














Aan het college van Burgemeester en Wethouders

Behandelvoorstelnr : 713805  
Brunssum, 20 februari 2017

T.b.v. **Interne agenda**  
d.d. 21 maart 2017

Verantw. Portefeuillehouder  
C.J.C.P. de Rijck

Ambtelijke routing	d.d.	Akk.	Bestuurlijke routing	Conf. adv.	Bespr.
Financiële toets	14-3-2017		Burgemeester		
Juridische toets (AJZ)	15-3-2017		Wethouder Offermans		
Juridische toets (Controlling)	15-3-2017		Wethouder Joosten		
Kwaliteitstoets	15-3-2017		Wethouder Heinen		
Hoofd Afdeling	10-3-2017		Wethouder de Rijck		
Directeur Dienst	15-3-2017		Wethouder Janssen		
			Secretaris		

Uiterste datum B&W vergadering: NVT  
Motivatie **fatale termijn** aangeven indien van toepassing: NVT

Onderwerp omschrijving:  
Rapportage IT Onderzoek gemeente Brunssum ihkv de jaarrekening 2016

Voorstel/beslisapunten:

**Uw college wordt voorgesteld te besluiten:**

- om kennis te nemen van het Rapport-IT onderzoek 2016 opgesteld door de accountant KSG in het kader van de jaarrekeningcontrole 2016. De bevindingen zijn reeds verwerkt in de uit te voeren maatregelen conform het reeds vastgestelde Informatiebeveiligingsplan 2016-2017;
- om kennis te nemen van de VNG-ledenbrief inzake Informatieveiligheid en de stand van zaken bij de gemeente Brunssum;
- om het voorliggende B&W voorstel ter kennisgeving te brengen naar de raad conform de afspraken gemaakt bij de afhandeling van het raadsbesluit: Oplegnotitie Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum (651978 Gemeentebld nr. 2016/13). Tevens wordt hiermee voldaan aan de oproep van VNG aan haar leden om de raad te informeren over Informatieveiligheid en Privacy;
- Om toepassing te geven aan artikel 55 lid 1 van de Gemeentewet en op grond van het belang van bedrijfs- en fabricagegegevens, zoals genoemd in artikel 10 lid 1 sub c van de Wet openbaarheid van bestuur, en op grond van artikel 10 lid 2 sub g (WOB) het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, geheimhouding op te leggen omtrent het in deze besloten vergadering behandelde inhoud van de bijlage inzake het Rapport-IT onderzoek 2016 met registratienr 714020;

Besluit BW:

**GEWIJZIGD AKKOORD**

- Om kennis te nemen van het Rapport-IT onderzoek 2016 opgesteld door de accountant KSG in het kader van de

jaarrekeningcontrole 2016. De bevindingen zijn reeds verwerkt in de uit te voeren maatregelen conform het reeds vastgestelde Informatiebeveiligingsplan 2016-2017;

- Om kennis te nemen van de VNG-ledenbrief inzake Informatieveiligheid en de stand van zaken bij de gemeente Brunssum;
- Om het voorliggende B&W voorstel ter kennisgeving te brengen naar de raad conform de afspraken gemaakt bij de afhandeling van het raadsbesluit: Oplegnotitie Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum (651978 Gemeenteblad nr. 2016/13). Tevens wordt hiermee voldaan aan de oproep van VNG aan haar leden om de raad te informeren over Informatieveiligheid en Privacy;
- De raad middels een raadsinformatiebrief te informeren;
- Om toepassing te geven aan artikel 55 lid 1 van de Gemeentewet en op grond van het belang van bedrijfs- en fabricagegegevens, zoals genoemd in artikel 10 lid 1 sub c van de Wet openbaarheid van bestuur, en op grond van artikel 10 lid 2 sub g (WOB) het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, geheimhouding op te leggen omtrent het in deze besloten vergadering behandelde inhoud van de bijlage inzake het Rapport-IT onderzoek 2016 met registratienr. 714020.

