gemeente Alblasserdam over het algeheel voldoende scoort in de zelfevaluaties en verantwoording aan het Rijk. Verbeterpunten en aandachtspunten zijn opgenomen in specifieke verbeterplannen en/of het strategische Regio Drechtsteden informatiebeveiligingsplan 2022.

De verantwoording op het gebied van informatieveiligheid en privacy is een jaarlijks terugkerend proces als onderdeel van de Plan-DO-Check-Act (PDCA-) cyclus. In de vernieuwde rapportagelijn zal er, zoals eerder gecommuniceerd, periodiek een update gecommuniceerd worden over de status van informatieveiligheid. En natuurlijk ook indien er eerder urgent relevante ontwikkelingen zijn.