

**B&W VOORSTEL**

Kenmerk: 20BW000139

Datum voorstel: 22 juli 2020	Onderwerp: Informatiebeveiligingsbeleid
Voorstel portefeuillehouder: 1. Het geactualiseerde informatiebeveiligingsbeleid vast te stellen. 2. Het voorgaande informatiebeveiligingsbeleid (15bes00215) in te trekken. 3. De raad informeren over het geactualiseerde informatiebeveiligingsbeleid.	
Team/ behandelend ambtenaar: STAF / B. Jansen (CISO)	Status voorstel: openbaar
Portefeuillehouder: B.E. Faber-de Lange	Datum b&w-vergadering: 18 augustus 2020
Doorgeleiding naar de raad: ja	Indien naar de raad: ter kennisname
Betrokkenen bij voorstel extern:	Betrokkenen bij voorstel intern: M. Spierings (ISO), L. van Ampting-Janssen (Teammanager TIO), MT
Advies type voorronde raad:	TIC: Ja

Bijlagen voor B&W:

- 20int02850 - Informatiebeveiligingsbeleid

Bijlagen voor raad:

- 20int02850 – Informatiebeveiligingsbeleid
- 20bw000139 - B&W voorstel “Informatiebeveiligingsbeleid”



Voorstel

1. Het geactualiseerde informatiebeveiligingsbeleid vast te stellen.
2. Het voorgaande informatiebeveiligingsbeleid (15bes00215) in te trekken.
3. De raad informeren over het geactualiseerde informatiebeveiligingsbeleid.

Inleiding

Het vorige informatiebeveiligingsbeleid (IB-beleid) van gemeente Overbetuwe is door het college van B&W in 2015 vastgesteld (besluit 15bw000463, d.d. 29 september 2015). Sinds 2015 hebben zich ontwikkelingen voorgedaan die het noodzakelijk maken om het beleid te actualiseren. De belangrijkste ontwikkeling is de komst van Baseline Informatiebeveiliging Overheid per 2020, kortweg de BIO, als opvolger van de Baseline Informatiebeveiliging Gemeente (BIG). De BIO is een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-standaarden.

Doel en beoogd effect

Een geactualiseerd IB-beleid biedt een raamwerk voor beveiligingsmaatregelen. Deze maatregelen treffen we om de gegevens van onze inwoners en bedrijven te beschermen. Dit IB-beleid is ook een voorwaarde om als gemeente aantoonbaar te voldoen aan de BIO.

In het beleid worden de rollen en verantwoordelijkheden rondom informatiebeveiliging uitgewerkt. Tevens wordt een kader geschetst voor de organisatie rondom informatiebeveiliging. In dit nieuwe beleid wordt de rol van de lijnmanagers prominenter neergezet. De lijnmanager is proceseigenaar, dus risico-eigenaar. Hieruit volgt dat hij of zij verantwoordelijk is om op basis van risico-afwegingen beveiligingsmaatregelen door te (laten) voeren.

Argumenten

1.1 Informatieveiligheid is als kwaliteitsaspect een integraal onderdeel van de bedrijfsprocessen. Het IB-beleid heeft als doel om een raamwerk te bieden van uitgangspunten om de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening en de informatiesystemen te waarborgen. Hiermee kan een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld worden, gericht op de bescherming van de informatievoorziening tegen interne en externe bedreigingen.

2.1 Het oude beleid is niet meer actueel, mede door de komst van de BIO.

3.1 De gemeenteraad op transparante wijze meenemen in de risicobeheersing en beveiliging van informatie.

Kanttekeningen en risico's

Dit voorstel heeft geen kanttekeningen en risico's

Financiën

Dit voorstel heeft geen financiële gevolgen



Vervolg

Planning

Op basis van het IB-beleid wordt periodiek een IB-plan (of programma) opgesteld waarin een vertaalslag plaatsvindt van de beleidsuitgangspunten. Dit IB-plan bestrijkt 1-2 jaar en hierin worden dan concreet de geprioriteerde maatregelen en actiepunten uitgewerkt. Daarnaast is informatiebeveiliging onderdeel van het grotere geheel van informatiebeleid. Informatiebeleid en –beveiliging zijn integraal onderdeel van middelensturing en daarmee onderdeel van de concernplanning. De informatiebeveiligingsactiviteiten worden opgenomen in de concernplanning. Lijnmanagers spelen een cruciale rol in informatiebeveiliging. Immers, op basis van risico-afwegingen is de lijnmanager verantwoordelijk voor het al dan niet doorvoeren van beveiligingsmaatregelen. Dit vereist dus een tijdsinvestering van lijnmanagers.

Communicatie

Beleids- en gedragsregels werken in de praktijk alleen als die ook voldoende bekend zijn en nageleefd worden. Communicatie over het IB-beleid is daarom noodzakelijk. In het kader van bewustwording moet worden zorggedragen voor training, opleiding en een continue aandacht voor een veilige omgang met informatie bij alle medewerkers. Ook hier geldt dat de lijnmanager een prominente rol vervult. Hij/zij heeft een voorbeeldfunctie.

Evaluatie

Het IB-beleid zal minimaal eens in de drie jaar worden geëvalueerd en zo nodig eerder.

