












Aan het college van Burgemeester en Wethouders

Behandelvoorstelnr : 660417
Brunssum, 11 juni 2016

T.b.v. **Interne agenda**
d.d. 30 augustus 2016

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

Ambtelijke routing	d.d.	Akk.	Bestuurlijke routing	Conf. adv.	Bespr.
Financiële toets	19-8-2016		Burgemeester		
Juridische toets (AJZ)	22-8-2016		Wethouder Offermans		
Juridische toets (Controlling)	23-8-2016		Wethouder Joosten		
Kwaliteitstoets	23-8-2016		Wethouder Gelissen		
Hoofd Afdeling	10-8-2016		Wethouder de Rijck		
Directeur Dienst	25-8-2016		Wethouder Janssen		
			Secretaris		

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

Onderwerp omschrijving:
Informatiebeveiligingsplan gemeente Brunssum 2016-2017

Vorstel/beslisapunten:

Uw college wordt voorgesteld te besluiten:

- om het Informatiebeveiligingsbeleid definitief vast te stellen.
- om in te stemmen met het Informatiebeveiligingsplan als kader en om goedkeuring te verlenen aan de uitvoering van de geschetste maatregelen zoals verwoord in de paragrafen 7.1 t/m 7.8. Aan het einde van 2017 zal het college een nieuwe planning worden voorgelegd waarbij ook de evaluatie van de voornoemde maatregelen is opgenomen.
- om het voorliggende B&W voorstel inclusief alle relevante bijlagen ter kennisgeving te brengen naar de raad ter beantwoording van 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).
- om de raad middels dit B&W voorstel tevens te informeren dat de volledige aansluiting bij de Informatiebeveiligingsdienst voor gemeenten (IBD), door middel van het doorgeven van de in gebruik zijnde hard- en software, is gerealiseerd.
- 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 Informatiebeveiligingsplan met registratienr 667248.

Besluit BW:
AKKOORD

- Het Informatiebeveiligingsbeleid definitief vast te stellen;
- In te stemmen met het Informatiebeveiligingsplan als kader en om goedkeuring te verlenen aan de uitvoering van de geschetste maatregelen zoals verwoord in de paragrafen 7.1 t/m 7.8. Aan het einde van 2017 zal het college een nieuwe planning worden voorgelegd waarbij ook de evaluatie van de voornoemde maatregelen is opgenomen;
- Het voorliggende B&W voorstel inclusief alle relevante bijlagen ter kennisgeving te brengen naar de raad ter beantwoording van 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);
- De raad middels dit B&W voorstel tevens te informeren dat de volledige aansluiting bij de Informatiebeveiligingsdienst voor gemeenten (IBD), door middel van het doorgeven van de in gebruik zijnde hard- en software, is gerealiseerd;
- 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 Informatiebeveiligingsplan met registratienr. 667248.

Registratienummer: 660417

1. Onderwerp omschrijving:

Informatiebeveiligingsplan gemeente Brunssum 2016-2017

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

- om het Informatiebeveiligingsbeleid definitief vast te stellen.
- om in te stemmen met het Informatiebeveiligingsplan als kader en om goedkeuring te verlenen aan de uitvoering van de geschetste maatregelen zoals verwoord in de paragrafen 7.1 t/m 7.8. Aan het einde van 2017 zal het college een nieuwe planning worden voorgelegd waarbij ook de evaluatie van de voornoemde maatregelen is opgenomen.
- om het voorliggende B&W voorstel inclusief alle relevante bijlagen ter kennisgeving te brengen naar de raad ter beantwoording van 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).
- om de raad middels dit B&W voorstel tevens te informeren dat de volledige aansluiting bij de Informatiebeveiligingsdienst voor gemeenten (IBD), door middel van het doorgeven van de in gebruik zijnde hard- en software, is gerealiseerd.
- 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 Informatiebeveiligingsplan met registratienr 667248.

