Gemeente Asten

Jaarverslag Informatiebeveiliging 2021

Bezoekadres Koningsplein 3 | 5721 GJ Asten
Postadres Postbus 290 | 5720 AG Asten
T (0493) 671 212 | F (0493) 671 213
www.asten.nl | gemeente@asten.nl

Titel:	Jaarverslag Informatiebeveiliging 2021
Versie:	0.2
Datum:	20 april 2022
Auteur(s):	I.M.C. Mekers

Inhoudsopgave

1. Inleiding

Voor u ligt het Jaarverslag Informatieveiligheid 2021 van de gemeente Asten. Met dit jaarverslag legt het college van B&W over het jaar 2021 verantwoording af aan de raad over de stand van zaken betreffende informatiebeveiliging.

Informatiebeveiliging staat onder druk en het aantal dreigingen blijft toenemen. Verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of wijzigen van informatie kan impact hebben op de bedrijfsvoering. Daarnaast hebben incidenten mogelijk ook negatieve gevolgen voor inwoners, bedrijven en partners. Informatieveiligheid is dus van groot belang!

Gemeente Asten wil een betrouwbare partner zijn voor haar inwoners, bedrijven en (keten)partners. Daarom is ons doel:

- Dat de gemeente 'in control' is als het gaat om dreigingen, incidenten, wijzigingen, processen en organisatie.
- Dat de dienstverlening ongestoord en betrouwbaar verloopt.
- Dat gegevens van onze inwoners, bedrijven, instellingen en medewerkers veilig zijn.
- Dat onze medewerkers privacy- en beveiligingsbewust zijn en beschikken over de juiste middelen om hun verantwoordelijkheid voor informatiebeveiliging en privacy te dragen.

1.1 Leeswijzer

Dit jaarverslag begint met de verplichte verantwoording over informatiebeveiliging volgens de ENSIA systematiek. Vervolgens wordt teruggeblikt op 2021 en een doorkijk gegeven naar 2022.

2. Resultaten ENSIA verantwoording over 2021

Via de ENSIA-systematiek[1] legt het college van B&W jaarlijks verantwoording af over de status van informatiebeveiliging aan het Rijk. De scope van ENSIA omvat:

- Zelfevaluatie Baseline Informatiebeveiliging Overheid (BIO).
- Zelfevaluatie Basisregistratie Personen (BRP) en Reisdocumenten.
- Zelfevaluatie DigiD en Suwinet.
- Zelfevaluatie GEO-informatiedomein: Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en Waardering Onroerende Zaken (WOZ).

Naast de zelfevaluaties kent de ENSIA-verantwoording over 2021 twee audits die door een externe auditor zijn uitgevoerd, namelijk over DigiD en Suwinet. In de volgende paragrafen wordt per zelfevaluatie een toelichting gegeven. De bij de zelfevaluaties behorende rapportages zijn als bijlagen opgenomen bij dit jaarverslag.

2.1 Zelfevaluatie BIO

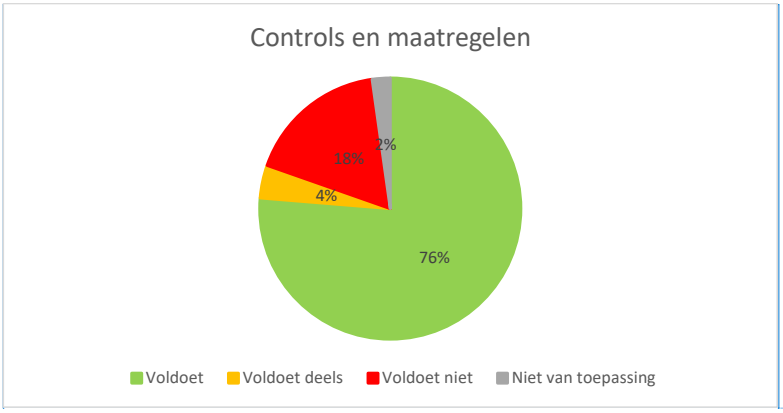
De BIO is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging en heeft risicomanagement als uitgangspunt. Dit betekent dat maatregelen genomen worden die passen bij de daadwerkelijke risico's. Immers, 100% veiligheid is nooit mogelijk vanwege het tempo van technische ontwikkelingen en de menselijke factor.

