Raadsleden en informatie-beveiliging

April 2025

Risico

Waarom is informatiebeveiliging belangrijk?

Gemeenten draaien op informatie. Zonder informatie stokt de dienstverlening aan inwoners en bedrijven. De openbare orde kan worden verstoord.

Bovendien neemt de cyberdreiging toe. En gemeenten zijn vanaf eind 2025 wettelijk verplicht om risico's in kaart te brengen en adequate maatregelen te nemen. Doen ze dat niet, dan kunnen sancties volgen op grond van de Cyberbeveiligingswet.

Daarom is het belangrijk dat gemeenten hun informatie en systemen goed op orde hebben en beveiligen. Als raadslid kunt u veel invloed uitoefenen op informatiebeveiliging. Organiseer uw betrokkenheid, laat u informeren, weet wat u kan vragen en benut hulpmiddelen.

Wat kan ik als raadslid doen?

- Zet 'informatiebeveiliging' regelmatig op de agenda van de raad. Bespreek dit met de griffier en de agendacommissie. Agendeer de jaarlijkse rapportage over informatiebeveiliging en datakwaliteit. Met deze rapportage, op basis van de ENSIA-methode, verantwoordt het college zich aan de raad. Behandel deze rapportage niet als 'ingekomen stuk'; de auditor controleert niet alle onderdelen.
- Vraag om een informatieavond of themasessie naar aanleiding van de jaarlijkse rapportage over informatiebeveiliging en datakwaliteit of rondom de bespreking van de voorjaars- of najaarsnota.
- Maak gebruik van het budgetrecht: Stellen we voldoende mensen en middelen ter beschikking?

- ☑ Stel de vraag: Kunnen we samenwerken met- of in het geval van een calamiteit uitwijken naar een andere gemeente?

- ☑ Stel vragen naar aanleiding van de jaarlijkse rapportage over informatiebeveiliging en datakwaliteit, jaarstukken, de voorjaars- of najaarsnota:

  - Welke systemen en processen mogen nooit stilvallen in onze gemeente? Het verstrekken van uitkeringen, uitgifte van paspoorten, het ophalen van afval, bedienen van bruggen en sluizen?
  - Wat zijn de belangrijkste risico's voor deze systemen en processen?
  - Welke maatregelen nemen we om deze risico's te 'managen'? Volstaan deze maatregelen?

- ☑ Stel kaders, bijvoorbeeld direct na de verkiezingen, naar aanleiding van de politieke agenda van de raad. Bij de begroting, bij beleids- en besluitvorming in de dagelijkse praktijk. Leg de kaders vast in het integraal veiligheidsplan.

- ☑ Beleg, als raad, dit onderwerp in een portefeuille of in een (audit)commissie.

- ☑ Maak gebruik van ondersteuning van de griffie, bekijk het aanbod van de VNG en van de Nederlandse Vereniging voor Raadsleden.

Over de ENSIA-methode

- Alle Nederlandse gemeentebesturen leggen jaarlijks, op hetzelfde moment, via dezelfde methode, verantwoording af over hun informatieveiligheid, datakwaliteit en data-integriteit.
- Zij verantwoorden zich via de ENSIA-methode aan de gemeenteraad en aan toezichthouders binnen de rijksoverheid.
- Het verantwoordingsmoment is dan ook hét vaste jaarlijkse moment waarop het college, risicogericht, de noodzakelijke verbeteringen doorvoert in de eigen organisatie. De VNG faciliteert gemeenten hierbij met collectieve producten en diensten vanuit o.a. de teams ENSIA en ADV en vanuit de Informatiebeveiligingsdienst (IBD).
- De gemeentelijke ENSIA-coördinator zorgt ervoor, dat alle beschikbare informatie gestroomlijnd samenkomt bij (de portefeuillehouder van) het college en de toezichthouders.
- Naast de verantwoordingsrapportage kunnen ook experts zoals de CISO en applicatie-beheerders aanvullend inzicht geven in de stand van zaken en in noodzakelijke verbeteringen.

Meer informatie

- Informatie over de manier waarop het college van burgemeester en wethouders jaarlijks verantwoording aflegt aan de raad over informatiebeveiliging en datakwaliteit via een jaarlijkse rapportage. ENSIA | VNG
- Tips voor raadsleden met de portefeuille veiligheid | Nederlandse Vereniging voor Raadsleden
- Informatie voor raadsleden over de bredere context van digitale veiligheid, inclusief weerbaarheid van inwoners en ondernemers. Checklist-raadsleden-digitale-veiligheid.pdf
- Praktisch, ondersteunend aanbod van de Informatiebeveiligingsdienst van de VNG voor de ambtelijke organisatie. De Baseline Informatiebeveiliging Overheid versie 2 (BIO2) is het nieuwe kader voor informatiebeveiliging binnen de overheid, waar gemeenten aan moeten voldoen. Aan de slag met de BIO2: gebruik de IBD-ondersteuningspoducten - Informatiebeveiligingsdienst