BERgeijkLEEF

Bourgondisch, bruisend en groen

Verantwoordingsrapportage ENSIA 2024

Informatiebeveiliging – BIO

Digid, Suwinet, BRP, PUN, BAG, BGT en BRO

GEMEENTE BERGEIJK 04-02-2024

Leeswijzer

Sinds 2017 leggen gemeenten verantwoording af over informatiebeveiliging via ENSIA (Eenduidige Normatiek Single Information Audit). ENSIA is het verantwoordingsstelsel voor informatiebeveiliging, waarmee gemeenten via zelfevaluatie controleren of de inrichting van de gemeentelijke informatiebeveiliging overeenkomt met de normen en maatregelen uit de BIO (Baseline Informatiebeveiliging Overheid).

Daarnaast verantwoorden gemeenten zich via ENSIA over specifieke normen betreffende DigiD (Digitale persoonsidentificatie), Suwinet (Structuur uitvoeringsorganisatie werk en inkomen) en de basisregistraties BRP (Basisregistratie Personen), PUN (Reisdocumenten), BAG (Basisregistratie Adressen en Gebouwen), BRO (Basisregistratie Ondergrond) en BGT (Basisregistratie Grootschalige Topografie).

Deze rapportage is opgesteld op basis van ENSIA 2024. De rapportage is een samenvatting van het geheel aan ENSIA rapportages over de mate waarin voldaan wordt aan eisen uit de BIO, DigiD, Suwinet, BRP, PUN, BAG, BRO en BGT. De rapportage is als volgt opgebouwd:

STATUS INFORMATIEBEVEILIGING (BIO)

- Bestuurlijke uitgangspunten
- Samenvatting van 5 thema's (groepering van 18 BIO hoofdstukken):
    - Beleid en organisatie
    - Toegangsbeveiliging
    - Continuïteit en incidenten
    - Informatiesystemen
    - Databescherming

BEOORDELING

Er is uitgegaan van een schaal met 3 categorieën:

onvoldoende voldoende goed

VERANTWOORDING AAN DE LANDELIJKE TOEZICHTHOUDER UIT ENSIA

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

ENSIA | Eenduidige Normatiek Single Information Audit

Groepering op thema: Verdeling van maatregelen BIO in bouwstenen

Totaal 180 maatregelen

BIO Hoofdstuk		Aantal maatregelen	Groepering op thema	Totaal aantal maatregelen	
H5	Informatiebeveiligingsbeleid	2	**1. BELEID EN ORGANISATIE**	20	180
H6	Organiseren van informatiebeveiliging	10			
H7	Veilig personeel	8			
H9	Toegangsbeveiliging	25	**2. TOEGANGSBEVEILIGING**	45	
H11	Fysieke beveiliging en beveiliging van de omgeving	20			
H16	Beheer van informatiebeveiligingsincidenten	14	**3. CONTINUÏTEIT EN INCIDENTEN**	30	
H17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	6			
H18	Naleving	10			
H12	Beveiliging bedrijfsvoering	30	**4. INFORMATIESYSTEMEN**	54	
H14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	12			
H15	Leveranciersrelaties	12			
H8	Beheer van bedrijfsmiddelen	14	**5. DATABESCHERMING**	31	
H10	Cryptografie	4			
H13	Communicatiebeveiliging	13			

Bouwstenen

Beschrijving van de groepering van de BIO hoofdstukken op thema

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van de gemeente Bergeijk:

- Volgt informatiebeveiligingsbeleid op basis van de BIO, het overheidsbrede normenkader voor informatiebeveiliging.
- Zorgt ervoor dat de juiste activiteiten ten aanzien van informatiebeveiliging door de gemeentelijke organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

De hele organisatie heeft een verantwoordelijkheid voor informatiebeveiliging. Op basis van risicomanagement worden risico's en gevolgen in kaart gebracht, maatregelen getroffen en geëvalueerd om informatiestromen te beheersen en het risico op incidenten te verkleinen.

1. BELEID EN ORGANISATIE
H5 / H6 / H7

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- De informatiebeveiligingsorganisatie is geregeld; zowel voor, tijdens als na het dienstverband.
- Medewerkers gaan bewust om met informatie

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.

2. TOEGANGSBEVEILIGING
H9 / H11

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Medewerkers hebben de juiste toegangsrechten / autorisaties (fysiek en digitaal)
- Medewerkers gaan zorgvuldig om met toegang tot informatie (wachtwoorden)

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 de omgeving en toegang tot de (digitale) informatievoorziening.

