




Aan het college van Burgemeester en Wethouders

Behandelvoorstelnr : 642440  
Brunssum, 17 maart 2016

T.b.v. **Openbare agenda**  
d.d. 24 mei 2016

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

Ambtelijke routing	d.d.	Akk.	Bestuurlijke routing	Conf. adv.	Bespr.
Financiële toets	19-5-2016		Burgemeester		
Juridische toets (AJZ)			Wethouder Offermans		
Juridische toets (Controlling)	19-5-2016		Wethouder Joosten		
Kwaliteitstoets	19-5-2016		Wethouder Gelissen		
Hoofd Afdeling	18-5-2016		Wethouder de Rijck		
Directeur Dienst	19-5-2016		Wethouder Janssen		
			Secretaris		

Onderwerp omschrijving:

Voorlopig vast te stellen Informatiebeveiligingsbeleid Gemeente Brunssum - editie 2016

Voorstel/beslispunten:

**Uw college wordt voorgesteld te besluiten:**

Het informatiebeveiligingsbeleid editie 2016 (Verseon registratiekenmerk 642635) voorlopig vast te stellen. Zodra het informatiebeveiligingsuitvoeringsplan 2016 (waarin informatiebeveiliging risico's, maatregelen, functies en prioriteiten zijn opgenomen) gereed is, zullen beide documenten u, tezamen met de beleidsregels meldplicht datalekken, integraal ter definitieve vaststelling worden aangeboden middels een separaat collegevoorstel.

Besluit BW:

**GEWIJZIGD AKKOORD**

Het college neemt kennis van het informatiebeveiligingsbeleid editie 2016 (verseon registratiekenmerk 642635). Zodra het informatiebeveiligingsuitvoeringsplan 2016 (waarin informatiebeveiliging risico's, maatregelen, functies en prioriteiten zijn opgenomen) gereed is, zullen beide documenten, tezamen met de beleidsregels meldplicht datalekken, integraal ter definitieve vaststelling worden aangeboden middels een separaat collegevoorstel.

Registratienummer: 642440

1. Onderwerp omschrijving:

Voorlopig vast te stellen Informatiebeveiligingsbeleid Gemeente Brunssum - editie 2016

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

Het informatiebeveiligingsbeleid editie 2016 (Verseon registratiekenmerk 642635) voorlopig vast te stellen. Zodra het informatiebeveiligingsuitvoeringsplan 2016 (waarin informatiebeveiliging risico's, maatregelen, functies en prioriteiten zijn opgenomen) gereed is, zullen beide documenten u, tezamen met de beleidsregels meldplicht datalekken, integraal ter definitieve vaststelling worden aangeboden middels een separaat collegevoorstel.

3. Aanleiding

De aanleiding voor het vaststellen van dit nieuwe Informatiebeveiligingsbeleid 2016 is wegens verscherpte wetgevingen en gemeentelijke eisen met betrekking tot de Informatiebeveiliging -en persoonsgegevens uitwisseling. Deze automatiseringsontwikkelingen op beveiliging en privacy gebied nemen een vlucht, waardoor het risico steeds groter is op bedrijfsvoerschade maar ook imagoschade. Hierdoor is de noodzaak en urgentie hoog om nieuwe maatregelen te nemen, zodat risico's kunnen worden voorkomen. Daarom laten wij eerst dit beleidskader vaststellen om later de maatregelen met kosten en benodigdheden in een uitvoeringsplan te verwerken en deze samen definitief vast te stellen. Dit beleid vervangt eveneens het inmiddels gedateerde beleid uit 2012. Het is nu noodzaak om dit nieuwe Informatiebeveiligingsbeleid 2016 alvast vast te stellen.

4. Probleemstelling

Door ontwikkelingen en nieuwe eisen wordt afbreukrisico van de bedrijfsvoeringen en dienstverlening steeds urgenter. We moeten de informatievoorziening goed op orde hebben plus de risico's die we lopen in beeld hebben en daar maatregelen op zetten. De maatregelen hebben betrekking op de informatie binnen de processen waarmee de diensten en producten van de gemeente worden geleverd, of deze digitale informatie nu intern of extern (ketenpartners) worden verwerkt, is en blijft de verantwoordelijkheid bij de gemeente Brunssum voor de juiste verwerking van de eigen informatie. Dit betekent kortweg dat wij intern maar ook dat iedere ketenpartner moet voldoen aan alle door de BIG gestelde eisen (2017). Voldoen wij of ketenpartners niet, dan loopt de gemeente Brunssum een groot risico op datalekken, waar men zelfs niet van bewust is. Bij datalekken kunnen door de Autoriteit persoonsgegevens (AP) zelfs boetes tot €820.000,- bij het College van B&W worden opgelegd.

