VEILIGHEIDSREGIO TWENTE
Samen werken aan een veilige regio

VOORSTEL

Algemeen Bestuur

ONDERWERP	Informatieveiligheid	AGENDAPUNT	E5
DATUM	10 juli 2017		
OPENBAAR	ja	BEHANDELD DOOR	Projectgroep informatieveiligheid
REGISTRATIENUMMER	[Registratienummer]	TELEFOONNUMMER	[Telefoonnummer]
PORTEFEUILLEHOUDER	Arco Hofland		

Besluit

De leden van het Algemeen Bestuur wordt gevraagd kennis te nemen van:
- de Europese Algemene Verordening Gegevensbescherming waaraan vanaf mei 2018 voldaan moet worden en van de acties die in het Plan van Aanpak Informatieveiligheid worden benoemd.
- het concept Baseline Informatiebeveiliging Veiligheidsregio Twente die als leidraad zal dienen voor uitvoering.

Aanleiding
Vanaf mei 2018 wordt de Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing waarmee de privacywetgeving wijzigt. Met het ingaan van deze nieuwe wet wordt een en ander gevraagd van onze organisatie qua capaciteit en begroting. Mede vanwege de primaire taak van de Veiligheidsregio om de continuïteit van de samenleving te borgen, is het van belang om de informatieveiligheid van de eigen organisatie op orde te hebben. Met dit voorstel wordt u geïnformeerd over het onderwerp ‘Informatieveiligheid’ binnen Veiligheidsregio Twente.

Baseline Informatiebeveiliging
De Landelijke Vakgroep Informatieveiligheid, waar alle 25 veiligheidsregio’s onderdeel van uitmaken, heeft de Baseline Informatiebeveiliging Gemeenten (BIG) overgenomen en daar waar nodig aangevuld. Hiermee vormt dit landelijk document het inhoudelijk normenkader voor informatieveiligheid. Veiligheidsregio Twente heeft op basis van dit landelijke document bijgaande Baseline Informatiebeveiliging Veiligheidsregio Twente in concept opgesteld. Hierin is het normenkader specifiek gemaakt voor Veiligheidsregio Twente en wordt voldaan aan de minimale wettelijke vereisten.

Deze Baseline is in lijn met het algemene beleid van Veiligheidsregio Twente en sluit aan bij de ambitie van het Veiligheidsberaad. Bij de uitvoering wordt daar waar mogelijk aangesloten bij Oost 5 en gemeentelijke samenwerkingsverbanden als SSNT.

Plan van aanpak Informatieveiligheid Veiligheidsregio Twente
Het bedrijfsvoeringsoverleg VRT (d.d. 3 november 2016) heeft ingestemd met het plan van aanpak Informatieveiligheid. Hierin worden enkele concrete acties benoemd:
1. **Bewustwordingsprogramma topprioriteit**. De meeste data-incidenten zijn het gevolg van menselijk handelen. Informatieveiligheid is een mensenkwestie, geen systeemkwestie. Dat besef ontbreekt in veel gevallen. Medewerkers van VRT, ketenpartners (die een rol vervullen binnen de crisisorganisatie) en bestuurders dienen bewust te zijn van de kans op en de impact van data-incidenten. Hiervoor wordt een bewustwordingsprogramma opgesteld. Dit programma ondersteunt bij het bewust maken van de gevaren van informatielekken of cyberaanvallen in het netwerk van de VRT. We zijn voornemens het programma op een ludieke wijze uit te rollen en bekend te maken bij alle gebruikers van het VRT netwerk.
2. **Inzichtelijk maken** waar binnen de VRT wordt gewerkt met informatie die beveiligd dient te worden, bijvoorbeeld persoonsgegevens of gevoelige informatie van bedrijven. Om deze reden worden informatiesystemen als Beaufort, Veiligheidspaspoort, LCMS, VNET/SharePoint, GMS en AFAS als eerste geanalyseerd.
3. De resultaten van bovenstaand onderzoek worden voor elk informatiesysteem afzonderlijk inzichtelijk gemaakt in een **Privacy Impact Assessment** (PIA). Dit is een wettelijke verplichting. In de PIA wordt

beschreven hoe, met welk doel, en door wie de informatie wordt verwerkt en hoe de informatie invloed kan hebben op de privacy. Ook staan hier de maatregelen beschreven die moeten worden getroffen om veiligheidsrisico's te minimaliseren tot een aanvaardbaar niveau binnen de wettelijke kaders.

4. Aanwijzen van een **Functionaris Gegevensbescherming** (FG) wordt met de wetswijziging voor overheidsorganisaties verplicht. Deze functionaris ziet toe op naleving van de AVG.
5. De ervaring leert dat ook in Twente een data-incident of een cyberaanval een reëel scenario is (recente voorbeelden zijn voorgevallen bij de gemeente Almelo en Meldkamer Twente). Om voorbereid te zijn, wordt een **protocol** ontwikkeld. Dit protocol is wettelijk verplicht en geeft duidelijkheid over de te nemen stappen op het gebied van techniek, communicatie en bestuur bij een data-incident.

Begroting
In de begrotingen 2017 en 2018 zijn geen specifieke middelen/capaciteit geraamd voor dit onderwerp. Vooralsnog worden deze inspanningen bekostigd uit incidentele middelen en de staande organisatie. De projectgroep maakt inzichtelijk wat de financiële en organisatorische consequenties zijn. Deze worden voorgelegd alvorens de begrotingsprocedure 2019 (Q4 2017) start.

Portefeuillehouder
Op 12 juni jl. is bovenstaand voorstel besproken door de Veiligheidsdirectie. Na gezamenlijk beraad is Herman Meuleman als portefeuillehouder aangewezen. Dhr. Meuleman heeft vanuit deze rol de opdracht gegeven aan de projectgroep Informatieveiligheid om de financiële en organisatorische gevolgen in Q4 2017 inzichtelijk te hebben.

Bijlage(n)

1 Baseline Informatiebeveiliging Veiligheidsregio Twente (concept)
2 Plan van aanpak BVO (d.d. 3 november 2016)

Enschede, 21 juni 2017

Het dagelijks bestuur

Secretaris, H.G.W. Meuleman	Vice Voorzitter, S.W.J.G. Schelberg

---

Aldus vastgesteld in de vergadering van het algemeen bestuur d.d. 10 juli 2017

Secretaris, H.G.W. Meuleman	Voorzitter, Dr. G.O. van Veldhuizen