Bouwstenen

Beschrijving van de groepering van de BIO hoofdstukken op thema

3. CONTINUÏTEIT EN INCIDENTEN
H16 / H17 / H18

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

De gemeente levert diensten aan inwoners en bedrijven. De gemeente neemt maatregelen om continuïteit hiervan te waarborgen. In geval van een incident zijn er plannen beschikbaar om de dienstverlening zo snel mogelijk te kunnen hervatten. Ook worden incidenten en de naleving ervan vastgelegd om herhaling ervan in de toekomst te voorkomen.

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.

De gemeente wisselt op veel verschillende manieren informatie uit, met verschillende ketenpartners. Medewerkers moeten over de juiste hardware, informatiesystemen en kanalen voor informatie-uitwisseling beschikken om dit op een veilige manier te doen. De gemeente richt hier maatregelen voor in.

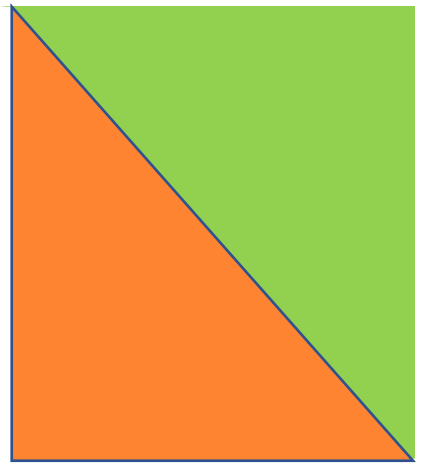
Status informatiebeveiliging BIO

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

Het bestuur van de gemeente Bergeijk:

- Volgt informatiebeveiligingsbeleid op basis van de BIO, het overheidsbrede normenkader voor informatiebeveiliging.
- Zorgt ervoor dat de juiste activiteiten ten aanzien van informatiebeveiliging door de gemeentelijke organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

De gemeente probeert haar informatie en informatiesystemen zo goed mogelijk te beschermen tegen onbevoegde wijziging, inzage of onderbreking van de werking ervan; om de bedrijfsprocessen en dienstverlening te waarborgen. Uit de zelfevaluatie van de BIO blijkt dat de gemeente Bergeijk haar informatiebeveiliging redelijk op orde heeft. Daarbij is niet alleen aandacht voor technische maatregelen waarmee incidenten voorkomen of opgelost kunnen worden, maar ook voor organisatorische procedures en bewustwording onder medewerkers. Een algemeen punt van aandacht is periodieke en systematische controle en bijsturing op de inrichting van beleid, procedures en maatregelen.



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

1. BELEID EN ORGANISATIE

Status:
Goed

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

Onderdelen:

onvoldoende voldoende goed

H5 / Informatiebeveiligingsbeleid	
H6 / Organiseren van informatiebeveiliging	
H7 / Veilig personeel	

Toelichting

De gemeente beschikt over een actueel informatiebeveiligingsbeleid. Rollen en verantwoordelijkheden zijn vastgelegd. Informatiebeveiliging is nog onvoldoende geborgd in dagelijkse werkzaamheden en projecten. Om urgentiebesef, kennis en kunde te vergroten in de organisatie, is er kempenbreed een bewustwordingsplatform; Digibewust de Kempen aangeschaft. Digibewust de Kempen is in het vierde kwartaal van 2024 gestart. Vanuit dit platform wordt ieder kwartaal informatiebeveiliging onderwerpen behandeld en getoetst. Nieuwe medewerkers krijgen in de eerste werkweek een kennismaking met het privacy en informatiebeveiliging team van Bergeijk en alles wat men moet weten over de richtlijnen bij gemeente Bergeijk over privacy en informatieveiligheid.

Verbeteracties

→ Eisen voor informatiebeveiliging, privacy en informatiebeheer opnemen bij inkoop.

→ Actualiseren van het informatiebeveiligingsbeleid. Aanleiding is de geplande inwerkingtreding van de Cyberbeveiligingswet per derde kwartaal 2025.

2. TOEGANGSBEVEILIGING

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

Status:
Goed

Onderdelen:

onvoldoende voldoende goed

H9 / Toegangsbeveiliging	
H11 / Fysieke beveiliging en beveiliging van de omgeving	