5. Doelen/beoogd resultaat

Voldoen aan de BIG NORM, kapstok voor het komende Informatiebeveiliging uitvoeringsplan 2016, betere grip op Informatiebeveiliging belang en de daarbij behorende wetten en risico's m.b.t interne en externe informatie en privacygevoelige handelingen of bewerkingen. Een beter veiligheid, processencontrole, Incidenten en datalekkenproces, integriteit, juistheid, privacy, betrouwbaarheid en naleving wetten en normenkaders zowel intern als extern door het aanstellen van een Informatiebeveiligingsfunctionaris (Chief Information Security Officer) en de Functionaris Gegevensbescherming (FG). Naast het voldoen aan de gestelde strategische eisen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), zijn ook nog de volgende argumenten als doel van belang:

- Het College van B&W heeft met betrekking de Informatiebeveiliging een eindverantwoording. Hiermede heeft het College een duidelijk kader om het ambtelijke apparaat de Informatiebeveiligingsopdracht te verstrekken met de daaronder liggende verantwoordingen binnen het Informatiebeveiligingskader.
- Het actualiseren op grond van de vereiste vernieuwingscyclus (4 jaar).
- Het inbrengen van nieuwe vereisten, veranderingen en aansluiting op wetten als Jeugdzorg, Participatiewet en WMO2015, de Wbp met daarin de nieuwe Meldplicht datalekken.
- Een betere grip, controle en sturing op en de jaarlijks terugkerende audits en zelfevaluaties zoals DigiD, BAG, PUN (PNIK), BRP en e.v.t. Archiefwet en BGT.
- Daarbij is deze versie geschreven volgens de Informatiebeveiligingsdienst (IBD) vereiste BIG norm (Baseline Informatiebeveiliging Nederlandse Gemeenten) die per 2017 zal worden getoetst.
- Daarnaast wordt in de reorganisatie het informatiebeveiligingsaspect aangescherpt m.b.t. de positionering van de Informatiebeveiligingsfunctionaris (Chief Information Security Officer) en de FG (Functionaris Gegevensbescherming) die mede de veiligheid, integriteit, juistheid, privacy en betrouwbaarheid verder aanscherpen, adviseren, instrueren en signaleren, zij zorgen ook voor orde in de chaos bij calamiteiten, om eventuele imagoschade te voorkomen/beperken.

- Door de modernisering en overplaatsen van de IT facilitering en beheer naar ketenpartner PIT (Parkstad-IT), maar ook het uitbesteden van onze websitebeheer en overige registraties zijn informatiebeveiliging afspraken en controles van belang.
- Ketenpartners die bewerkingen of beheer uitvoeren voor de Gemeente Brunssum dienen op zijn minst een bewerkersovereenkomst te hebben m.b.t. de meldplicht datalekken.
- Duidelijkheid m.b.t. de normkaders en verplichtingen voor Suwi bij de sociale dienst verwerkingen van ISD BOL.
- Kapstok voor een nieuw Informatiebeveiligingsplan (uitvoeringsplan) met 133 maatregelen om de beveiliging aan te scherpen en volgens de wetgevingen te borgen.
- Over de voortgang van dit beleid wordt de raad geïnformeerd in de P&C cyclus, zoals ook door de rekenkamercommissie is verwoordt.
- Een informatiebeveiligingsbeleid aansluitend en adviserend op protocollen en monitors zoals de risico-inventarisatie & -evaluatie (RI&E), de monitor voor een vroegschoolse educatie (VVE), de vergunningverlening, toezicht en handhaving (VTH) en het regionaal informatie en expertise Centrum (RIEC).
- Beter bewustwording van Informatiebeveiliging bij de medewerkers en het management..
- Een actieve Informatiebeveiligingsforum aangestuurd door de Informatiebeveiligingsfunctionaris die incidenten en maatregelen samen nauw controleren en tot uitvoer brengen voor de veiligheidswaarborging.
- Datalekken risico jaarlijks op te nemen in de begroting als zijnde top risico (€820.000,-).

a. wat willen we bereiken?

Door het actualiseren van het oude Informatiebeleid, voldoet de gemeente Brunssum aan de door de IBD en KING gestelde 133 strategische BIG eisen evenals de nieuwe wetgevingen met o.a. de meldplicht datalekken. Voert hierdoor een veiliger informatie beleid met grip op een continue veranderende ontwikkeling in de informaticultuur, het uitvoerbaar maken van de gestelde maatregelen op de gehele interne informatiebeveiliging en bewaker naleving bij ketenpartners. Een betrouwbare en veilige gemeente voor de ketenpartners en de burgers is wat we willen bereiken.

b. wat gaan we ervoor doen?

