Openbaar Zaaknummer: Z/24/232322

Informatienota voor de Gemeenteraad

Onderwerp: ENSIA 2023: Stand van zaken informatieveiligheid gemeente Wijchen 2023 door CISO

Datum: 9 april 2024

Kernboodschap

Het college van burgemeester en wethouders van de gemeente Gemeente Wijchen legt over het jaar 2023 verantwoording af over de stand van zaken op het gebied van informatieveiligheid binnen de gemeentelijke organisatie. Dit gaat op basis van de landelijke en voor gemeenten verplichte Eenduidige Normatiek Single Information Audit (ENSIA) systematiek. We leggen verantwoording af aan de gemeenteraad (horizontale verantwoording) en aan de verschillende toezichthouders (verticale verantwoording).

Eerdere besluiten

Datum	**Korte omschrijving eerder genomen besluit (vermeld zo mogelijk het zaaknummer/documentnummer)**
Tot 2023	In voorgaande jaren werden de ENSIA-stukken onder geheimhouding aangeboden. Dit jaar is de rapportage vanuit de CISO openbaar en liggen de geheime stukken waarmee de gemeente verantwoording aflegt aan de rijksoverheid indien gewenst ter inzage bij de Griffie.

Toelichting

De ENSIA-verantwoording voor het jaar 2023 gaat over onderstaande onderdelen:

- Implementatie van de Baseline Informatiebeveiliging Overheid (BIO) - Zelfevaluatie
- Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet) – Geauditeerde zelfevaluatie
- Digitale Persoonsidentificatie (DigiD) – Geauditeerde zelfevaluatie
- Basis Registratie Personen (BRP) - Zelfevaluatie
- Paspoort Uitvoeringsregeling Nederland (PUN) - Zelfevaluatie
- Basisregistratie Grootschalige Topografie (BGT) - Zelfevaluatie op datakwaliteit
- Basisregistratie Adressen en Gebouwen (BAG) - Zelfevaluatie op datakwaliteit
- Basisregistratie Ondergrond (BRO) - Zelfevaluatie op datakwaliteit.

ENSIA-verantwoording

Onderstaande tabellen geven per ENSIA-onderdeel een korte toelichting, bevindingen en de stand van zaken weer. Voor de leesbaarheid is per onderdeel met behulp van kleuren de algemene status weergegeven.

Legenda:

Ruim voldoende tot goed	***Voldoende***	***Net onvoldoende***	***Onvoldoende***
Het onderdeel is volledig op orde, in control Mogelijk zijn er minimale verbeterpunten	Het onderdeel is globaal op orde, in control Er zijn enkele verbeterpunten	Het onderdeel is net niet in control Er zijn meerdere verbeterpunten	Het onderdeel is niet in control Er zijn veel verbeterpunten, bijsturing is nodig

Verantwoording per ENSIA-stelsel
De onderstaande tabel geeft per stelsel (domein) een korte toelichting, bevindingen en de stand van zaken weer.

ENSIA-stelsel	Toelichting, bevindingen en stand van zaken	Status
Implementatie BIO Baseline Informatiebeveiliging Overheid	Om op het gebied van informatieveiligheid weerbaar te blijven volgen we de landelijke Baseline Informatiebeveiliging Overheid (BIO). Deze BIO is het normenkader waarbij we op basis van een eigen risico-afweging keuzes maken in het implementeren van beheers- en beveiligingsmaatregelen. Hierbij blijft een basispakket aan generieke maatregelen voor iedere (overheid)organisatie verplicht. Het strategisch informatiebeveiligingsbeleid is geldig tot 2024 en in lijn met de voor overheden verplichte landelijke Baseline Informatiebeveiliging Overheid (BIO). Deze BIO bestaat uit het implementeren van technische- en organisatorische maatregelen waarvan ook een stuk privacy-borging in het kader van de Algemene Verordening Gegevensbescherming afhankelijk is. Het beleid geeft onze organisatie kaders en richting om op het gebied van informatieveiligheid weerbaarder te worden en dat ook te blijven. Het vertalen van beleid naar de implementatie en uitvoering van maatregelen vraagt om een gedegen en voor veel onderdelen langdurig traject, omdat het vaak de werkwijze binnen organisatieprocessen beïnvloedt. In het kader van informatieveiligheid is onze menselijke verdedigingslinie een van de belangrijkste. Hierbij werken we continu aan bewustwording op het gebied van informatiebeveiliging en privacy bij onze medewerkers. Hierover	***Voldoende***

