B&W dd. 14 MAART 2017, nr. 3A

reg.nr. B&W-17-0343

Advies aan B&W gemeente De Marne

B&W d.d. 21 FEB. 2017 **Agendapunt:** 1A

Registratienummer: B&W-17-0317

Voorlopig classificatienummer archief:

Relatie met eerdere registratienummers:

Onderwerp:
Informatiebeveiligingsbeleid en -plan

Datum advies: 04-01-2017
Steller advies: A. Pettinga

Voorstel:
Voortgangsrapportage, informatiebeveiligingsbeleid en -plannen vaststellen voor de gemeente De Marne.

Dit voorstel betreft:
1. Voortgangsrapportage informatiebeveiliging BMW
2. Informatiebeveiligingsbeleid De Marne
3. Informatiebeveiligingsplan De Marne
4. Projectplan 'Implementatie BIG' BMW

	PARAAF	DATUM
Afdelingshoofd J.C.H.G.M. Bottema		
Gemeentesecretaris J.C.H.G.M. Bottema		
Portefeuillehouder F.H. Wiersma	A	20/2/17
Gezien/akkoord: Financiën	x	14/2/17
Gezien/akkoord: Communicatie	-	
Gezien/akkoord: P&O	-	
Gezien/akkoord: Juridische Zaken	1	
Gezien/akkoord: Concern-controller	vacature.	
Gezien/akkoord: Inkoop		
Mede-advisering: n.v.t.		
Mede-advisering: n.v.t.		
Mede-advisering: n.v.t.		

Besluit:

Aanhouden
20/2 terug
Conform 14/3/17

	AKKOORD	BESPREKEN
Burgemeester		
Wethouder Berghuis		
Wethouder De Visser		
Wethouder Van Gelder		
Secretaris		

A-lijst of B-lijst B&W **A:** **B:**

Behandeling in raad (voorstel bijvoegen):	Ja ○ Nee ●
Datum raadsvergadering:	
Akkoord raad:	Ja ○ Nee ○
Begrotingswijziging:	Ja ○ Nee ○
Naar de OR / GO:	Ja ○ Nee ●
Datum vergadering:	
Akkoord OR / GO:	Ja ○ Nee ○
Persbericht naar pers (bijvoegen):	Ja ○ Nee ●
Persbericht op website (bijvoegen):	Ja ○ Nee ●
Op openbare besluitenlijst:	Ja ● Nee ○
Info aan dorpsvereniging:	Ja ○ Nee ●
Ter goedkeuring aan G.S.:	Ja ○ Nee ●

Toelichting op voorstel: zie volgblad

College van B&W adviesnota informatiebeveiligingsbeleid en -plan

1. Onderwerp

Het verbeteren van de informatieveiligheid binnen de gemeente De Marne. Dit door het vaststellen van een Information Security Management Systeem (ISMS) waarmee de informatiebeveiliging in opzet wordt geregeld, en het aanstellen van een informatiebeveiligingsfunctionaris waarmee informatiebeveiliging organisatorisch geborgd wordt. Onderdeel van dit ISMS is het informatiebeveiligingsbeleid en –plan.

2. Samenvatting

De eindverantwoordelijkheid voor de informatiebeveiliging ligt bij het College van B&W. De gemeente De Marne hecht groot belang aan informatieveiligheid en wil in navolging van de Resolutie Informatieveiligheid die unaniem door de ledenraad van de VNG eind 2013 is omarmd, de Baseline Informatiebeveiliging Gemeenten (BIG) volgen en invoeren.
Dit gaan we doen door het vaststellen van een op de BIG gebaseerd informatiebeleid, een informatiebeveiligingsplan voor de periode 2016 - 2018 om de BIG in de organisatie in te voeren, onder leiding van de informatiebeveiligingsfunctionaris.
Deze documenten vervangen de bestaande en versnipperde administratieve organisatie rond informatiebeveiliging, leggen rollen en verantwoordelijkheden vast, richten een effectieve stuurcyclus in, leggen de basis voor bewustwording en zorgen voor een eerste planning van implementatie van het informatiebeveiligingsbeleid.

Op 2 februari 2016 heeft het college van B&W ingestemd met de adviesnota 'Informatiebeveiliging BMW-gemeenten' waarin wordt voorzien in de aanstelling van de informatiebeveiligingsfunctionaris die bijdraagt aan de borging van de genomen en te nemen maatregelen.

3. Voorgesteld besluit / beslispunten

1. Vaststellen van voortgangsrapportage 'Informatiebeveiliging BMW-gemeenten – fase 1 en 2' (bijlage 1).

2. Vaststellen van informatiebeveiligingsbeleid (bijlage 2) op basis van de Baseline Informatiebeveiliging Gemeenten (BIG) om daarmee een solide basis te leggen onder informatiebeveiliging binnen de gemeente De Marne.

3. Vaststellen van het informatiebeveiligingsplan (bijlage 3) om zo richting en sturing te geven aan de te implementeren maatregelen. In het bijzonder wordt aandacht gevraagd voor de te accepteren risico's in paragraaf 2.3.

