

Raadsinformatiebrief

Onderwerp	: Informatieveiligheid
Aanleiding	: Toezeggingen Raad/commissie
Datum	: 22 mei 2017
Doel	: Het ter kennisname verstrekken van informatie
Portefeuillehouder	: P.J. Verheij (078) 770 6003
Primaathouder	: C. Rinkel – van der Boom (078) 770 6068 I. Paauwe (078) 770 6076

Geachte leden van de gemeenteraad,

Graag informeren wij u over het volgende.

Inleiding

Op dinsdag 29 augustus 2017 is er een BIO informatieveiligheid, waarbij de ontwikkelingen op het gebied van informatieveiligheid worden toegelicht door de Chief Information Security Office van CIO-office Bureau Drechtsteden. Middels deze RIB wordt u vast geïnformeerd over de stand van zaken informatieveiligheid.

Informatieveiligheid

Informatieveiligheid is de verzamelnaam voor beheersmaatregelen die genomen worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. De kwaliteit van informatievoorziening wordt voornamelijk gedefinieerd in termen van beschikbaarheid, vertrouwelijkheid en integriteit.

- *Beschikbaarheid*: betekent dat informatie(systemen) beschikbaar zijn op de juiste momenten.

Hierdoor hebben burgers en bedrijven toegang tot onze website en toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en dienstverlening richting onze burgers en bedrijven ongestoord voort te zetten.

- *Vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden.

Dit betekent dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Voor de gemeente Alblasterdam is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens van burgers en gegevens van bedrijven niet toegankelijk is voor onbevoegden.

- *Integriteit*: het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het voor de gemeente Alblasterdam van belang dat de correcte informatie tijdig aanwezig is in de systemen. Maar ook dat zelfs na een bepaalde periode de correctheid en de volledigheid van informatie eenvoudig gecontroleerd kan worden.

Visitatiecommissie

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG op 29 november 2013 hebben gemeenten ingestemd met de Resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente". Gemeenten hebben hiermee aangegeven welke stappen zij zullen zetten op informatieveiligheid en wat zij hiervoor nodig hebben.

In lijn met de resolutie heeft de VNG de tijdelijke Visitatiecommissie Informatieveiligheid ingesteld. Deze commissie adviseert de gemeenten op bestuurlijke niveau over informatieveiligheid. De Visitatiecommissie Informatieveiligheid heeft daarvoor op 20 april 2016 en 11 mei 2016 de zes gemeenten binnen de Drechtsteden bezocht.

Op basis van deze bezoeken heeft de Visitatiecommissie de volgende aanbevelingen gedaan:

1. Ga verder op de ingeslagen weg en maak de vervolgstap naar een structureel beleid op het gebied van informatieveiligheid;
2. Benadruk het belang van informatieveiligheid voor politiek-urgente thema's richting de Colleges en de Raden;
3. Systematiseer het leren; werk aan een leerprogramma;
4. Sluit tot en met stap 4 aan bij de Informatie Beveiligingsdienst (IBD);
5. Sturen op het blijven verbeteren vanuit de lijn.

Baseline Informatiebeveiliging Gemeenten (BIG)

Iedere gemeente stelt haar informatiebeveiligingsbeleid vast aan de hand van het basisnormenkader Baseline Informatiebeveiliging Gemeenten (BIG) en moet voldoen aan de regelgeving omtrent privacy. Hierdoor hebben gemeenten een grote verantwoordelijkheid. Ze zijn verantwoordelijk voor het op orde hebben van hun informatieveiligheid en het waarborgen van de privacy van haar inwoners.

Vanuit de visie '*Digitale overheid 2017*' van minister Plasterk moet de overheid in 2017 volledig digitaal zijn wat haar dienstverlening betreft. Uiteraard mag hierbij het onderwerp informatiebeveiliging niet ontbreken. Om de informatie binnen gemeenten zo goed als mogelijk beveiligd te hebben, is de implementatie van de BIG een goede start. In de Resolutie '*Informatieveiligheid, randvoorwaarde voor de professionele gemeente*' onderschrijft iedere gemeente een informatieveiligheidsbeleid vast te stellen aan de hand van de BIG. Met het aannemen van deze Resolutie Informatieveiligheid hebben gemeenten zich tevens verplicht tot de implementatie van de BIG binnen hun gemeente. Belangrijk, aangezien gemeenten veel (persoons-)gegevens beheren die uiteraard goed beveiligd dienen te zijn. Het streven is om de BIG bij alle Nederlandse gemeenten ingevoerd te hebben in 2017.

BIG GAP-analyse Alblisserdam

In 2017 wordt voor de gemeente Alblisserdam een BIG GAP-analyse uitgevoerd. Bij de GAP-analyse wordt eerst gekeken naar wat er al is versus wat er volgens de BIG zou moeten zijn. De uitkomst van de GAP-analyse is een lijst met maatregelen die ontbreken en die geïmplementeerd moeten worden. De GAP-analyse wordt ondersteund met een spreadsheet waarin alle maatregelen staan uit de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) met daarbij een te beantwoorden vraag. In de spreadsheet wordt aangegeven of een maatregel wel of niet of gedeeltelijk genomen is. De uitkomst van de GAP-analyse is een lijst met maatregelen, die genomen zijn of nog genomen moeten worden. In de spreadsheet kan in één oogopslag gezien worden hoe het staat met het totaal van de maatregelen per hoofdstuk.