ENSIA-stelsel	Toelichting, bevindingen en stand van zaken	Status
	worden alle medewerkers geïnformeerd en hiervoor volgen alle medewerkers een bewustwordingsprogramma vanaf 2024. De organisatie van informatiebeveiliging en privacy is ingericht met centrale functies zoals de Chief Information Security Officer en een Functionaris Gegevensbescherming. Daarnaast zijn er een aantal adviserende functies zoals privacy ambassadeurs en beveiligingsbeheerders. Specifiek gekeken naar de borging van informatieveiligheid over het geheel gezien scoren we ons zelf op een voldoende. Deze score komt voort uit resultaten van onder andere de verschillende ENSIA-onderdelen waaronder een externe audit. Informatieveiligheid heeft altijd aandacht nodig, het is een continu proces wat steeds meer in ons DNA komt te zitten, Alleen zo kunnen we de veranderingen in wetgeving opvangen, de verschillende aanvallen van buitenaf weerstaan en weerbaar blijven. Betrouwbare medewerkers zijn een belangrijke schakel op het gebied van informatieveiligheid. Daarom vragen we waarborgen aan nieuwe medewerkers en externen. Voorbeelden hiervan zijn de Verklaring Omtrent Gedrag (VOG), integriteit- en geheimhoudingsverklaringen en afspraken in overeenkomsten met (keten)partners. Rondom ongewenste en hiermee onbevoegde toegang ontstaan de meeste informatiebeveiligingsincidenten. Toegang gaat naast digitale toegang tot onze informatievoorziening ook over fysieke toegang tot gebouwen en (beveiligde) ruimten. Het proces in- en uitdienst is in de basis op orde. Hiermee is toegang tot onze voordeur (zowel digitaal als fysiek) geregeld. Ransomware is wereldwijd een van de grootste cyberdreigingen. Cybercriminelen komen relatief eenvoudig binnen door bijvoorbeeld een geslaagde Phishing-actie. De impact van een geslaagde Ransomware-aanval is ontzettend groot. Landelijke voorbeelden laten zien dat organisaties die getroffen zijn door ransomware maanden tot jaren nodig hebben om weer volledig operationeel te zijn. De processen voor de afhandeling van beveiligingsincidenten en bedrijfscontinuïteit zijn in de basis op orde. Databescherming gaat voornamelijk over de integriteit en vertrouwelijkheid van gegevens. "De juiste informatie op het juiste moment bij de juiste persoon". Deze data zitten in ontzettend veel en verschillende systemen zoals vak-applicaties, basisregistraties,	

ENSIA-stelsel	Toelichting, bevindingen en stand van zaken	Status
	Zaaksysteem, netwerkmappen, websites en het e-mailsysteem. Binnen al deze omgevingen moet data geclassificeerd worden op beschikbaarheid, integriteit en vertrouwelijkheid. Vanwege de complexiteit en hoeveelheid aan werk vraagt het invoeren een meerjarenaanpak. De AVG schrijft voor dat (persoons)gegevens moeten zijn afgeschermd als deze niet direct nodig zijn voor het uitvoeren van werkzaamheden. Dit is het "Need to Know"-principe. Het afschermen van gegevens in informatiesystemen gaat op basis van dataclassificatie en rechtentoekenning.	
Suwinet Structuur uitvoeringsorganisatie Werk en Inkomen	Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet, Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers, Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen en Wet gemeentelijke schuldhulpverlening. Voor de regiogemeenten Druten, Beuningen en Berg en Dal voeren wij werkzaamheden uit op het gebied van Bijzonder Onderzoek. Voor de uitvoering van deze taken wordt gebruik gemaakt van Suwinet-Inkijk en DKD-Inlezen. Vanwege de hoeveelheid en gevoeligheid van (persoons)gegevens binnen Suwinet is bepaald dat iedere gemeente naast de zelfevaluatie ook extern getoetst wordt op naleving van het normenkader. Het uitvoeren van de audit voor Suwinet is een vereiste van de Regeling SUWI. Het onderzoek van de externe auditor geeft aan dat de gemeente Wijchen voldoet aan de wettelijk gestelde eisen en normen in het kader van informatieveiligheid rondom het gebruik en beheer van alle Suwinet-aansluitingen.	***Voldoende***
DigiD Digitale Persoonsidentificatie	DigiD is voor inwoners de manier om zichzelf digitaal te identificeren. DigiD wordt gebruikt voor iBurgerzaken en e-formulieren. Onvoldoende of onjuist beheer van een DigiD-aansluiting kan grote gevolgen hebben voor de landelijke keten en uiteindelijk persoonsinformatie van inwoners. Daarom heeft de toezichthouder bepaald dat iedere DigiD-aansluiting naast een jaarlijkse zelfevaluatie ook (extern) getoetst wordt op naleving van het normenkader. Het onderzoek van de externe auditor geeft aan dat onze processen rondom DigiD op orde zijn. Wij voldoen aan de gestelde informatiebeveiligingsnormen. Naast het onderzoek rondom organisatorische waarborgen heeft er ook een technische penetratietest plaatsgevonden. Ook deze uitkomst is positief, er	***Ruim voldoende tot goed***