Toelichting

Er is sprake van 2 soorten toegangsbeveiliging: beveiliging van digitale systemen en fysieke beveiliging van de informatie in het gebouw. Er is een beleid voor zowel fysieke als logische (digitale) toegangsbeveiliging vastgesteld. In het beleid en onderliggende procedures is aandacht voor functiescheiding en autorisaties binnen informatiesystemen zodat informatie beveiligd is tegen onbevoegde inzage.
Op het gebied van digitale beveiliging wordt toegang en autorisatie voor informatiesystemen toegekend op basis van functieprofiel. Er is ook een vastgestelde procedure voor het aan- en afmelden van gebruikers. Er wordt jaarlijks ook controle uitgevoerd op de bestaande accounts en toegang tot systemen. Autorisaties binnen systemen zijn nog een punt van aandacht. Het is belangrijk om inzicht te hebben in toegang tot bepaalde informatie; mede omdat in bepaalde systemen logging (technisch) nog niet mogelijk is. Apparatuur is beveiligd op basis van beleid voor mobiele apparatuur. Er wordt standaard gewerkt met apparatuur waar lokaal geen data wordt opgeslagen en/of bewerkt. Alleen geautoriseerde apparatuur krijgt toegang tot het netwerk. In 2024 is op basis van een geactualiseerd wachtwoordbeleid de wachtwoordenmanager, MindYourPass, met verplichte training uitgerold.

Verbeteracties

→ Het afdwingen van MindYourPass op basis van het in het wachtwoordbeleid onderkende gecategoriseerde informatiesystemen.
→ Periodieke controle van autorisaties binnen systemen inrichten, naast controle van accounts en toegang tot systemen.

3. CONTINUÏTEIT EN INCIDENTEN

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

Status: Voldoende

Onderdelen: onvoldoende voldoende goed

H16 / Beheer van beveiligingsincidenten	Voldoende
H17 / Bedrijfscontinuïteitsbeheer & informatiebeveiliging	Voldoende
H18 / Naleving	Voldoende

Toelichting

Medewerkers melden beveiligingsincidenten bij het Privacy & Informatiebeveiliging Team (PIT) Bergeijk (CISO en Privacy Officer). De beveiligingsincidenten en de opvolging hiervan, zowel op technisch als organisatorisch gebied, worden vastgelegd ter verantwoording en verbetering. Hierover gerapporteerd aan het management. Het bewust handelen en bewust zijn van informatieveilig handelen vraagt om continue aandacht. Hiervoor zijn in 2024 bewustwordingsacties uitgezet via een maandelijkse campagne en gerichte mailings.

Om de continuïteit van dienstverlening en bedrijfsvoering te borgen bij cyberincidenten, zijn er technische continuïteitsplannen beschikbaar. Organisatorisch waren er nog geen plannen beschikbaar. Er is een crisisplan cyberincidenten ontwikkeld en vastgesteld voor de Kempengemeenten, GRSK en Kempenplus, om in geval van een aanval op de Kempen-infrastructuur snel en efficiënt te kunnen handelen. In 2025 worden, aanvullend op het crisisplan, bedrijfscontinuïteitsplannen uitgewerkt voor de kritische bedrijfsapplicaties.

Verbeterpunten

→ Opstellen van een uitgewerkt BCM (bedrijfscontinuïteit management) – plan.

4. INFORMATIESYSTEMEN

Veilige omgang met informatiesystemen en afspraken hierover maken met onze leveranciers

Status:
Goed

Onderdelen:

onvoldoende voldoende goed

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

Toelichting

De gemeente ontwikkelt zelf geen nieuwe software. Bij de inkoop van software worden eisen gesteld aan de leverancier op het gebied van informatiebeveiliging. Er wordt gebruik gemaakt van landelijke standaard inkoopvoorwaarden (GIBIT) waarin rekening wordt gehouden met informatiebeveiligingseisen. Indien er sprake is van verwerking van persoonsgegevens wordt een verwerkersovereenkomst afgesloten.
Implementatie van nieuwe software of wijzigingen van bestaande functionaliteiten wordt gedaan aan de hand van vastgestelde procedures. Voor bedrijfs-kritische systemen wordt jaarlijks een audit (TPM) opgevraagd.
Het SSC voert tevens werkzaamheden uit om onbeveiligde toegang tot gemeentelijke informatie te voorkomen in de vorm van maatregelen tegen malware (o.a. virusscanners en blokkeren van verdachte sites) en uitvoeren van herstelwerkzaamheden bij kwetsbaarheidsmeldingen. Logging binnen systemen is een punt van aandacht. Voor zover mogelijk voldoen logregels aan de gestelde eisen, maar niet alle applicaties hebben logfunctionaliteiten.