3. Aanleiding

Op 24 mei heeft u voorlopig het nieuwe informatiebeveiligingsbeleid van de gemeente Brunssum vastgesteld (642635). Aanpassing van het gezamenlijk informatiebeveiligingsbeleid van de BOL-gemeenten uit 2012 was noodzakelijk i.v.m. de gewijzigde wet- en regelgeving. Wijzigingen die een gevolg zijn van de ontwikkelingen in het sociaal domein en de vergaande informatisering, digitalisering en automatisering van de gemeentelijke bedrijfsprocessen. Door KING is derhalve een richtlijn opgesteld waaraan gemeenten moeten voldoen inzake hun informatiebeveiliging. De Baseline Informatiebeveiliging Gemeenten (BIG). Het nieuwe nog voorlopige beleid is gebaseerd op de BIG en de concrete vertaling hiervan naar een planning van nog te implementeren maatregelen is vervat in een informatiebeveiligingsplan. Dit plan ligt nu voor.

Het vorige informatiebeveiligingsbeleid en -plan is in 2012 in samenwerking met de gemeenten Onderbanken, Landgraaf (BOL) en ISD BOL opgesteld onder aansturing van een gezamenlijke informatiebeveiligingsfunctionaris (307006, 321375). Het beleid en plan van destijds was gebaseerd op de code voor Informatiebeveiliging (NEN 27002). Het fundament voor de BIG vormt deze internationale code. Na pensionering van de gemeenschappelijke functionaris is de samenwerking tussen de BOL-gemeenten en ISD-BOL op dit vlak beëindigd.

4. Probleemstelling

De genoemde baseline omvat meer dan 133 punten op het gebied van informatiebeveiliging waarvoor een gemeente maatregelen moet treffen. Direct willen voldoen aan alle 133 punten is een utopie, niet werkbaar en gelet op de beperkte inzet van middelen (personeel en financiën) niet realistisch. Derhalve is er een plan opgesteld waarin de meest voor de hand liggende maatregelen zijn opgenomen die op basis van urgentie, risico en Quick-win zijn geselecteerd. Een zogenaamde top 10. Deze top 10 is vastgesteld en beoordeeld door het Informatiebeveiligingsforum en het MT.

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-assesement, 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?

Informatiebeveiligingsbeleid en een dito plan opstellen dat voldoet aan de eisen van de voornoemde BIG.

Jaarlijks wordt het plan op basis van de Plan-Do-Check-Act aangepast en opnieuw ter vaststelling aangeboden aan het college. Het informatiebeveiligingsforum onder voorzitterschap van de informatiebeveiligingsfunctionaris ziet toe op een correcte uitvoering en implementatie van de maatregelen.

- inschakeling Beter burens 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.:

- de EDP-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

a. 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

De BIG is een normenkader voor Informatiebeveiliging gebaseerd op een aantal ISO- en NEN normeringen. Het uiteindelijke kader omvat een 133-tal maatregelen waaraan een organisatie zou moeten voldoen. In de bijlage treft u het volledige plan aan waarbij voor iedere maatregel is aangegeven of de gemeente Brunssum daaraan voldoet en welke aanvullende acties eventueel noodzakelijk zouden moeten zijn. (667248)

Om te komen tot een praktisch, controleerbare en doelmatige uitvoering van het plan is in samenwerking met het Informatiebeveiligingsforum en het MT een zogenaamde Top 10 van maatregelen opgesteld. Hierdoor komt de nadruk op die maatregelen te liggen die vanuit de oogpunten van wettelijke urgentie, risico's en Quick-win binnen 1 ½ jaar te implementeren zijn. Hierbij is uiteraard rekening gehouden met de beschikbare middelen (financieel/personeel). In de onderstaande paragrafen treft u een samenvatting van maatregelen inclusief doorlooptijd en financiële consequenties aan. Tevens is er een link gelegd met maatregelen zoals deze in het plan zijn opgenomen. Voor meer details wordt verwezen naar het complete plan in de bijlage.