ENSIA-stelsel	Toelichting, bevindingen en stand van zaken	Status
	zijn geen kwetsbaarheden ontdekt. De veiligheid van DigiD en websites staat onder druk. Het landelijke dreigingsbeeld geeft aan dat digitale risico's onverminderd groot zijn en cyberaanvallen steeds meer succesvol zijn met alle gevolgen van dien. De beveiliging vraagt steeds meer aandacht waarbij het een uitdaging is om dit huidige niveau vast te houden.	
BRP Basis Registratie Personen	BRP is de basisregistratie waarin alle inwoners zijn geregistreerd. Gemeenten beheren deze BRP voor hun inwoners. Uiteindelijk worden alle BRP-registraties landelijk gekoppeld, zodat overheidsinstanties, zorgverleners en andere dienstverleners die gebruik mogen maken van deze BRP beschikken over de juiste persoonsinformatie. Vanwege het grote landelijke belang rondom de BRP zijn gemeenten verplicht om jaarlijks een zelfevaluatie uit te voeren. ***Bestandscontrole op de persoonslijsten.*** Bij de bestandscontrole in de Basisregistratie personen van 2023 is 100% van de actuele persoonslijsten correct bevonden. Dit is in lijn met eerdere jaren, waarin de score steeds nagenoeg hetzelfde positieve resultaat liet zien. Dit voldoet ruimschoots aan de landelijke norm.	***Ruim voldoen de tot goed***
PUN Paspoort Uitvoeringsregeling Nederland	Gemeenten verzorgen de aanvraag en het uitreiken van reisdocumenten voor hun inwoners. Reisdocumenten zijn erg waardevol en vaak de sleutel tot identiteitsfraude. De processen rondom het aanvragen en uitreiken zijn daarom strikt. De burgemeester is verantwoordelijk voor de borging van deze processen en moet hierover jaarlijks verantwoording afleggen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties. Via de ENSIA-verantwoording infomeren we ook het eigen bestuur over de stand van zaken. De zelfevaluatie PUN over het jaar 2023 is afgerond met een score van 100% Dit is een goed eindresultaat. Vorig jaar was de score eveneens 100%. Processen en de uitvoering rondom het aanvragen, beheren en uitreiken van reisdocumenten zijn op orde.	***Ruim voldoen de tot goed***
BAG Basisregistratie Adressen en Gebouwen	De BAG bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Kopieën van al deze gegevens zijn verzameld in een landelijke voorziening. Deze voorziening wordt landelijk gebruikt door overheden, organisaties en particulieren. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BAG. De zelfevaluatie BAG over het jaar 2023 is afgerond met een score van 100%. Hiermee voldoen we evenals vorig jaar ruim aan de landelijk gestelde norm van minimaal 75%. Vorig jaar was de	***Ruim voldoen de tot goed***

ENSIA-stelsel	Toelichting, bevindingen en stand van zaken	Status
	score eveneens 100%. De huidige processen borgen dat de gemeente voldoet aan de gestelde eisen. Waakzaamheid blijft uiteraard geboden, vooral met de invoering Omgevingswet.	
BGT Basisregistratie Grootschalige Topografie	De BGT is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd. Kortom: de inrichting van de fysieke omgeving. De BGT is een landelijk uniforme registratie die alleen gemaakt kan worden vanuit een goede samenwerking tussen de diverse bronhouders. Gemeenten zijn als bronhouder medeverantwoordelijk voor de kwaliteit van deze landelijke basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BGT. De BGT is gegenereerd uit de geometrische databron Kernregistratie Topografie (KRT) voor haar informatie. De KRT is een interne databron binnen onze organisatie waarin alle geografische objecten van de gemeente Wijchen zijn geregistreerd. De KRT is leverancier van data naar de overige basisregistraties BAG, BGT en de BRO, waarbij wordt voldaan aan de wet- en regelgeving. De zelfevaluatie BGT over het jaar 2023 is afgerond met een score van 97%. Hiermee voldoen we ruim aan de landelijk gestelde norm van minimaal 75%. Vorig jaar was de score 95%.	***Ruim voldoen de tot goed***
BRO Basisregistratie Ondergrond	De BRO bevat bodem- en ondergrondgegevens. Het gebruik van deze gegevens is de laatste decennia sterk toegenomen. Een goede informatievoorziening over de ondergrond is van wezenlijk belang voor het realiseren van bestuurlijke ambities als het omgevingsplan, de energietransitie, watertoets en dergelijke. Als we willen dat onze inwoners hier ook actief in participeren, moet het fundament hiervoor op orde en goed ingevuld zijn. De BRO is een van de elementen die de verschillende opgaves mogelijk moeten maken. De gemeente is bronhouder voor deze basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BRO. De zelfevaluatie BRO over het jaar 2023 is wederom positief afgerond met een score van 89%. Hiermee voldoen we nog steeds ruim aan de landelijk gestelde norm van minimaal 60%. Vorig jaar was de score zelfs 100%.	***Ruim voldoen de tot goed***