De BIO bestaat uit controls op 14 gebieden, bijvoorbeeld toegangsbeveiliging en beheer van bedrijfsmiddelen. Een deel van deze controls is uitgewerkt in verplichte maatregelen, omdat zij:

- Voortvloeien uit wet- en regelgeving.
- Zo basaal zijn dat zij het fundament vormen van een betrouwbare c.q. professionele informatievoorziening.
- Dienstbaar zijn aan de beveiliging in een procesketen of netwerk.

In de volgende figuur worden de resultaten uit de zelfevaluatie getoond.

[1] Eenduidige Normatiek Single Information Audit, voor meer informatie zie www.ensia.nl.



Voldoen aan meer controls en maatregelen gaat onder andere gerealiseerd worden door het oppakken van iBewustzijns-trainingen en door de geplande overgang naar ICT NML.

Met opmerkingen [IM1]: Aanpassen aan laatste stand van zaken (obv Excel bestand).

Met opmerkingen [IM2]: Herschrijven

2.2 Zelfevaluaties BRP en Reisdocumenten

De BRP is onderdeel van het stelsel van basisregistraties van de Nederlandse overheid. De Nederlandse overheid registreert persoonsgegevens in de BRP. Alle overheidsinstellingen en bestuursorganen zijn verplicht voor hun taken gebruik te maken van die gegevens. Voor het uitgeven van reisdocumenten hebben gemeenten met betrekking tot. wetgeving te maken met de Paspoortuitvoeringsregeling Nederland 2001 (PUN).

Jaarlijks moeten gemeenten verantwoording afleggen over het gebruik van de BRP en de PUN. Het inhoudelijke deel, dat onder andere kijkt naar de kwaliteit van de persoonsgegevens in het BRP en de inrichting van de verwerkingsprocessen, wordt door de vakafdeling uitgevoerd en is geen onderdeel van dit jaarverslag. Het beveiligingstechnische deel is op basis van de BIO-richtlijnen uitgevraagd.

2.2.1 BRP

Aan de hand van de vragenlijst is de zelfevaluatie BRP uitgevoerd. Op grond daarvan is de verantwoordingsrapportage[2] opgesteld die door het college van B&W is vastgesteld. De zelfevaluatie BRP levert een puntenscore op van 1.160 uit het maximaal aantal te behalen punten van 1.200. Deze score is te beoordelen als zeer goed.

2.2.2 Reisdocumenten

Aan de hand van de vragenlijst is de zelfevaluatie Reisdocumenten uitgevoerd. Op grond daarvan is de verantwoordingsrapportage[3] opgesteld die door het college van B&W is vastgesteld. De zelfevaluatie Reisdocumenten levert een puntenscore op van 1.170 uit het maximaal aantal te behalen punten van 1.200. Deze score is te beoordelen als zeer goed.

[2] Uittreksel BRP (ENSIA)
[3] Uittreksel Reisdocumenten (ENSIA)

2.3 Zelfevaluatie DigiD en Suwinet

De verantwoording aan de toezichthouder is gebeurd via een collegeverklaring[4] en bijlagen[5] in voorgeschreven format. Onze externe auditor heeft deze verantwoording beoordeeld en gewaarmerkt. Daarnaast heeft hij een assurance-rapport opgesteld waarin staat dat de verklaring een juist beeld geeft van de werkelijkheid.

2.3.1 DigiD

Gemeente Asten is DigiD aansluithouder. De DigiD aansluiting wordt gebruikt voor authenticatie voor bijvoorbeeld melden voorgenomen huwelijk en aangifte van verhuizing. Over 2021 heeft onze externe IT-auditor een audit uitgevoerd op het gebruik van DigiD en geconstateerd dat gemeente Asten aan het normenkader voldoet.

2.3.2 Suwinet

Suwinet is het systeem voor informatie-uitwisseling in de keten van werk en inkomen. De SUWI Verantwoordingsrichtlijn is het normenkader waaraan de beveiliging van Suwinet moet voldoen.

Gemeenschappelijke regeling Senzer
De gemeente heeft haar SUWI-taken op het gebied van de Participatiewet, IOAW en IOAZ opgedragen aan de gemeenschappelijke regeling Senzer als uitvoerend lichaam (mandaat). Desondanks blijft de gemeente verantwoordelijk voor Suwinet.