7.1 Kwalitatief en kwantitatieve borging van de functies Informatiebeveiliging en privacy

Formeel is op dit moment de taak van functionaris Informatiebeveiliging ondergebracht binnen het takenpakket van een medewerker binnen de afdeling Controlling. Voor de uitvoering van deze taak zijn maximaal 8 uur vrijgemaakt. Het aanstellen van een onafhankelijke Informatiebeveiligingsfunctionaris (Chief Information Security Officer, CISO) door

uw college wordt de InformatiebeveiligingsDienst (IBD) alsmede de VNG ten strengste geadviseerd. De onafhankelijkheid wordt enerzijds gewaarborgd door het feit dat deze functionaris niet werkzaam is binnen de uitvoerende afdelingen, anderzijds door het feit dat de onafhankelijkheid is opgenomen in de taakomschrijving van de desbetreffende functie.

Kijkend naar het belang van een goede integere, stabiele en betrouwbare informatiehuishouding van onze bedrijfsvoering en dienstverlening is een stevige structurele invulling van de functie van informatiebeveiliging onontkoombaar. Rekening houdende met gehouden audits, de ambities, het informatiebeleidsplan en de uitvoeringsmaatregelen die nu liggen is een structurele invulling van 28 uur nodig.

In de reorganisatie is een klein deel van deze uren gefinancierd uit bestaande middelen (i.c. de oude functie van 8 uur). In de Perspectiefnota is aangegeven dat we op dit taakgebied vanwege wettelijke verplichtingen gaan uitbreiden en daarvoor zijn aanvullende financiële middelen noodzakelijk.

Vooruitlopend op de aanstaande reorganisatie, waarin rekening is gehouden met deze taakomvang is naast deze bestaande taak van 8 uur, 16 uur aanvullende tijdelijke versterking gezocht. Sinds medio 2015 is een informatiebeveiligingsdeskundige van de gemeente Landgraaf voor 16 uur gedetacheerd bij de gemeente Brunssum. Dit ter ondersteuning van de functionaris Informatiebeveiliging, waar in samenwerking totaal aan 28 uur wordt besteed om in control te zijn en uiteindelijk te voldoen aan de Baseline kader (BIG) en dit ook te blijven. De samenwerking met bovengenoemde informatiebeveiligingsdeskundige is medio juli 2016 beëindigd aangezien de persoon in kwestie een vaste betrekking elders heeft aanvaard. De leidinggevenden van AJZ/Controlling en Informatiebeheer zijn momenteel op zoek naar de inzet van externe expertise inzake ondersteuning informatiebeveiliging tot aan de start van de nieuwe organisatie.

Naast de formele invulling van bovengenoemde functie zijn we in het kader van de Privacy Wetgeving verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. Beide functionarissen vormen ook de formele aanspreekpunten voor de uitvoering van de diverse wet- en regelgeving zoals de Wbp (Wet bescherming persoonsgegevens) en AVG (Algemene verordening gegevensbescherming) door de Autoriteit Persoonsgegevens. (AP) en de Informatie Beveiligingsdienst (IBD). In de nieuwe organisatie zijn via de minimumvariant hiervoor geen middelen voor handen. Getracht is in 1e instantie deze werkzaamheden weg te zetten bij het huidige takenpakket van medewerkers. Maar omdat het taakgebied Privacy/Gegevensbescherming alleen maar ingewikkelder en omvangrijker wordt is dit niet mogelijk gebleken. In de Perspectiefnota wordt voorgesteld hiervoor 24 uur structureel vrij te maken.

Echter gelet op de nieuwe wettelijke normen zoals in de AVG opgenomen en de toegenomen druk op het privacy beleid als gevolg van de ontwikkelingen in het sociaal domein wordt, voor een gemeente met omvang van Brunssum, 24 uur invulling geadviseerd. Momenteel wordt deze functie binnen de gemeente Brunssum niet ingevuld. In het nieuwe organisatieplan is rekening gehouden met de invulling van een minimumvariant van 16 uur voor de informatiebeveiligingsfunctionaris en 8 uur voor de FG. In de Perspectiefnota Begroting 2017 is in ieder geval het voorstel gedaan om deze op te hogen naar het advies respectievelijk 28 en 24 uur.