Door het vaststellen van dit beleid vormen we een kapstok voor het binnenkort (mei/juni) nog voor te leggen Informatiebeveiligingsplan met de 133 uit de BIG norm gestelde maatregelen (Incl. Top10 of 12 belangrijke en snel uitvoerbare maatregelen). Het aanstellen van een Informatiebeveiligingsfunctionaris (Chief Information Security Officer) en de Functionaris Gegevensbescherming (FG) om controle, sturing op uitvoering en toezicht te hebben op dit beleid volgens nieuwe functie kaders die in het uitvoeringsplan zijn omschreven.

Een IB-Forum actief en reactief in te zetten op de uitvoering en controle. De Top maatregelen uit het uitvoeringsplan realiseren inherent aan dit beleid. Zorgen dat het personeel IB bewust is en blijft, dat het gebouw volgens protocol toegankelijk is. Dat er inzicht is over onze dossier en data uitwisseling zowel intern als extern (ketenpartners met waarborging en indekking op datalekken).

- inschakeling Beter burens wenselijk/mogelijk?

Nee

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

Nee

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

- Indicator:

Het Informatiebeveiliging Forum toetst 6 wekelijks de voortgang van maatregelen en naleving met rapportering naar het MT en jaarlijks naar het College van B&W. Daarnaast zorgt de Informatiebeveiligingsfunctionaris (CISO) voor een continue planning met PVA en een centrale audit overzicht (ISMS).

- Bron

De bron van deze opzet zijn de IBD en KING die de gemeenten verhoogde Informatiebeveiliging eisen opleggen. Men kan stellen dat de BIG norm de gehele Informatiebeveiliging kapstok is waar dit beleid op is gebaseerd.

6. Kaders

De in het beleid genoemde structuur ter naleving vormen eveneens de kaders uit de BIG norm. De 133 maatregelen uit de BIG worden later via het Informatiebeveiligingsplan aan u gepresenteerd, die een kader vormen ter uitvoering.

a. algemene beleidskaders (landelijk, provinciaal, lokaal)

BIG norm en meldplicht datalekken norm.

b. autonoom beleid/taken in medebewind?

Autonoom

c. past het voorstel in de strategische visie?

- ja

- toelichting

Dit beleidsstuk is met name en volgens de BIG norm een strategisch beleid

d. relatie met programmabegroting?

- programma:

- beleidsveld:

## 7. Argumenten/overwegingen

Dit beleid is als eerder aangegeven een kapstok voor de gehele Informatiebeveiliging en het uitvoeringsplan, het beleid wordt 4 jaarlijks herzien.

## 8. Advies

Het vaststellen van dit beleid zorgt voor een nieuw Informatiebeveiligingsbeleidskapstok 2016

## 9. Aanpak/uitvoering

We volgen het Informatiebeveiligingsbeleid op en voeren de komende Informatiebeveiligingsplan voortkomende top maatregelen uit. Daarnaast zorgen deze stappen voor een structurele invulling van een bekwame Informatiebeveiligingsfunctionaris (CISO) evenals een structurele Functionaris Gegevensbescherming (FG), vanwege de Meldplicht datalekken wetsaanpassing in de Wbp en de komende Europese privacy verordening (AVG) die de Wbp vervangt. Hierna is de aanstelling van een (FG) verplicht. Bij het e.v.t. niet uitvoeren van enkele door de BIG norm gestelde maatregelen volgen wij zowel intern als met de ketenpartners het “pas toe leg uit” principe op volgens de informatiebeveiligingsdienst (IBD) en BIG norm gestelde eisen bij het wel of/niet naleven van de norm, moet men wel uitleggen waarom en wat men er in de plaats of anders voor doet, ter uiteindelijke veilige waarborging. Dit zal de Informatiebeveiligingsfunctionaris toetsen op zowel waarheid als procedure correctheid en dit via het Informatiebeveiliging Forum rapporteren aan het management.

Dit beleid zal onder voorbehoud moeten worden vastgesteld tot het informatiebeveiligingsuitvoeringsplan gereed is en u medio mei/juni zal worden gepresenteerd om gezamenlijk met dit beleid definitief vast te stellen. Na beiden te hebben vastgesteld kunnen wij ook verder met het naleven van de BIG norm gestelde maatregelen.

Door deze aanpak en volgorde werken wij aan een veiligere gemeente. Hierdoor is er eveneens een betere en centralere grip, advisering, controle, coördinatie en signalering op procedures en naleving m.b.t. de interne als externe veiligheid van onze gemeentelijke en de burgers persoonlijke informatie of data.