4. Vaststellen van het projectplan 'Implementatie BIG' (bijlage 4) waarin de uitvoeringsconsequenties van de BIG implementatie in beeld worden gebracht.

4. Inleiding

4.1 Uitgangspunten

De gemeente De Marne hecht groot belang aan informatieveiligheid. De volgende uitgangspunten zijn daarbij relevant:

1. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het **college van B&W als eindverantwoordelijke.** De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd in landelijke en Europese wet- en regelgeving en landelijke normenkaders.

2. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en dient bij vermeende inbreuken hiervan melding te maken.
3. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures en zijn zich bewust van hun rol ten aanzien van informatieveiligheid.
4. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.
5. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
6. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
7. Een Informatiebeveiligingsfunctionaris ondersteunt vanuit **een onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.

Het informatiebeveiligingsplan is het resultaat van de toetsing van de ambities uit het informatiebeveiligingsbeleid met de bestaande praktijk.

4.2 Baseline Informatiebeveiliging Gemeenten.

Centraal in zowel het informatiebeveiligingsbeleid als het -plan staat de Baseline Informatiebeveiliging Gemeenten (BIG). Deze door alle gemeenten geadopteerde baseline is gebaseerd op de ISO27001 standaard en vormt een integraal stelsel van IT beveiligingsmaatregelen, personele en fysieke beveiliging, governance (sturing & borging) en naleving.

Op 29 november 2013 is de Resolutie Informatieveiligheid unaniem aangenomen in de ledenvergadering van de VNG. Daarmee wordt de Baseline Informatiebeveiliging Gemeenten (BIG) geïntroduceerd. De BIG is gebaseerd op de wereldwijde ISO 27001/27002 standaard. Het voordeel van een dergelijke standaard is dat niet voor elk organisatie onderdeel, voor ieder proces of systeem een aparte risicoanalyse uitgevoerd hoeft te worden; voor alles geldt de baseline. Een tweede voordeel is dat alle gemeenten onderling, maar ook waterschappen en departementen beter op elkaar aansluiten door het gebruik van dezelfde norm.

De BIG bestaat uit 11 beveiligingscategorieën met 133 beheersmaatregelen en 303 bijbehorende beveiligingsmaatregelen om de beheerdoelstellingen te bereiken. Deze 11 beveiligingscategorieën zijn:

1. Beveiligingsbeleid
2. Organisatie van informatiebeveiliging
3. Beheer van bedrijfsmiddelen
4. Beveiliging van personeel
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen
9. Beheer van informatiebeveiligingsincidenten
10. Bedrijfscontinuïteitsbeheer
11. Naleving

4.3 Het fundament: informatiebeveiligingsbeleid en –plan.

Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder de informatiebeveiliging van de gemeente De Marne. Op basis van een zogenoemde GAP-analyse met sleutelfunctionarissen op het gebied van beveiliging zijn gezamenlijk de huidige situatie en de knelpunten geïnventariseerd. Op basis van het verschil tussen de huidige situatie en de gewenste situatie zijn vervolgens de te nemen maatregelen bepaald. Deze zijn in de elf hierboven genoemde beveiligingscategorieën gebundeld in het informatiebeveiligingsplan. De uitvoering daarvan is gepland over de planperiode 2016 tot en met 2018. Daarvoor wordt een separaat projectplan opgesteld.

4.4 De bouwstenen: Information Security Management Systeem.

De baseline is opgebouwd uit 11 categorieën of domeinen met daarin 133 beheersmaatregelen. Er zijn 303 potentiële beveiligingsmaatregelen uitgewerkt. Voor het houden van overzicht over deze maatregelen is door de gemeente De Marne een Information Security Management Systeem (ISMS) ingevoerd, waarmee de maatregelen (fasegewijs) zullen worden ingevoerd.
Vanuit dit ISMS zijn het voorliggende informatiebeleid, een informatiebeveiligingsplan voor de periode 2016 - 2018 en een set van verordeningen, protocollen, regels en overeenkomsten opgesteld voor goedkeuring door het College van B&W. Zij vormen de basis van de volledige administratieve organisatie rond informatiebeveiliging.

4.5 De aanjager en coördinator: informatiebeveiligingsfunctionaris

De implementatie van de BIG maatregelen geschiedt op basis van het informatiebeveiligingsbeleid en -plan, ondersteund door het ISMS. De (dagelijkse) aansturing, coördinatie, monitoring en verantwoording valt onder verantwoordelijkheid van de informatiebeveiligingsfunctionaris. Hij/zij is projectleider van de BIG implementatie en ziet daarnaast toe op de naleving van toetsing van het informatiebeveiligingsbeleid en -plan. In het geval van beveiligingsincidenten en/of datalekken is de informatiebeveiligingsfunctionaris de 'spin in het web'. Wel is het belangrijk hier te onderstrepen dat de informatiebeveiligingsfunctionaris niet *verantwoordelijk* wordt voor informatiebeveiliging; deze verantwoordelijkheid is en blijft bij het lijnmanagement. Dit staat ook zo omschreven in het informatiebeveiligingsbeleid.

