

REKENKAMERS



Aan de raad van de gemeente Westerveld
Postbus 50
7970 AB HAVELTE

Nieuwleusen, 2 juli 2026

Geachte raadsleden,

Hierbij bieden wij u namens de Rekenkamer Westerveld het onderzoeksrapport over het rekenkameronderzoek 2025 inzake de informatiebeveiliging van de gemeente Westerveld aan.

Het onderzoek maakt deel uit van een gezamenlijk initiatief van de personele unie van de rekenkamers van Meppel, Staphorst, Steenwijkerland en Westerveld. Voor iedere gemeente is een afzonderlijk onderzoek uitgevoerd. Het voorliggende rapport bevat uitsluitend de bevindingen voor Westerveld.

Voordat wij ingaan op de inhoud van het onderzoek, willen wij stilstaan bij de totstandkoming van dit rapport. Het rapport bereikt u later dan wij als rekenkamer hadden gewenst. De oorzaak hiervan ligt onder meer in de wisseling van raad en college gedurende het onderzoeksproces en de zorgvuldige afstemming die heeft plaatsgevonden tussen de betrokken gemeenten, de griffiers, de onderzoekers en de rekenkamers over de omgang met gevoelige informatie. Die zorgvuldigheid vonden wij noodzakelijk, maar heeft geleid tot vertraging.

De rekenkamer realiseert zich dat dit onderzoek een relatief technisch karakter heeft. Informatiebeveiliging is een specialistisch vakgebied waarin technische, organisatorische en juridische aspecten samenkomen. Om de toegankelijkheid van het rapport te vergroten, is daarom een managementsamenvatting opgenomen waarin de belangrijkste conclusies, risico's en aanbevelingen overzichtelijk zijn weergegeven.

De centrale conclusie van het onderzoek is overwegend positief. De onderzoekers constateren dat de gemeente Westerveld informatiebeveiliging serieus neemt en dat de afgelopen jaren belangrijke stappen zijn gezet om de digitale weerbaarheid van de organisatie te versterken. Binnen de organisatie is sprake van een groot bewustzijn van het belang van informatiebeveiliging en op organisatorisch, technisch en

fysiek vlak zijn veel maatregelen getroffen om de informatievoorziening te beschermen. De basis is daarmee aanwezig om de informatiebeveiliging verder door te ontwikkelen en duurzaam te borgen. Daarbij constateren de onderzoekers dat verdere versterking noodzakelijk blijft. De aanbevelingen richten zich onder meer op het verder versterken van de governance rondom informatiebeveiliging, het beter borgen van beleid en processen, het verder ontwikkelen van risicomanagement en het vergroten van de aantoonbaarheid van de getroffen beheersmaatregelen. Daarnaast vragen de onderzoekers aandacht voor de inrichting van business continuity management, leveranciersmanagement en het structureel evalueren en verbeteren van de informatiebeveiliging. Deze aanbevelingen dragen eraan bij dat de gemeente haar digitale weerbaarheid ook op de langere termijn kan blijven waarborgen.

De onderzoekers constateren daarnaast dat de gemeenteraad een belangrijke rol vervult bij het versterken van de digitale weerbaarheid van de gemeente. Daarbij merken zij op dat de ENSIA-verantwoording slechts een beperkt beeld geeft van de feitelijke staat van de informatiebeveiliging, omdat deze grotendeels is gebaseerd op zelfevaluaties en zich voornamelijk richt op de opzet en het bestaan van beheersmaatregelen. Om de kaderstellende en controlerende rol goed te kunnen vervullen, is het daarom van belang dat de raad het onderwerp informatiebeveiliging regelmatig bespreekt en zich hierover periodiek laat informeren, bijvoorbeeld door de CISO.

De rekenkamer onderschrijft de conclusies en aanbevelingen van het rapport. Daarbij merken wij op dat het rapport een groter aantal aanbevelingen bevat dan gebruikelijk is bij rekenkameronderzoeken. Dit hangt rechtstreeks samen met het technische karakter van het onderwerp. Veel aanbevelingen hebben betrekking op operationele en specialistische onderdelen van informatiebeveiliging en zijn primair gericht aan het college van burgemeester en wethouders en de ambtelijke organisatie.

De rekenkamer adviseert uw raad daarom niet om zich op het niveau van afzonderlijke technische maatregelen uit te spreken. Veel van de aanbevelingen vragen specialistische kennis en raken de inrichting van processen, systemen en beveiligingsmaatregelen. Wij geven uw raad in overweging het college de ruimte te bieden om, binnen de bestuurlijke kaders die de raad stelt, een eigen afweging te maken over de wijze waarop en de volgorde waarin de aanbevelingen worden overgenomen en uitgevoerd.

De rol van de raad ligt daarbij primair in het beoordelen van de richting en de ambitie van de voorgestelde verbeteringen. De vraag voor de raad is niet zozeer welke technische maatregel moet worden getroffen, maar of het college voldoende doet om de digitale weerbaarheid van de gemeente duurzaam te versterken, risico's beheersbaar te houden en de continuïteit van de gemeentelijke dienstverlening te waarborgen. De verantwoordelijkheid van de raad ligt daarmee vooral in het stellen van kaders, het volgen van de voortgang en het bewaken van de resultaten.

Juist op dat punt heeft uw raad een belangrijke rol. Digitale veiligheid is niet uitsluitend een technische of ambtelijke aangelegenheid, maar nadrukkelijk ook een bestuurlijke verantwoordelijkheid. De gemeenteraad vervult hierin een belangrijke kaderstellende en controlerende rol door het onderwerp regelmatig te agenderen, prioriteiten te stellen, toe te zien op de beheersing van digitale risico's en ervoor te zorgen dat voldoende middelen beschikbaar zijn om de digitale weerbaarheid van de gemeente te versterken.

Wij bevelen uw raad daarom aan om:

- informatiebeveiliging structureel en regelmatig op de bestuurlijke agenda te plaatsen, hierover actief het gesprek te voeren met het college en bij de behandeling van de begroting blijvend

aandacht te hebben voor voldoende middelen om de informatiebeveiliging en digitale weerbaarheid van de gemeente verder te versterken;

- gebruik te maken van de beschikbare handreikingen en hulpmiddelen van de VNG om invulling te geven aan de kaderstellende en controlerende rol van de raad;
- periodiek met het college en de CISO in gesprek te gaan over de ontwikkeling van de digitale weerbaarheid en de beheersing van risico's.

De rekenkamer benadrukt dat de aanbevelingen niet moeten worden gezien als een aanwijzing voor tekortschietend functioneren. Integendeel, zij zijn vooral gericht op het verder versterken en professionaliseren van een organisatie die op veel onderdelen al een solide basis heeft gelegd. Wij danken alle betrokken bestuurders, medewerkers en overige gesprekspartners voor hun openheid en medewerking aan dit onderzoek.

Wij hopen dat dit rapport bijdraagt aan een constructieve bespreking van de digitale weerbaarheid van onze gemeente.

Indien uw raad daaraan behoefte heeft, is de rekenkamer graag bereid het onderzoek, de conclusies en de aanbevelingen nader toe te lichten tijdens een bijeenkomst van uw raad of een commissie. Uiteraard zijn wij daarbij ook beschikbaar om vragen over het onderzoek en de bevindingen te beantwoorden.

Met vriendelijke groet,

Namens de rekenkamer Westerveld,

5.1.2e

5.1.2e

Voorzitter



Bijlage:

- Rekenkameronderzoek Informatiebeveiliging Gemeente Westerveld
- Bestuurlijke reactie conceptrapport college Westerveld d.d. 17 februari 2026

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	3