Nadat de GAP-analyse in kaart is gebracht, welke maatregelen wel of niet genomen zijn, volgt de Impactanalyse. De Impactanalyse geeft antwoord op de vraag in welke volgorde maatregelen geïmplementeerd gaan worden. Dit is belangrijk omdat niet alle ontbrekende maatregelen in één keer genomen kunnen worden. Afwegingen hierbij zijn:

- geaccepteerd risico;
- beschikbaar budget;

- ontwikkelingen op gebied van samenwerking;
- landelijke ontwikkelingen.

De Impactanalyse concentreert zich op de kosten dan wel de tijd en de moeite die nodig is om een maatregel te implementeren. De uitkomst van de Impactanalyse is de GAP tussen wat er al is en wat er nog niet is én een volgorde voor de implementatie van de maatregelen. Er wordt een opzet gemaakt waarin eigenaren benoemd worden voor iedere maatregel.

Informatiebeveiligingsplan

Om de gegevens en informatiesystemen waarover we beschikken, op deze gebieden te kunnen beschermen, is het noodzakelijk een informatiebeveiligingsbeleid te hebben.

In 2015 is het informatiebeveiligingsbeleid Drechtsteden vastgesteld. Procedures en regels die voortvloeien uit het informatiebeveiligingsbeleid dienen lokaal te worden vastgelegd, vastgesteld (op het juiste niveau), uitgevoerd en periodiek geëvalueerd. Na vaststelling van de GAP-analyse en de Impact-analyse wordt het informatiebeveiligingsplan lokaal aangepast. In het informatiebeveiligingsplan wordt vastgelegd welke maatregelen genomen zijn, welke maatregelen nog genomen moeten worden en welke besluiten daarover genomen zijn. Het informatiebeveiligingsplan is een 'levend' document en moet minimaal jaarlijks worden bijgesteld.

ENSIA

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit. Het heeft als doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG) en Inkomen (SUWInet) is samengevoegd en gestroomlijnd. De verantwoording sluit aan bij de gemeentelijke P&C-cyclus en is in lijn met de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG). De horizontale verantwoording over informatieveiligheid sluit hiermee aan op de gemeentelijke planning- en controlcyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad.

Wat betekent dit voor onze gemeente?

De nieuwe verantwoordingsprocedure start met een zelfevaluatie door uw gemeente met behulp van de ENSIA-tool. Het college van B&W legt vervolgens verantwoording over informatieveiligheid af aan uw gemeenteraad in het jaarverslag. Het verantwoordingsproces sluit hierdoor aan op de planning- en controlcyclus. Het gemeentebestuur heeft zo meer overzicht over de informatieveiligheid van haar gemeente. Ook kan het bestuur beter sturen. Op hoofdlijnen ziet het ENSIA-verantwoordingsproces er voortaan als volgt uit:

- Gemeenten voeren vanaf juli 2017 een zelfevaluatie informatieveiligheid uit;
- Het college stelt een collegeverklaring op;
- Een IT-auditor controleert de collegeverklaring en stelt een assurance-rapport op;
- Het college van B&W rapporteert in een paragraaf van het jaarverslag over 2017 over de informatieveiligheid;
- De gemeenteraad controleert de informatieveiligheid van de gemeente en stelt de jaarstukken vast in 2018.

ENSIA coördinator

Om het nieuwe verantwoordingsproces goed in te richten en de zelfevaluatie vragenlijsten in te vullen is betrokkenheid uit verschillende delen van de gemeenten gewenst. Denk hierbij aan de

portefeuillehouder, gemeentesecretaris, de verantwoordelijke personen Bedrijfsvoering (ICT/HR/Inkoop), Burgerzaken (BRP/PUN), Sociaal Domein (SUWInet), DigiD, BAG-beheer en BGT-beheer. Door de VNG is aan het College van B&W gevraagd om de coördinator voor ENSIA aan te wijzen. De rol van ENSIA coördinator is belegd binnen de afdeling Concernstaf. De coördinator werkt mee aan het begeleiden, bewaken en waar nodig bijsturen van het ENSIA-verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor de hele gemeente en het organiseren van samenwerking.

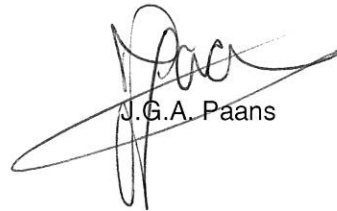
Met vriendelijke groet,
burgemeester en wethouders

de secretaris,

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the end.

S. van Heeren

de burgemeester,

A handwritten signature in black ink, featuring a large, stylized 'P' and 'A' followed by a long horizontal stroke.

J.G.A. Paans