Registratienummer: 713805

1. Onderwerp omschrijving:

Rapportage IT Onderzoek gemeente Brunssum ihkv de jaarrekening 2016

2. Voorstel/beslispunten: Uw college wordt voorgesteld te besluiten:

- om kennis te nemen van het Rapport-IT onderzoek 2016 opgesteld door de accountant KSG in het kader van de jaarrekeningcontrole 2016. De bevindingen zijn reeds verwerkt in de uit te voeren maatregelen conform het reeds vastgestelde Informatiebeveiligingsplan 2016-2017;
- om kennis te nemen van de VNG-ledenbrief inzake Informatieveiligheid en de stand van zaken bij de gemeente Brunssum;
- om het voorliggende B&W voorstel ter kennisgeving te brengen naar de raad conform de afspraken gemaakt bij de afhandeling van het raadsbesluit: Oplegnotitie Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum (651978 Gemeenteblad nr. 2016/13). Tevens wordt hiermee voldaan aan de oproep van VNG aan haar leden om de raad te informeren over Informatieveiligheid en Privacy;
- Om toepassing te geven aan artikel 55 lid 1 van de Gemeentewet en op grond van het belang van bedrijfs- en fabricagegegevens, zoals genoemd in artikel 10 lid 1 sub c van de Wet openbaarheid van bestuur, en op grond van artikel 10 lid 2 sub g (WOB) het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, geheimhouding op te leggen omtrent het in deze besloten vergadering behandelde inhoud van de bijlage inzake het Rapport-IT onderzoek 2016 met registratienr 714020;

**3. Aanleiding**

In het kader van de jaarrekeningcontrole 2016 heeft onze accountant KSG een onderzoek verricht op de betrouwbaarheid, continuïteit en beschikbaarheid van de automatiseringsomgeving en informatiebeveiliging van het netwerk als geheel van de gemeente Brunssum.

**4. Probleemstelling**

In 2016 heeft de gemeente Brunssum haar Informatiebeveiligingsbeleid aangepast en opnieuw vastgesteld. Het nieuwe beleid (642635) is gebaseerd op de landelijke norm voor gemeenten, de Baseline Informatiebeveiliging Gemeenten (BIG). Voor de uitvoering van het beleid is een beveiligingsplan voor de jaren 2016 en 2017 opgesteld (660417).

De jaarlijkse IT rapportage van de accountant geven samen met het:

- DiGiD-assesment. Correct en veilig gebruik van DigiD t.b.v. de E-dienstverlening (713473)
- Zelfevaluatie Basisregistratie Personen (BRP) en Reisdocumenten (649264)
- KPI-audit Informatiebeheer. Twee jaarlijkse beoordeling correct Informatiebeheer op basis van de Wet RGT voor het taakveld archiefbeheer (709262)

een beeld over de voortgang waarmee de gemeente Brunssum haar informatiebeveiligingsbeleid uitvoert en implementeert.

Tevens zal de raad middels toezending van dit B&W besluit worden geïnformeerd over de voortgang en stand van zaken informatiebeveiliging conform de afspraken die destijds zijn gemaakt bij de afhandeling van het raadsbesluit: Oplegnotitie Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum (651978 Gemeenteblad nr. 2016/13)

**5. Doelen / beoogd resultaat**

*a. wat willen we bereiken?*

De gemeente Brunssum wil haar informatiebeveiliging op een hoger niveau tillen zodat het voldoet aan de Baseline Informatiebeveiliging Gemeenten.

- Hierbij willen we inzicht krijgen in de risico's die we als organisatie lopen en welke maatregelen hiervoor getroffen moeten worden.
- De periodieke audits van de diverse gremia (o.a. de EDP-audit van de accountant, het DiGiD-assesment, en de zelfevaluatie van de Basis Registratie Personen en Reisdocumenten) laten een positief resultaat zien.
- De ketenpartners van o.a het sociaal domein, jeugdzorg aanbieders en ICT voldoen in het kader van de gegevensuitwisseling zoveel mogelijk aan de voor hun opgestelde eisen van Informatiebeveiliging

*b. wat gaan we ervoor doen?*

Uitvoering geven aan het vastgestelde Informatiebeveiligingsbeleid conform de BIG. Dit doen we middels een Informatiebeveiligingsplan dat we jaarlijks bijstellen. Het informatiebeveiligingsforum onder voorzitterschap van de informatiebeveiligingsfunctionaris ziet toe op een correcte uitvoering en implementatie van de maatregelen.

