Gemeente Oegstgeest

Initiatiefvoorstel van het presidium

onderwerp	Initiatiefvoorstel verbetering informatiebeveiliging
zaaknummer	Z/21/149192
team	Griffie
opgesteld door	S .Dewkalie
datum voorstel	13 september 2021
datum raad	28 oktober 2021

Het presidium stelt de raad voor het volgende te besluiten:

voorstel

de aanbevelingen van de Rekenkamercommissie over te nemen en het college op te dragen om:

1) de IT-netwerken te versterken door de geconstateerde kwetsbaarheden op te heffen;
2) minimaal jaarlijks risicoanalyses, penetratietesten en kwetsbaarhedenscans uit te voeren;
3) systematisch operationele procedures te beoordelen, systematisch de risico's met verbonden partijen te inventariseren, en het informatiebeveiligingsbeleid zo nodig aan te passen;
4) het verwerkingsregister volledig en/of geactualiseerd te maken;
5) de informatiebeveiligingsrisico's en beheersingsmaatregelen op te nemen in de paragraaf Weerstandsvermogen en in een speciale paragraaf informatiebeveiliging in de gemeentelijke programmabegroting;
6) sluitende afspraken te maken met verbonden partijen op het gebied van informatiebeveiliging;
7) kennisuitwisseling over informatiebeveiliging te stimuleren tussen FG's, CISO's en verbonden partijen;
8) jaarlijks afzonderlijk te rapporteren over informatiebeveiliging en privacybeleid, en de betrokkenheid van de gemeenteraad hierbij te vergroten (bijvoorbeeld door training).

Toelichting voorstel

inleiding

De Rekenkamercommissie WVOLV publiceerde in april 2021 de resultaten van een onderzoek naar de informatiebeveiliging van de gemeenten Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg, alsmede van hun verbonden partijen.
Gemeente Oegstgeest heeft het beleid rondom informatiebeveiliging op orde, maar de uitvoering ervan kan beter. Daartoe doet de Rekenkamercommissie acht aanbevelingen.

beoogd effect

Een betere bescherming van privacygevoelige informatie van burgers en ondernemers. Bijvoorbeeld over gezondheid, financiën en eventuele contacten met Justitie.

argumenten

Organisaties zijn wettelijk verplicht zorgvuldig met privacygevoelige informatie van burgers en ondernemers om te gaan. Uit eerder rekenkameronderzoek uit 2016 bleek dat er wat betreft informatiebeveiliging en privacy nog ‘grote stappen nodig’ waren in de vier gemeenten.

Het nieuwe rekenkameronderzoek bracht onder meer aan het licht dat de gemeentelijke IT-netwerken kwetsbaar zijn en dat er te weinig risicoanalyses worden uitgevoerd. Ook beoordelen de gemeenten niet-systematisch procedures, en mogen zij meer sturing geven aan het informatiebeveiligingsbeleid van organisaties waarin zij zeggenschap hebben.

kanttekeningen

NVT

financiën

NVT

duurzaamheid

NVT

communicatie of vervolg

Het informeren van de verbonden partijen en Rekenkamercommissie WVOLV over het genomen raadsbesluit en de vervolgacties hieruit.

publieks-samenvatting	De gemeenteraad heeft besluiten genomen die ertoe bijdragen dat privacygevoelige informatie van burgers en ondernemers beter beschermd wordt.
bijlage(n)	- 2021-02-08-IBP-Rekenkameronderzoek-Informatiebeveiliging-WVOLV - 2020-05-18-Brief-raadsleden-en-commissieleden-over-onderzoek-informatiebeveiliging - 2021-04-26-Aanbiedingsbrief-van-RKC-WVOLV-over-onderzoek-informatiebeveiliging - 2021-04-08-Bestuurlijke-reactie-van-Oegstgeest-op-concept-aanbiedingsbrief-en-eindrapportage-informatiebeveiliging - 2021-04-28-Persbericht-van-RKC-WVOLV-over-onderzoek-naar-informatiebeveiliging - https://www.rekenkamerwvolv.nl/informatiebeveiliging-van-gemeenten-en-verbonden-partijen/

Raadsbesluit

onderwerp	Initiatiefvoorstel verbetering informatiebeveiliging
zaaknummer	Z/21/149192
team	Griffie
opgesteld door	S. Dewkalie
datum voorstel	13 september 2021
datum besluit	28 oktober 2021

De gemeenteraad van Oegstgeest;

gelezen het voorstel van het presidium ;

gelet op de beraadslaging in de commissie Burger van oktober 2021;

besluit de aanbevelingen van de Rekenkamercommissie over te nemen en het college op te dragen om:

1. de IT-netwerken te versterken door de geconstateerde kwetsbaarheden op te heffen;
2. minimaal jaarlijks risicoanalyses, penetratietesten en kwetsbaarhedenscans uit te voeren;
3. systematisch operationele procedures te beoordelen, systematisch de risico's met verbonden partijen te inventariseren, en het informatiebeveiligingsbeleid zo nodig aan te passen;
4. het verwerkingsregister volledig en/of geactualiseerd te maken;
5. de informatiebeveiligingsrisico's en beheersingsmaatregelen op te nemen in de paragraaf Weerstandsvermogen en in een speciale paragraaf informatiebeveiliging in de gemeentelijke programmabegroting;
6. sluitende afspraken te maken met verbonden partijen op het gebied van informatiebeveiliging;
7. kennisuitwisseling over informatiebeveiliging te stimuleren tussen FG's, CISO's en verbonden partijen;
8. jaarlijks afzonderlijk te rapporteren over informatiebeveiliging en privacybeleid, en de betrokkenheid van de gemeenteraad hierbij te vergroten (bijvoorbeeld door training).

Aldus besloten in de openbare vergadering van de raad van Oegstgeest op 28 oktober 2021.

de griffier de voorzitter