In 2021 heeft Senzer een audit laten uitvoeren door een gecertificeerde IT-auditor. De Third Party Memorandum (TPM) die door de auditor is opgesteld laat zien dat Senzer aan het normenkader voldoet. Daardoor voldoet gemeente Asten (als verantwoordelijke) ook aan de normen.

Burgerzaken
Gemeente Asten gebruikt Suwinet-Inkijk binnen Burgerzaken voor BRP-(adres)onderzoeken. Over 2021 heeft onze externe IT-auditor een audit uitgevoerd op het gebruik van Suwinet-Inkijk en geconstateerd dat gemeente Asten aan het normenkader voldoet.

2.4 Zelfevaluatie GEO-informatiedomein

2.4.1 BAG

De zelfcontrole BAG is een wettelijke verplichting voor gemeentelijke bronhouders BAG. Aan de hand van de vragenlijst is de zelfevaluatie BAG uitgevoerd. Op grond daarvan is de verantwoordingsrapportage[6] opgesteld die door het college van B&W is vastgesteld. De zelfevaluatie BAG door de lijnverantwoordelijken levert een score op van 78%. De score is te beoordelen als goed. De score wordt vooral beïnvloed door een lage actualiteit. Dit heeft zijn oorzaak in langdurige uitval van een van de medewerkers. De volledigheid en juistheid van de gegevens is niet in het geding geweest. De personele bezetting is nu weer op orde en dat komt ook tot uiting in de laatste score (100%). Het team heeft er vertrouwen in dat zij deze score kunnen vasthouden.

[4] Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet
[5] Collegeverklaring bijlage DigiD en Collegeverklaring bijlage Suwinet
[6] Verantwoordingsrapportage BAG, BGT en BRO 2021

2.4.2 BGT

De zelfcontrole BGT is een wettelijke verplichting voor gemeentelijke bronhouders BGT. Aan de hand van de vragenlijst is de zelfevaluatie BGT uitgevoerd. Op grond daarvan is de verantwoordingsrapportage[7] opgesteld die door het college van B&W is vastgesteld. De zelfevaluatie BGT door de lijnverantwoordelijken levert een score op van 100%. De score is te beoordelen als uitstekend. De zelfevaluatie levert geen verbeterpunten op.

2.4.3 BRO

De zelfcontrole BRO is een wettelijke verplichting voor gemeentelijke bronhouders BRO. Aan de hand van de vragenlijst is de zelfevaluatie BRO uitgevoerd. Op grond daarvan is de verantwoordingsrapportage[8] opgesteld die door het college van B&W is vastgesteld. De zelfevaluatie BRO door de lijnverantwoordelijken levert een score op van 100%. De score is te beoordelen als uitstekend. De zelfevaluatie levert geen verbeterpunten op.

2.4.4 WOZ

Vanaf 2021 is de zelfcontrole WOZ een wettelijke verplichting voor gemeentelijke bronhouders WOZ. Aan de hand van de vragenlijst is de zelfevaluatie WOZ uitgevoerd. Op grond daarvan is de verantwoordingsrapportage[9] opgesteld die door het college van B&W is vastgesteld. De zelfevaluatie WOZ door de BSOB wordt niet in een score uitgedrukt. Vijf van de zes onderdelen scoren “groen”. BSOB heeft voor 2022 een aantal verbetermaatregelen ingepland.

[7] Verantwoordingsrapportage BAG, BGT en BRO 2021
[8] Verantwoordingsrapportage BAG, BGT en BRO 2021
[9] Verantwoordingsrapportage WOZ 2021

3. Terugblik 2021

3.1 Beleid

In 2021 is het "Strategisch Informatiebeveiligingsbeleid 2021 – 2023" door het college vastgesteld. Met dit beleid zet gemeente Asten een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren. Het strategisch informatiebeveiligingsbeleid sluit aan bij de Baseline Informatiebeveiliging Overheid en de daarop gebaseerde 10 bestuurlijke principes voor informatiebeveiliging.

Vanuit het SUWI-normenkader is bepaald dat een gemeente dient te beschikken over een beveiligingsplan specifiek gericht op het gebruik van Suwinet. Voorheen was de beveiliging van Suwinet opgenomen in het informatiebeveiligingsbeleid. Het opstellen van het Strategisch Informatiebeveiligingsbeleid 2021 – 2023 was een goed moment om ook een separaat Beveiligingsplan Suwinet op te stellen. Ook dit beveiligingsplan is door het college vastgesteld.