Voor de ondersteuning van beide functies en het beheer van de informatiebeveiliging in het algemeen geldt dat men moet beschikken over een informatiesysteem voor het beheer van de audits, de risicoanalyses en de toepassing van de maatregelen. Een dergelijk systeem, een information security management system (ISMS) zal geïmplementeerd moeten worden.

Omschrijving:	Kwalitatief en kwantitatieve borging van de functies Informatiebeveiliging en privacy		
Planmaatregel nr	2.2, 2.3.2, 6.2, 15.3	BIG Ref	6.1.2, 6.1.8, 15.2.1, 15.1.4
Personele consequenties	Invulling van de taak CISO alsmede FG zijn meegenomen de personeelsplanning van de aanstaande reorganisatie voor respectievelijk 8 en 0 uur, de zogenaamde minimumvariant.. De geadviseerde bijstelling (resp. 20 en 24 uur) is hier niet in meegenomen. In de Perspectiefnota 2017 is dit advies wel meegenomen.		
Financiële consequenties	De financiële ruimte voor de detachering van de gemeente Landgraaf was tot eind 2016 afgedekt. Tevens is additionele ruimte gevraagd voor ondersteuning bij dit traject middels een voorstel voor resultaatbestemming 2015. De aanschaf van het ISMS zal gedekt worden uit de resultaatbestemming 2015. Genoemde middelen worden ook ingezet voor de inhuur van externe expertise tot aan de start van de nieuwe organisatie (1-1-2017)		
Planning	Eind 2016 formele reorganisatie, begin 2017 formele aanwijzing CISO en FG door college		
Risico's	Momenteel is er geen sprake van structurele borging van kennis en expertise. De opgebouwde kennis zal na ingang van de nieuwe organisatie verdwijnen. De adviezen vanuit de Perspectiefnota inzake het aantal uren inzet kan door de Raad alsnog tijdens de begrotingsbehandeling niet gehonoreerd worden.		

7.2 Verscherpte autorisatie en toegangsbeveiliging

Onder deze noemer worden een aantal maatregelen benoemd die in de loop van het komend 1½ jaar uitgevoerd worden. Hierbij moet o.a. worden gedacht aan:

- het verbeteren van de autorisatieprocedures voor nieuwe medewerkers, het wijzigen van de autorisatie en de

uitdiensttreding medewerker. Deze processen worden in het kader van procesmanagement als pilot project uitgevoerd.

- Het verbeteren van de beveiligingsmaatregelen voor tijd- en onafhankelijk werken (thuiswerken)
- Het aanscherpen van de autorisaties voor de primaire informatiesystemen van Verseon, Burgerzaken, Financiën, WMO, Jeugdzorg enz.

Omschrijving:	Verscherpte autorisatie en toegangsbeveiliging		
BIG norm(en)	9.8, 11.6	BIG Ref	9.2.5, 9.2.7, 11.4.2
Personele consequenties	Geen		
Financiële consequenties	De kosten voor het aanpassen van het autorisatieproces worden, gelet op het feit dat het hier een pilot-project betreft opgevangen binnen het budget Gegevensbeheer. De eventuele kosten voor aanpassing van de autorisatie en rechtenstructuur binnen de primaire informatiesystemen worden opgevangen binnen de reguliere exploitatiebudgetten. De extra beveiligingsmaatregelen voor het tijd- en plaats onafhankelijk werken zijn afgedekt binnen het exploitatiebudget PIT.		
Planning	Aanpassen autorisatieprocessen Q3 2016 Aanpassing autorisatie primaire informatiesystemen Q4 2016 Extra beveiligingsmaatregelen tijd- en plaats onafhankelijk werken Q3 2016		
Risico's			