*- inschakeling Beter Buren wenselijk / mogelijk?*

Gelet op het taakveld is de inzet van Beter Buren niet mogelijk

*- zelf initiatief nemen e/o initiatief burgers / maatschappelijk middelveld / bedrijfsleven bevorderen?*

Bij het onderwerp Informatiebeveiliging is het niet mogelijk om burgers en/of het maatschappelijk middelveld te betrekken

*c. hoe meten we of het beoogde resultaat is bereikt?*

- Indicator: Resultaat periodieke audits waarin het aspect informatiebeveiliging wordt beoordeeld

- Bronnen o.a.:

- deze IT-audit van de accountant tijdens de jaarlijkse rekeningcontrole. Informatiebeveiliging vormt een apart onderdeel van de paragraaf Bedrijfsvoering in de P&C-cyclus
- DiGiD-assesment. Correct en veilig gebruik van DigiD t.b.v. de E-dienstverlening
- Zelfevaluatie Basisregistratie Personen (BRP) en Reisdocumenten
- KPI-audit Informatiebeheer. Twee jaarlijkse beoordeling correct Informatiebeheer op basis van de Wet RGT voor het taakveld archiefbeheer.

## **6. Kaders**

*algemene beleidskaders (landelijk, provinciaal, lokaal)*

Baseline Informatiebeveiliging Gemeenten (BIG)

Wet Datalekken

Wet Bescherming Persoonsgegevens

Algemene Verordening Gegevensbescherming

*b. autonoom beleid/taken in medebewind?*

Bedrijfsinformatieplan 2012-2016 (474753)

Informatiebeveiligingsbeleid 2016-2020 (642635)

Vervangingsbesluit (561857)

*c. past het voorstel in de strategische visie?*

- ja

- toelichting: In het visie document Brunssum 2025 heeft het college en de raad zich uitgesproken voor een verdere uitbreiding van de digitale dienstverlening met als ambitie en een excellente dienstverlening. Voor beide zaken geldt dat een adequate informatiebeveiliging een randvoorwaarde vormt.

*d. relatie met programmabegroting?*

- programma: Informatiebeveiliging is opgenomen in de paragraaf Bedrijfsvoering en vormt derhalve geen onderdeel van een programma

- beleidsveld: Informatiebeveiliging is gekoppeld aan het Beleidsveld Informatievoorziening.

## **7. Argumenten / overwegingen**

In hoofdlijnen komt de accountant tot de conclusie dat in het kader van de jaarrekeningcontrole geen significante tekortkomingen in de automatiseringsomgeving zijn vastgesteld. Op basis van het vastgestelde beleid en de uitvoering van de geplande maatregelen wordt vastgesteld dat de ICT -infrastructuur van de gemeente Brunssum zich steeds meer positief ontwikkelt.

De bevindingen die tijdens de controle van de IT 2015 (614423) zijn geconstateerd zijn grotendeels opgelost. Er wordt wel nog gewezen op de uitvoering van de noodzakelijke penetratietest bij de gemeenschappelijke regeling Parkstad-IT. Deze staat gepland voor het tweede kwartaal van 2017. De accountant zal geïnformeerd worden over de uitkomsten van de test en de eventuele opvolgende maatregelen. Tevens stemt de accountant met doelstellingen en de opzet van het migratieplan in.

Tijdens de huidige IT-controle zijn een 6-tal bevindingen geconstateerd. Deze bevindingen/constateringen hebben betrekking op de autorisatieprocedure, het wachtwoordbeleid, de migratie naar PIT en de periodieke certificering van PIT. In de uitvoering van het informatiebeveiligingsplan 2016-2017 zijn diverse maatregelen opgenomen die genoemde constatering en tekortkomingen moeten tegengaan. Het opstellen van een additioneel verbeterplan is derhalve niet noodzakelijk.

