Advies*Nota*

Gemeente Brummen

AAN BURGEMEESTER EN WETHOUDERS				**OPENBAAR**
			Datum :	13-8-2014
Afdeling	:	Beleid en Bedrijfsvoering	Casenr. :	BWZ14.0303
Adviseur	:	N. Edwards NE/285	Doc.nr. :	BW14.0446
Medeadviseur(s)	:	Geen		
Portefeuillehouder(s)	:	J.B. Paauw		
Portefeuille(s)	:	Informatievoorziening, archief en automatisering		
Burgerparticipatie	:	Niet van toepassing		
Onderwerp	:	Vaststellen Informatiebeveiligingsplan		

VOORSTEL/ADVIES

Besluiten om:

1. vaststellen Informatiebeveiligingsplan met bijbehorende procedures en bijlages

COLLEGEBESLUIT

Datum	**Besluit**	**Vervolgprocedure**
26/08/2014	Conform advies	Raad: t.k.n. OR:

Inleiding

Het informatiebeveiligingsplan 2014 is de actualisering van het informatiebeveiligingsplan van 2010-2012. Het plan is de basis voor een planmatige aanpak van- en blijvende aandacht voor informatiebeveiliging. Informatiebeveiliging is niet alleen een technische aangelegenheid. Door de grote afhankelijkheid van de Informatie en Communicatie Technologie, de ICT, vooral bij de kritische primaire processen, gaat dit niet meer op. Gegevens worden steeds meer gedeeld tussen de afdelingen, maar ook met andere organisaties en ten slotte niet in de laatste plaats met de burger. Daarom rust op de organisatie de taak adequate voorzieningen te treffen om de betrouwbaarheid en de continuïteit van de informatievoorziening te waarborgen.
Tot die voorziening behoren ook duidelijke afspraken over taken en verantwoordelijkheden rondom het bewaren, beheren en verstrekken van gegevens. Deze voorzieningen vloeien mede voort uit de “zorgvuldigheidsplicht” van de gemeente, immers onzorgvuldig handelen kan leiden tot aansprakelijkheid.

Argumenten

1.1 Het huidige informatiebeveiligingsplan is verouderd
Het huidige plan dateert van 2010. Ten opzichte van vier jaar geleden worden ook vanuit de Rijksoverheid steeds meer eisen gesteld aan beveiliging van informatie. Normen zijn aangescherpt. Er wordt nu niet alleen controle uitgeoefend op het hebben van bepaalde procedures, maar ook op de opzet en de werking ervan. Auditeurs en accountants doen daar gericht onderzoek naar.

1.2 De kwaliteit van de gemeentelijke gegevens vraagt om continue aandacht
De inhoudelijke kwaliteit van de gemeentelijke gegevens staat in rechtstreeks verband met de kwaliteit van de beheerprocessen organisatiebreed. Deze processen moeten zijn vastgelegd in het informatiebeveiligingsplan.

1.3 Het werken met (vooral digitale) informatie vereist aandacht voor beveiligingsaspecten
De betrouwbaarheid van informatiesystemen evenals de mate van beschikbaarheid, juistheid en volledigheid van informatie en de mate waarin informatie wordt afgeschermd voor onbevoegden moet een ongestoorde dienstverlening waarborgen. Informatie is van cruciaal belang voor de voortgang van de gemeentelijke processen.

1.4. Vanuit de overheid worden er steeds strengere eisen opgelegd t.b.v. informatievoorzieningen
Het VNG heeft hiervoor de IBD opgestart welke een Baseline informatiebeveiliging heeft opgesteld (BIG). Door deze als leidraad te gebruiken voor de gemeentelijke informatiebeveiliging zal de auditlast worden verminderd

Kanttekeningen

Het draagvlak voor het Informatiebeveiligingsplan ligt enerzijds in de wet- en regelgeving en anderzijds in toenemende bewustwording van het belang van informatie voor de organisatie en van de noodzaak om de vertrouwelijkheid, integriteit en de continuïteit van de informatievoorziening zeker te stellen.

Communicatie

Om het gewenste draagvlak te verkrijgen is het communiceren over (informatie)beveiliging van groot belang en moet daarom aan de orde komen in het werkoverleg van afdelingen/teams, bij opleiding en training en functioneringsgesprekken.

Financiële toelichting

Voor het goed uit kunnen voeren en implementeren van de diverse procedures is veel tijd nodig, dit zal meer druk op de gehele organisatie leggen.

Juridische grondslag

Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG en PUN, maar ook de archiefwet.
Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Uitvoering

Opvolgend aan dit plan zullen de overige procedures in de loop van 2014 ook aan dit informtaiebeveilingsplan toegevoegd moeten worden om zo een compleet beleid te krijgen rondom informatiebeveiliging. Het MT zal moeten bewaken dat de uitvoering informatiebeveiliging binnen de organisatie goed verloopt

Stukken ter vaststelling

INFORMATIEBEVEILIGINGSPLAN 2014-2017	ZK14.02847	INT14.2624
1.	Bijlagelijst bij het informatiebeveiligingsplan	INT14.2652
2.	Beveiligingsplan Reisdocumenten	INT14.2610
3.	Bijlage D PUN	INT14.2612
4.	Formulier Identificatievragen	INT14.2613
5.	Procedure Overvalinstructie	INT14.2614
6.	Werkinstructie identiteitsfraude	INT14.2615
7.	Procedure backup en Restore	INT14.2616
8.	Functiescheidingsmatrix	INT14.2617
9.	Functiebeschrijving beveiligingsambtenaar	INT14.2618
10.	Gedragscode integer handelen	INT14.2619
11.	Bijlage functieverdeling	INT14.2625
12.	Bijlage wijzigingsbeheer	INT14.2627
13.	Bijlage wachtwoordbeleid	INT14.2626
14.	Bijlage Toegangsbeleid Gemeente Brummen	INT14.2628
15.	Bijlage mobiele gegevensdragers	INT14.2629
16.	Bijlage Logging beleid	INT14.2631
17.	Bijlage Kenmerken kluisruimte	INT14.2645
18.	Bijlage Kenmerken computerruimte	INT14.2644
19.	Bijlage Incident Management en Response Beleid	INT14.2639
20.	Bijlage Hardening beleid	INT14.2640
21.	Bijlage Cloud Computing beleid	INT14.2641

22.	Bijlage Backup en Recovery Beleid	INT14.2642
23.	Bijlage Anti Malware beleid	INT14.2643
24.	Afvoer ICT middelen	INT14.2646
25.	Autorisatieprocedure tot informatiesystemen	INT14.2647
26.	Bijlage Backup registratie	INT14.2648
27.	Bijlage functies	INT14.2649
28.	Bijlage Proces verbaal vernietiging van verwijderbare media	INT14.2650