7.3 Afspraken met en toezicht op ketenpartners

Voor een groot gedeelte van onze ketenpartners geldt dat voor hun een vergelijkbare Baseline Informatiebeveiliging van toepassing is op hun informatiehuishouding. Na inventarisatie zullen alle ketenpartners van de gemeente Brunssum verplicht worden om aan te geven welke status de implementatie van de Baseline bij hun heeft. Daarnaast wordt er een bewerkersovereenkomst tussen hen en de gemeente Brunssum vastgesteld. Voor toekomstige en huidige ketenpartners geldt dat opname van de Baseline en de bewerkersovereenkomst een verplicht onderdeel wordt van de dienstverleningsovereenkomst. Middels een jaarlijkse rapportage gekoppeld aan de P&C-cyclus wordt ook over informatiebeveiliging door hen gerapporteerd. Inmiddels zijn al bewerkersovereenkomsten met PIT, BSGW en het Gegevenshuis afgesloten. De eis inzake de Baseline vormt een onderdeel van het DVO.

Omschrijving:	Afspraken met en toezicht op ketenpartners		
BIG norm(en)	6.12, 6.24, 10.1, 11.8, 11.10	BIG Ref	6.1.2, 6.2.3, 10.8.2
Personele consequenties	Geen		
Financiële consequenties	Het voldoen aan additionele beveiligingseisen kan consequenties hebben voor de hoogte van het DVO wat wordt afgesloten met de ketenpartner.		
Planning	Inventarisatie ketenpartners Q4 Aanspreken inzake opname Baseline en bewerkersovereenkomst Q1 2017 Toetsing jaarlijks bij opstellen jaarrekening P&C cyclus Q1 2018		
Risico's			

7.4 Implementatie Wet op Datalekken

In het kader van de Wet op Datalekken is de gemeente Brunssum verplicht om een registratie procedure in te stellen en een functionaris te benoemen die belast is met het verplicht melden van een datalek bij de Autoriteit Persoonsgegevens (AP). In principe zou deze functionaris de CISO of FG kunnen zijn. We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Het niet naleven van de meldplicht kan een boete opleveren van maximaal € 820.000,=. Het te voeren beleid omtrent de melding van Datalekken is gelijktijdig vastgesteld met het Informatiebeveiligingsbeleid (verseonn:642635) De uitvoeringsprocedure zal zo veel mogelijk gekoppeld worden aan de bestaande procedures voor informatiebeveiligingsincidenten.

Omschrijving:	Implementatie Wet op Datalekken		
BIG norm(en)	2.3.2, 5.1, 13.2, 15.3	BIG Ref	5.1.1, 6.1.8, 6.2.2, 10.2.1
Personele consequenties	Formele benoeming contactpersoon (CISO of FG) voor het melden van datalekken bij het AP		
Financiële consequenties	Vormt een additionele taak, maar kan deel uitmaken van een takenpakket van aanwezige functionarissen		
Planning	Opstellen procedure melding Datalekken Q3 2016 Aanstellen contactpersoon AP Q4 2016		
Risico's	In de risicoparagraaf van de gemeente Brunssum zijn datalekken met als genoemde maximale boete van € 820.000,= opgenomen.		

7.5 Bewustwording Informatiebeveiliging

Via diverse kanalen worden de medewerkers structureel gewezen op het nut van Informatiebeveiliging en de risico's die deze organisatie mogelijk kan lopen. Veelal worden er waarschuwingen en instructies via mail of intranet afgegeven. Echter dit is gebaseerd op incidenten. De bewustwording zal zodanig geborgd moeten worden dat er bij medewerkers een gevoel voor informatiebeveiliging gaat ontstaan waardoor proactief gereageerd kan worden.