3.2 Bewustwording

Onbewust menselijk handelen is de belangrijkste dreiging voor de gemeentelijke informatievoorziening. Investeren in het verhogen van het besef bij medewerkers dat informatiebeveiliging belangrijk is, is dus een efficiënte maatregel.

Phishing campagne
Bij een phishing aanval krijgen medewerkers een e-mail waarin bijvoorbeeld gevraagd wordt om gegevens in te voeren. Deze valse e-mails zien er vaak bedrieglijk echt uit. Door middel van phishing kunnen kwaadwillenden (gevoelige) informatie in handen krijgen.

In 2021 zijn in samenwerking met een externe partij drie phishing tests uitgevoerd en heeft gemeente Asten inzicht gekregen in welke mate zij kwetsbaar is voor een dergelijke aanval. De resultaten van de campagnes laten zien dat phishing mails steeds beter herkend worden door de medewerkers, maar ook dat periodiek uitvoeren van phishing tests noodzakelijk is.

Bewustwording
De BIO schrijft voor dat alle medewerkers die gebruik maken van informatiesystemen en –diensten een training iBewustzijn volgen. In 2021 is gemeente Asten gestart met een laagdrempelige manier van toetsen van de kennis van informatieveiligheid en privacy. Hierbij ontvangen medewerkers wekelijks een vraag waarop zij na beantwoording meteen feedback krijgen. De software die dit regelt geeft via rapportages een continu beeld van de kennis van informatieveiligheid en privacy binnen de organisatie.

3.3 Beveiligingsincidenten

Beveiligingsincidenten zijn gebeurtenissen die inbreuk maken op de informatieveiligheid. Dat kan van alles zijn: verlies of verminking van gegevens, storingen op systemen of ongeautoriseerde inzage van gegevens. Deze incidenten kunnen veroorzaakt worden door menselijk handelen, door bewuste inbreuken of door het uitvallen van techniek bij onszelf of bij partners.

Het aantal beveiligingsincidenten over 2021 is minimaal. Het grootste incident had te maken met een kwetsbaarheid in Log4j. In de Nederlandse pers is ook volop aandacht geweest voor deze

kwetsbaarheid. Gemeente Asten heeft met betrekking tot Log4j daar waar nodig updates in de applicaties uitgevoerd. Als gevolg van deze kwetsbaarheid is zijn de systemen ook één weekend niet beschikbaar geweest voor zowel inwoners als medewerkers.

Door de Informatiebeveiligingsdienst (IBD) zijn we regelmatig gewaarschuwd voor mogelijke bedreigingen van buitenaf. Afhankelijk van de kwetsbaarheid zijn maatregelen genomen. Deze bedreigingen hebben geen invloed gehad op onze systemen en onze informatieverwerking.

3.4 Informatiebeveiliging en privacy

Informatiebeveiliging en privacy zijn nauw met elkaar verbonden. Op dit vlak wordt dan ook intensief samengewerkt. Er is onder andere een gezamenlijk register voor datalekken. Daarnaast wordt in de verwerkersovereenkomsten die worden afgesloten aandacht besteed aan zowel privacy als informatiebeveiliging.

4. Vooruitblik 2022

4.1 ISMS

Gemeente Asten legt over de status van informatiebeveiliging jaarlijks verantwoording af. Hiervoor moeten twee zaken geregeld zijn:

- De organisatie moet haar processen zodanig hebben ingericht dat zij kan garanderen dat aan de eisen uit normenkaders (onder andere BIO en AVG) wordt voldaan.
- De organisatie moet aan kunnen tonen dat de processen ook in de praktijk op deze wijze worden uitgevoerd door hiervoor bewijsdossiers te vormen.

Een Information Management Security System (ISMS) helpt bij het continu beoordelen of de informatiebeveiliging passend en effectief is en of deze bijgesteld moet worden. Het ISMS gaat in 2022 breder gebruikt worden, daarnaast gaat ook ICT NML het ISMS gebruiken om op onderdelen verantwoording af te leggen.

4.2 Bewustwording

Het huidige bewustwordingsprogramma loopt tot medio 2022. Er gaat onderzocht worden of dit programma wordt voortgezet of dat voor een ander bewustwordingsprogramma wordt gekozen.