4.6 Relevante wettelijke beleidskaders.

De relevante wettelijke beleidskaders voor het voorgestelde informatiebeveiligingsbeleid en –plan zijn:

- Baseline Informatiebeveiliging Gemeenten
- Wet Basisregistratie Personen (BRP)
- Wet Basisregistratie Adressen & Gebouwen (BAG)
- Wet Structuur Uitvoeringsorganisatie Werk & Inkomen (Suwi)
- Participatiewet
- Wet Maatschappelijke Ondersteuning (WMO) 2015
- Jeugdwet
- Archiefwet
- Wet algemene bepalingen Burgerservicenummer
- Wet Bescherming Persoonsgegevens (Wbp)
- Wet Computercriminaliteit

5. Te bereiken effect

Het beoogd effect is eind 2018 te voldoen aan de Baseline Informatiebeveiliging Gemeenten en daarna het informatiebeveiligingsbeleid conform de BIG te continueren.

5.1 Quick wins

Tijdens de GAP-analyse zijn een aantal quick wins geïdentificeerd. Dit zijn maatregelen die met relatief weinig inspanning veel effect hebben. Met de uitvoering van deze maatregelen wordt dan ook niet gewacht tot 2017. Denk hierbij aan:

- Vaststellen informatiebeveiligingsbeleid en –plan
- Aanstellen informatiebeveiligingsfunctionaris
- Opstellen en implementeren procedure beveiligingsincidenten en datalekken
- Starten bewustwordingstraject
- Professionalisering van het proces identificatie en authenticatie
- Inventariseren en beheren van bewerkersovereenkomsten
- DigiD-assessment onderbrengen in deze structuur

6. Argumenten

1. Door in te stemmen met de beslispunten geeft het College van B&W aan dat het veel belang aan informatiebeveiliging en handelt het conform de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente[1]'.
2. Met het invoeren van het ISMS neemt de gemeente een belangrijke stap naar het voldoen aan de Baseline Informatiebeveiliging Gemeenten (BIG). Dit betekent dat:
    a. De gemeente efficiënt gaat werken aan informatieveiligheid door een algemene standaard te gaan gebruiken.
    b. De gemeente een hulpmiddel krijgt om aan alle eisen op het gebied van informatieveiligheid te kunnen voldoen.
    c. De auditlast verminderd wordt door een integrale benadering.
    d. De gemeente een aantoonbaar betrouwbare partner wordt voor haar omgeving en met name voor de ketenpartners die van een vergelijkbare norm uitgaan.
3. De gemeente krijgt de beschikking over een goed geborgde verbetercyclus op basis van Plan-Do-Check-Act voor haar informatiebeveiliging.
4. De gemeente krijgt de beschikking over een uitgebreide ondersteuning voor het bevorderen van het organisatiebewustzijn op het gebied van informatieveiligheid.
5. De gemeente borgt de informatiebeveiliging op de lange termijn door de aanstelling van een informatiebeveiligingsfunctionaris.

7. Financiën

De structurele kosten op het gebied van informatiebeveiliging, waaronder de aanstelling van een gezamenlijke informatiebeveiligingsfunctionaris, staan beschreven in de gelijktijdig aangeboden adviesnota 'Informatiebeveiliging BMWE'. Verdere dekking wordt nu niet gevraagd.
De kosten in uren en euro's voor het uitvoeren van maatregelen zelf, zoals beschreven in het 'Projectplan implementatie BIG', dienen terug te komen in de capaciteitsplanningen en begrotingen van de betreffende vakafdelingen. In deze nota wordt dan ook geen dekking gevraagd voor de kosten van de uitvoering van de maatregelen zelf.

8. Communicatie

Intern:

- Het management bevordert de algehele communicatie en bewustwording rondom informatieveiligheid op basis van het voorliggende beleid.
- Het management bevordert dat medewerkers (en externe gebruikers van de systemen) zich houden aan beveiligingsrichtlijnen. Afspraken hierover worden vastgelegd in de HR-cyclus resp. het inkoopcontract.

---

[1] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

- In werkoverleggen wordt periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in de Planning & Control cyclus en het HR beleid.

Extern:

- Externe communicatie is noodzakelijk binnen contractrelaties, verder niet.

9. Vervolgtraject

Binnen de gemeente zal op basis van het voorliggende beleid en gebruik makend van het ISMS een stapsgewijze verbetering van de informatiebeveiliging plaatsvinden. Leidraad daarvoor is het vast te stellen informatiebeveiligingsplan, dat jaarlijks zal worden geactualiseerd.
Trekker van de verbeteringen is de informatiebeveiligingsfunctionaris, die vanuit zijn onafhankelijke rol andere delen van de organisatie moet kunnen aansturen.