Omschrijving:	Bewustwording Informatiebeveiliging		
BIG norm(en)	8.5, 10.7	BIG Ref	8.1.2, 8.2.2
Personele consequenties	Geen		
Financiële consequenties	Eventuele kosten gekoppeld aan een bewustwordingscampagne zullen betaald worden uit het budget wat beschikbaar is gesteld vanuit de resultaatbestemming 2015		
Planning	Het aspect Informatiebeveiliging zal worden meegenomen in de geplande optimalisatie van directie-, afdelings- en persoonlijke plannen. 2017 Implementeren E-learning Informatiebeveiliging Q4 2016 Structureel onderdeel intranet informatiebeveiliging Q2 2017		
Risico's	Vroegtijdige beëindiging ondersteuning gemeente Landgraaf. Hierdoor gaat stagnatie ontstaan in de verdere uitvoering van de maatregelen conform het voorliggende informatiebeveiligingsplan. Deze stagnatie kan deels worden opgevangen door de inhuur van derden		

7.6 Uitwijk, Back-up & Recovery, PEN-test

Door de vergaande samenwerking met Parkstad-IT (PIT) is het continuïteitsniveau van de centrale systemen significant verhoogd. Systemen zijn 24 uur, 7 dagen beschikbaar. Er is sprake van een volledige gespiegelde omgeving en de back-up en recovery procedures dekken vrijwel alle wettelijke procedures af. Echter het formeel implementeren van een periodieke uitwijk- en back-up & recoverytest heeft nog niet plaats gevonden. De deelnemers aan de GR-PIT hebben aangegeven dat een dergelijke periodieke test zodanig moet worden ingericht dat deze geldig is voor alle deelnemers t.b.v. alle afzonderlijke audits en controles. Tevens zal er jaarlijks een zogenaamde netwerk penetratie (PEN) test worden uitgevoerd

Omschrijving:	Uitwijk, Back-up & Recovery		
BIG norm(en)	10.6, 14.1	BIG Ref	10.5.1, 11.4.7, 15.1.3, 15.2.2
Personele consequenties	Geen		
Financiële consequenties	Is opgenomen in de jaarlijkse bijdrage aan PIT		
Planning	Eerste gemeenschappelijke uitwijktest eind 2016 Rapportage backup & Recovery test begin 2017		
Risico's	Geen test kan leiden tot een negatieve score. Het gaat niet om de uitslag van de test		

7.7 Consequenties gewijzigde wetgeving Privacy (landelijk en Europees)

Op 25 mei 2018 zal de nieuwe Algemene Verordening Gegevensbescherming als opvolger van de Wet Bescherming Persoonsgegevens (WBP) ingaan. Deze nieuwe verordening heeft betrekking op geheel Europa en heeft consequenties voor de informatiehuishouding van alle aangesloten organisaties.

Omschrijving:	Consequenties gewijzigde wetgeving Privacy (landelijk en Europees)		
BIG norm(en)	15.3	BIG Ref	10.6.2, 15.1.4
Personele consequenties	Is op dit moment onduidelijk		
Financiële consequenties	Is op dit moment onduidelijk		
Planning	Inventarisatie consequenties wijziging 2016 Verdere uitwerking en implementatie van de AVG 2017 Vaststellen nieuwe verordening 1-1-2018		
Risico's			

7.8 Clean Desk - Clear Screen

Beide aspecten hebben na de verbouwing in 2007 behoorlijke aandacht gekregen echter die is ondertussen verwaterd. Behoorlijke stappen in het clear desk aspect zijn gemaakt door het vergaand digitaal zaakgericht werken maar een voorzichtige observatie geeft aan dat er op veel plekken cruciale informatie op bureaus achterblijft. Niet alle informatie is voor ieders ogen bestemd.