Voor meer details wordt korthedshalve verwezen naar de IT-rapportage in de bijlage (714020)

Op 20 februari jongstleden heeft de VNG een ledenbrief verzonden gericht aan het college en de raad met als onderwerp: Informatieveiligheid en privacy (715889). In deze brief adviseert de VNG haar leden om zich regelmatig te laten informeren over de maatregelen die getroffen worden in hun gemeente inzake informatieveiligheid en privacy. Het voorliggende B&W voorstel inclusief het IT-rapport geven een actueel beeld van de Informatieveiligheid en Privacy bij de gemeente Brunssum. Vandaar dat deze ledenbrief gekoppeld is aan dit voorstel.

In de ledenbrief vraag de VNG aandacht voor de volgende onderwerpen:

#### **Verantwoording Informatieveiligheid, ENSIA**

*Status Gemeente Brunssum:* Met ENSIA worden alle aparte audits waarin Informatiebeveiligheid en Privacy worden getoetst (zie par 5.c) samengebracht tot een audit. Binnen de gemeente Brunssum is het Informatiebeveiligingsforum belast met de implementatie van ENSIA. Dit vormt ook een onderdeel van het Informatiebeveiligingsplan 2017.

#### **Aansluiten bij de InformatiebeveiligingsDienst (IBD)**

*Status Gemeente Brunssum:* Sinds vorig jaar is de gemeente Brunssum volledig aangesloten bij de IBD en maken gebruik van alle diensten die door de IBD geleverd worden.

#### **Aansluiten samenwerkingsverbanden IBD**

*Status Gemeente Brunssum:* De samenwerkingsverbanden ISD-BOL, BSGW en Het Gegevenshuis worden benaderd met het verzoek om aan te sluiten bij de IBD. Met alle bovengenoemde samenwerkingsverbanden worden op korte termijn of zijn bewerkersovereenkomsten getekend.

#### **Nieuwe Europese privacywetgeving (AVG)**

*Status Gemeente Brunssum:* Momenteel wordt een nieuw beleidsplan Privacy opgesteld dat is gebaseerd op de AVG. Naar verwachting zal dit medio 2017 worden aangeboden aan het college ter vaststelling. De nieuwe Europese verordening is vanaf mei 2018 van kracht.

### **8. Advies**

Het college wordt geadviseerd om in te stemmen met de conclusies van de accountant inzake de inrichting van de informatievoorziening en de informatiebeveiliging van de gemeente Brunssum. De geconstateerde bevindingen worden als zodanig meegenomen in de uitvoering van het informatiebeveiligingsplan 2017.

Daarnaast wordt het college geadviseerd om op het daadwerkelijke IT-rapport, zoals opgenomen in de bijlage bij dit voorstel, geheimhouding op te leggen conform artikel 55 lid 1 van de Gemeentewet. In het plan is informatie opgenomen waardoor de kans op inbreuk van de informatiebeveiliging aanzienlijk verruimd wordt. Als gronden voor het opleggen van de geheimhouding gelden artikel 10 lid 1 sub c en artikel 10 lid 2 sub g van de Wet Openbaarheid Bestuur. Respectievelijk hebben deze betrekking op:

- bedrijfs- en fabricagegegevens, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
- het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.

Tevens wordt het college geadviseerd om het voorliggende B&W voorstel inclusief alle relevante bijlagen, behalve het IT-rapport, ter kennisgeving te brengen naar de raad conform de afspraken die zijn gemaakt bij de afhandeling van het raadsbesluit: Oplegnotitie Quick Scan "Brunssum op weg naar BIG, digitale veiligheid Brunssum" van de rekenkamercommissie Brunssum.