Verbeterpunten

→ Volgen ontwikkeling logfunctionaliteiten in gemeentelijke informatiesystemen (actie vanuit leveranciers)

5. DATABESCHERMING

Veilige omgang met data in onze software

Status:
Voldoende

Onderdelen:

onvoldoende voldoende goed

H8 / Beheer van bedrijfsmiddelen	
H10 / Cryptografie	
H13 / Communicatiebeveiliging	

Toelichting

Het werken met mobiele apparatuur van de gemeente wordt geborgd met de uitleverklaring en de bruikleenovereenkomst die medewerkers tekenen bij ontvangst van de mobiele apparatuur. Hiermee hebben medewerkers een kader voor het veilig gebruik van gemeentelijke apparatuur en de gemeentelijke informatie die op deze apparatuur verwerkt wordt. Voor veilige uitwisseling van elektronische informatie maken we als gemeente gebruik van veilige verbindingen, zoals Digikoppeling en PKIoverheidcertificaten. Ook is scheiding van netwerken ingericht. Medewerkers werken in een beveiligde netwerkomgeving, waardoor de gemeentelijke informatie is beschermd tegen toegang van buitenaf. Er zijn al verschillende cryptografische maatregelen getroffen om veilig informatie uit te wisselen. Algemeen cryptografiebeleid, waarin moet worden opgenomen op welke manier de gemeente cryptografie inzet, wie verantwoordelijk is voor implementatie en op welke wijze het beschermingsniveau moet worden vastgesteld.

Verbeterpunten

→ Vaststellen cryptografiebeleid.

Getoetste collegeverklaring ENSIA - DIGID

Status: Voldoet

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. De gemeente Bergeijk heeft twee DigiD-aansluitingen.

Shift2	Inwoners kunnen digitaal aanvragen doen via de website na identificatie via DigiD.	
iBurgerzaken	Inwoners kunnen digitaal aanvragen doen bij de gemeente op het gebied van burgerzaken in de applicatie iBurgerzaken, zoals het doorgeven van verhuizing, geboorte, overlijden en huwelijk.	

De DigiD-aansluitingen worden jaarlijks getoetst op opzet en bestaan aan de hand van een normenset. Nieuw is dat de aansluiting in 2024 ook op een aantal normen in getoetst op de werking. De leverancier levert hiervoor een TPM verklaring aan de gemeente.

Uit de audit is gebleken dat wij voldoen aan alle gestelde normen.

Getoetste collegeverklaring ENSIA - Suwinet

Status:
Goed

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 (Uitvoeringsinstituut Werknemersverzekeringen (UWV), Sociale Verzekeringsbank (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.

onvoldoende goed

Participatiewet/IOAZ/IOAW - Suwinet Inkijk - DKD Inlezen	Voor de uitvoering van taken met betrekking tot de participatiewet en bijzondere bijstand wordt gebruik gemaakt van Suwinet. Taken zijn belegd bij het samenwerkingsverband Kempenplus

KempenPlus en de Gemeenschapelijke Regeling Kempengemeenten zijn verantwoordelijk voor het opzetten en implementeren van interne beheersmaatregelen ter waarborging van de vertrouwelijkheid van Suwinetgegevens die worden verwerkt voor de gemeenten. De interne beheersmaatregelen voor het veilig gebruik van Suwinetvoorzieningen zijn daarbij leidend.

De auditor heeft geconstateerd dat de opgenomen interne beheersmaatregelen volgens de criteria in alle materiële opzichten effectief zijn en daarmee voldoen.

Status Basisregistratie Personen en Reisdocumenten

Status:
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.

Goed

onvoldoende goed

Basisregistratie Personen (BRP)
De zelfevaluatie BRP over het jaar 2024 is afgerond met een score van 1160 van maximaal 1200 zijnde 96,7%

Goed

Wet- en regelgeving voor Reisdocumenten
De zelfevaluatie Reisdocumenten over het jaar 2024 is afgerond met een score van 751 van maximaal 800 zijnde 93,9%

Goed

De gemeente voldoet in grote mate aan de maatregelen betreffende de BRP en reisdocumenten. De geformuleerde verbeterpunten op het gebied van interne controle zullen in 2025 worden opgepakt.

Status GEO-basisregistraties

Status: Voldoet

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

Basisregistratie Adressen en Gebouwen (BAG)
De zelfevaluatie BAG over het jaar 2024 is afgerond met een score van 84%; Norm 75%

Basisregistratie Grootschalige Topografie (BGT)
De zelfevaluatie BGT over het jaar 2024 is afgerond met een score van 88%; Norm 75%

Basisregistratie Ondergrond (BRO)
De zelfevaluatie BGT over het jaar 2024 is afgerond met een score van 71%; Norm 60%

BAG: In 2024 zijn de achterstanden op de mutaties ingehaald. Focus voor 2025 ligt op het blijven borgen van de werkwijze en mogelijke verbeteringen door te voeren.
BGT: Focus voor 2025 ligt op het blijven borgen van de werkwijze en mogelijke verbeteringen door te voeren.
BRO: Verbeterpunt zit op het borgen van het proces. BRO dient meer aandacht te verkrijgen vanuit van de totale organisatie. Dit wordt in 2025 opgepakt.