Omschrijving:	Clean Desk - Clear Screen (schoon bureau en geblokkeerd scherm)		
BIG norm(en)	11.5	BIG Ref	11.3.2, 11.3.3
Personele consequenties	Informatiebeveiliging vormt een vast onderdeel van het jaar- en beoordelingsgesprek		
Financiële consequenties	Kosten voor bewustwordingscampagne en korte workshops. Deze kunnen eventueel betaald worden uit opleidingsbudget.		
Planning	Opstellen plan van aanpak Clean Desk, Clear Screen Q4 2016 Uitvoering PvA en regelmatige terugkoppeling in IB-forum 2017		
Risico's	Vroegtijdige beëindiging ondersteuning gemeente Landgraaf. Hierdoor gaat stagnatie ontstaan in de verdere uitvoering van de maatregelen conform het voorliggende informatiebeveiligingsplan. Deze stagnatie kan deels worden opgevangen door de inhuur van derden		

8. Advies

Het college wordt geadviseerd om het Informatiebeveiligingsbeleid definitief vast te stellen. Daarnaast wordt het college verzocht om in te stemmen met het Informatiebeveiligingsplan als kader en om goedkeuring te verlenen aan de uitvoering van de geschetste maatregelen zoals verwoord in de paragrafen 7.1 t/m 7.8. Aan het einde van 2017 zal het college een nieuwe planning worden voorgelegd waarbij ook de evaluatie van de voornoemde maatregelen is opgenomen.

Daarnaast wordt het college geadviseerd om op het daadwerkelijke Informatiebeveiligingsplan, 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 Informatiebeveiligingsplan, ter kennisgeving te brengen naar de raad ter beantwoording van 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). Inzake de aansluiting van de vierde fase op de Informatiebeveiligingsdienst voor gemeenten (IBD), door middel van het doorgeven van de in gebruik zijnde hard- en software, kan de raad worden medegedeeld dat dit is gerealiseerd.

9. Aanpak/uitvoering

a. financiële gevolgen en dekking

- kosten:

Door de raad is een incidenteel budget van € 75.000,- uit de resultaat bestemming 2015 beschikbaar gesteld voor ondersteuning bij de realisatie van de top 10 maatregelen zoals genoemd in het informatiebeveiligingsplan. Naar alle waarschijnlijkheid zal dit budget volledig worden ingezet.

Inzake personele inzet is in het reorganisatieplan rekening gehouden met de minimumvariant voor de IB (16 uur) en FG (8 uur). In de Perspectiefnota 2017 is een voorstel opgenomen om de geadviseerde inzet (resp. 24 en 16 uur) te implementeren.

- dekking (product-/activiteitencode): K510014, 430001
- restantbudget na aftrek kosten: €
- restantbudget voldoende om resterende verplichtingen te dekken: niet van toepassing.

b. Risico's?

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

c. Tijdpad/ mijlpalen/ vervolgtraject/ evaluatie

Een volledig beschrijving van de mijlpalen en planning treft u in paragraaf 7 van dit voorstel alsmede in het Informatiebeveiligingsplan. Het informatiebeveiligingsforum is belast met het toezicht op en de uitvoering van het informatiebeveiligingsplan. Het MT alsmede het college zullen in het kader van P&C cyclus betrokken worden bij de planning en de realisatie van het informatiebeveiligingsplan. Zoals aangegeven zal eind 2017 het college een nieuwe planning worden aangereikt waarbij een evaluatie van de voornoemde maatregelen is opgenomen. Op deze wijze wordt invulling gegeven aan de PDCA-cyclus (Plan-Do-Check-Act)

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 MT. Momenteel nemen de volgende functionarissen deel aan het IB:

- Tijdelijke inhuur CISO (Functionaris Informatiebeveiliging) tevens voorzitter.
- Functionaris Informatiebeveiliging, vervangend voorzitter
- Hoofd Informatiebeheer, plv functionaris Informatiebeveiliging
- Directeur Backoffice/ Gemeentewinkel
- Hoofd Burgerzaken
- Hoofd AJZ/Controlling
- Consulente P&O
- Beleidsmedewerker Informatievoorziening GEO & Sociaal Domein.

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

e. communicatie intern en extern?

- advies/instemming/informatie OR: De OR zal tijdens een regulier overleg geïnformeerd worden over 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. B&W voorstel Informatiebeveiligingsbeleid (642635)
2. Informatiebeveiligingsplan (667248)