### a. Financiële gevolgen en dekking

- kosten: € (incidenteel/structureel)

- dekking (product-/activiteitencode):

- restantbudget na aftrek kosten: €

- restantbudget voldoende om resterende verplichtingen te dekken: ja/nee

### b. Risico's? ja

- omschrijving risico ('s):

Het niet vaststellen heeft als consequentie dat de gemeente niet kan voldoen aan de BIG norm en nieuwe wetgevingen omtrent Informatiebeveiliging. Dit kan resulteren in het volgende:

- Dat men geen overzicht heeft op de uit te voeren maatregelen ter veiligheid.
- Men niet slaagt of slecht scoort bij audits of zelfevaluaties en afsluiten van Burgerzaken, Basisregistraties en SUWINET het gevolg kan zijn, gevolgd door een boete clausule.
- Men bij een datalek niet geheel kan aantonen dat men veilig omgaat met informatie en dat er dan een boete van wel €820.000,- bij het College van B&W kan worden opgelegd aangezien men hier ten immer eindverantwoordelijk is voor de goede en veilige verwerking van Privacygevoelige data.
- Bij het niet naleven van de BIG en Wbp met meldplicht datalekken kan er niet alleen een boete uit voortkomen, maar indien er burgers zijn benadeeld door onterechte aanpassing of lekken van persoonsgegevens is het mogelijk om imagoschade op te lopen door media en rechtsorde.
- Bij uitval of aanpassing van systemen, maar ook onterechte aanpassen van persoonsgegevens (hardware en software) door interne of externe ketenpartners is het mogelijk dat de gemeente niet kan functioneren en de burgers niet kan ondersteunen. Dit kan uiteraard ook leiden tot imagoschade.
- Het niet aanstellen van een Informatiebeveiligingsfunctionaris (Chief Information Security Officer) en de Functionaris Gegevensbescherming (FG) zal leiden tot onoverzichtelijkheid, geen grip op Informatiebeveiliging en de Wbp, evenals de naleving van beide.
- De wettelijke kaders en adviezen en eisen m.b.t. tot het aanstellen van beide functies worden dan niet nageleefd.
- Het niet naleven van dit beleid met plan resulteert eveneens in een organisatie wat niet bewust genoeg is op het gevaar m.b.t. de persoonlijke informatie -en fysieke uitwisseling. (b.v. Wie doet wat en wie mag dit, onder welke voorwaarde mag je het gebouw betreden).
- Bij het niet op orde hebben of controle op naleven van de BIG, maar ook contracten m.b.t. de meldplicht datalekken bij ketenpartners, kan dit leiden tot boetes of imagoschade zoals bovengenoemde scenario's.
- Per 1 juli 2016 zijn de gemeenten onderhevig aan een toetsing m.b.t. datalekken (de autoriteit persoonsgegevens zal deze op steekproefsgewijze uitvoeren). Indien een datalek niet of niet goed is gemeld, afgehandeld of is teruggekoppeld volgens meldplicht datalekken protocol, zal dit leiden tot een boete tot wel €820.000,-
- Datalekken risico valt onder de top 5 gemeentelijke kosten risico's en is dus zeer serieus te noemen.

financieel/anders t.w.:

- omschrijving beheermaatregelen: De BIG normenkader met 133 maatregelen. Waaruit kosten kunnen voortvloeien m.b.t. laten uitvoeren en oplossen van. Onderzoek, Analyses en ondersteuning. Aanstellen van 2 Functionarissen.

Begroting risico stelpost op datalekken (€820.000,-).

- gevolgen voor weerstandsvermogen: Is middels bij financiën opgenomen en geborgd in de risico-inventarisatie.

c. Tijdpad/ mijlpalen/ vervolgtraject/ evaluatie

d. uitvoerende partners intern en extern (werkstructuur)

e. communicatie intern en extern?

- advies/instemming/informatie OR :

Ja, informatief m.b.t. voortgang van de informatieveiligheid in combinatie met de risico-inventarisatie & -evaluatie (RI&E), waar informatiebeveiliging raakvlakken mee heeft.

- persbericht :nee, dit is een intern organisatie beleid, vertrouwelijk en alleen toegankelijk voor het College van B&W, het management met daarnaast de Informatiebeveiliging functionaris (CISO), eventueel de FG en Informatiebeveiliging Forum.

- terinzagelegging :nee

- overig extern :nee

## 10. Bijlagen

Informatiebeveiligingsbeleidsplan 2016 (registratiekenmerk 642635)

Begrippenlijst Informatiebeveiliging 2016 (registratiekenmerk 647066)

Beleidsregels meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) (registratiekenmerk 645562)

Handreiking Functionaris Gegevensbescherming (FG) functieprofiel (door de Autoriteit Persoonsgegevens) (registratiekenmerk 647071)

Handreiking Informatiebeveiligingsfunctionaris (CISO) functieprofiel (door het IBD) (registratiekenmerk 647069)