Hiermee wordt eveneens voldaan aan de oproep van de VNG in haar ledenbrief om de raad actief te informeren over de stand van zaken van de Informatieveiligheid en Privacy

### **9. Aanpak / uitvoering**

#### *a. financiële gevolgen en dekking*

Voor de uitvoering van het Informatiebeveiligingsplan zijn voldoende gelden beschikbaar gesteld. Additionele middelen zijn niet nodig om de geconstateerde bevindingen op te lossen.

- kosten: € (incidenteel / structureel)
- dekking (product- / activiteitencode):
- restantbudget na aftrek kosten: €
- restantbudget voldoende om resterende verplichtingen te dekken: ja

#### *b. risico's?*

- omschrijving risico ('s): voor een volledige omschrijving van alle risico's en genomen beheermaatregelen wordt verwezen naar het informatiebeveiligingsplan 2016-2017 (667248)
- omschrijving beheermaatregelen: zie hierboven
- gevolgen voor weerstandsvermogen: de gevolgen voor het weerstandsvermogen zijn meegenomen in de

*c. tijdpad / mijlpalen / vervolgtraject / evaluatie*

**Autorisatieprocedures:** De bevindingen 1,2 en 4 worden verwerkt in het project optimalisatie autorisatieprocedures. Deze optimalisatieslag is reeds ingezet a.g.v. de daadwerkelijke migratie naar de PIT infrastructuur. Afronding staat gepland voor medio 2017

**Wachtwoordbeleid:** De geadviseerde Single-Sign-On functionaliteit (SSO) komt bij steeds meer applicaties voor maar is nog niet als volledige standaard geïmplementeerd. Naar verwachting zijn binnen 2 jaar alle omgevingen geschikt voor SSO. De geadviseerde 2-weg authenticatie zal einde eerste kwartaal 2017 volledig geïmplementeerd worden.

**Migratie naar PIT:** Het advies voor het overzetten van de mappenstructuur en de daaraan gekoppelde rechten is volledig overgenomen en maakt deel uit van de migratieplanning. De migratie zal medio 2017 zijn afgerond.

**Certificering PIT:** Parkstad IT heeft aangekondigd om in het 2<sup>de</sup> kwartaal 2017 haar ICT-infrastructuur laten certificeren conform de geadviseerde standaarden.

*d. uitvoerende partners intern en extern (werkstructuur)*

Het informatiebeveiligingsforum (IB) onder voorzitterschap van de functionaris Informatiebeveiliging komt periodiek (6 weken) bij elkaar. Het forum kent een zodanige samenstelling dat integraliteit gegarandeerd is met een geborgde koppeling naar het DT. Momenteel nemen de volgende functionarissen deel aan het IB:

- Tijdelijke inhuur CISO (Functionaris Informatiebeveiliging) tevens voorzitter.
- Functionaris Informatiebeveiliging, vervangend voorzitter
- Hoofd Informatiemanagement, plv functionaris Informatiebeveiliging
- Directeur
- Hoofd Publieksdiensten
- Hoofd Bestuurszaken
- Consulente P&O
- Coördinator Informatiemanagement.

Het forum ziet toe op een correcte uitvoering van het beleid en het plan, stelt zaken bij en ziet toe op de uitvoering van maatregelen bij datalekken en beveiligingsincidenten.

Daarnaast worden zaken formeel en informeel afgestemd met Parkstad-IT. Dit gebeurt veelal door de contractmanager (hoofd Informatiemanagement).

*e. communicatie intern en extern?*

- advies/instemming/informatie OR: Het dagelijks bestuur van de OR is tijdens een regulier overleg geïnformeerd over de voortgang van het informatiebeveiligingsbeleid en het -plan. Formeel is geen advies en instemming noodzakelijk echter gelet op het aspect bewustwording is informeren gewenst.
- persbericht: nee, het betreft hier gevoelige informatie alsmede informatie van bedrijfsvoering,
- terinzagelegging: nee
- overig extern:

## 10. Bijlagen

1. Rapport IT-onderzoek 2016 (714020)
2. Ledenbrief VNG inzake Informatieveiligheid en Privacy (715889)