PROVINCIE FLEVOLAND

Mededeling

Onderwerp
Uitwerking aanbevelingen informatieveiligheid

Registratienummer
1977437
Datum
12 oktober 2016
Auteur
drs. G. de Vos
Afdeling/Bureau
BDO

Openbaarheid
Passief openbaar

Portefeuillehouder
Rijsberman, M.A.

Ter kennisname aan PS en burgerleden

Kern mededeling:
De commissie Bestuur heeft op 28 september 2016 gesproken over het onderzoeksrapport van de Randstedelijke Rekenkamer (RRK) *Informatieveiligheid.* Daarbij adviseert de commissie om de aanbevelingen te verduidelijken. Met de griffie heeft het college deze aanbevelingen uitgewerkt. Daarbij is aansluiting gezocht bij de bestuurlijke reactie van het college.

Mededeling:

De aanbevelingen van de Randstedelijke Rekenkamer zijn via Provinciale Staten gericht aan het college. GS wordt gevraagd de aanbevelingen uit te werken. In bijgevoegde mededeling aan Provinciale Staten wordt deze informatie toegevoegd, voorafgaand aan de besluitvorming over dit onderzoek. Deze is geagendeerd op 26 oktober 2016.

De aanpak van Gedeputeerde Staten hebben wij verwoord in de bestuurlijke reactie. Aan de hand van de vier beslispunten genoemd onder beslispunt 3 van het staten voorstel verduidelijken wij die beantwoording op hoofdlijnen. Jaarlijks rapporteren wij op hoofdlijnen over de voortgang van de uitvoering van de aanbevelingen van de rekenkameronderzoeken. Meestal vindt dit plaats bij de jaarrekening. Voor dit onderzoek wordt voorgesteld aanvullende informatie over de voortgang op te nemen in de paragraaf Bedrijfsvoering, onderdeel informatievoorziening, van de begroting 2018.

1a.
Vraag GS om ervoor te zorgen dat rollen en verantwoordelijkheden bij informatieveiligheid door de gehele organisatie goed worden ingevuld.

Op concernniveau zijn de afgelopen zomer deze systemen geïnventariseerd en de directie verwacht dat in 2017 de tien meest kritische systemen zijn aangepakt en van betere beveiliging voorzien. In de afdelingsplannen voor 2017 wordt aandacht besteed aan het aspect informatievoorziening / -veiligheid. Deze activiteit is voor 1 februari 2017 afgerond. Daarbij wordt de afdelingen gevraagd te beschrijven:
1. Van welke systemen de afdeling gebruik maakt.
2. Voor welke systemen de afdeling verantwoordelijk is.
3. Wie van deze systemen is aangewezen als systeemeigenaar en hoe deze rol wordt ingevuld
4. Welke de relevante risico's van de tien meest kritische systemen zijn en welke beheersmaatregelen daarvoor worden geformuleerd.

1b.
Vraag GS om u te informeren over de invulling van rollen en verantwoordelijkheden
en de scheiding van functies bij informatieveiligheid.

Bij het vaststellen van het informatiebeveiligingsbeleid in mei 2015 is de volgende rolverdeling vastgelegd:
1. de directie is verantwoordelijk voor het vaststellen van het beleid;
2. het voorbereiden en toetsen van het beleid zijn belegd bij de adviseur informatieveiligheid;
3. het uitvoeren en verbeteren ligt bij de afdelingshoofden / systeemeigenaren.

Mededeling

4. In 2017 wordt deze tweejaarlijkse beoordeling uitgevoerd.

Bij de ontwikkeling van de concernbrede informatievoorziening heeft de directie in juni 2016 besloten om de controlerende rol - met name de tweejaarlijkse onafhankelijke toetsen - onder de verantwoordelijkheid van de concerncontroller te brengen. Er zijn geen aanvullende verbeteractiviteiten nodig.

2a.
Vraag GS om te bewaken dat alle generieke maatregelen voor informatieveiligheid zo snel mogelijk worden uitgevoerd.

1. Alle geïdentificeerde maatregelen zijn geïnventariseerd en geprioriteerd voor de komende vier jaren.
2. De maatregelen met een hoog risico worden in 2016 gemitigeerd.
3. De maatregelen met een midden risico worden in 2017 ter hand genomen.
4. De directie monitort maandelijks de uitvoering van de door haar vastgestelde verbeteracties.
5. Eind 2017 wordt een onafhankelijke beoordeling uitgevoerd over de mate waarin de informatievoorziening en de informatieveiligheid op orde zijn.

2b.
Vraag GS om te bewaken dat voor alle processen en systemen wordt bepaald of een risicoanalyse nodig is, dat deze risicoanalyses worden uitgevoerd en dat aan vullende maatregelen die daaruit voortkomen, worden uitgevoerd.

1. De systemen zijn geïnventariseerd (juli 2016).
2. De eerder genoemde IV-Raad heeft de tien meest kritische systemen bepaald (september 2016).
3. dat elke systeemeigenaar van een kritisch systeem in het eigen afdelingsplan een aanpak voor de beheersing van dat systeem opstelt. De directie bespreekt de te nemen aanvullende maatregelen (september 2017).
4. De beheersmaatregelen worden vergeleken met de andere provincies via de interprovinciale monitor.
5. Beoordeeld wordt waar kan worden samengewerkt.