

REKENKAMER



De gemeenteraad Steenwijkerland
Postbus 162
8330 AD Steenwijk

- per mail verzonden -

Nieuwleusen, 22 juni 2026

Onderwerp: rekenkamerrapport 2025

Geachte raadsleden,

Hierbij bieden wij u namens de rekenkamer Steenwijkerland het onderzoeksrapport over de informatiebeveiliging van de gemeente Steenwijkerland aan.

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 onderzoekers en de rekenkamers over de omgang met gevoelige informatie. Die zorgvuldigheid vonden wij noodzakelijk, maar heeft geleid tot vertraging.

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 Steenwijkerland.

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. Steenwijkerland beschikt over een goed doordachte en breed gedragen aanpak van informatiebeveiliging. Binnen de organisatie is sprake van een hoog bewustzijnsniveau en informatiebeveiliging heeft een duidelijke plaats binnen de bestuurlijke en ambtelijke organisatie. De onderzoekers constateren dat de gemeente op veel onderdelen volwassen opereert en dat medewerkers en management zich verantwoordelijk tonen voor een veilige informatievoorziening.

Tegelijkertijd laat het onderzoek zien dat verdere versterking noodzakelijk blijft. De belangrijkste aandachtspunten liggen op het gebied van risicobeheer, crisisvoorbereiding, de beheersing van hybride en cloudomgevingen, de actualiteit van beleid en documentatie en de borging van kennis en verantwoordelijkheden. Ook wordt aandacht gevraagd voor de continuïteit van kritische processen bij cyberincidenten en voor het verder formaliseren van procedures en afspraken.

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 speelt een belangrijke rol bij het stellen van kaders, het bewaken van prioriteiten en het beschikbaar stellen van voldoende middelen.

Wij bevelen uw raad daarom aan om:

- informatiebeveiliging structureel en ten minste jaarlijks op de bestuurlijke agenda te plaatsen;
- duidelijke kaders en doelstellingen vast te stellen voor digitale veiligheid en weerbaarheid;
- blijvend aandacht te hebben voor de benodigde financiële en organisatorische randvoorwaarden;
- actief gebruik te maken van de kennis, instrumenten en handreikingen die onder meer door de VNG beschikbaar worden gesteld.

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.

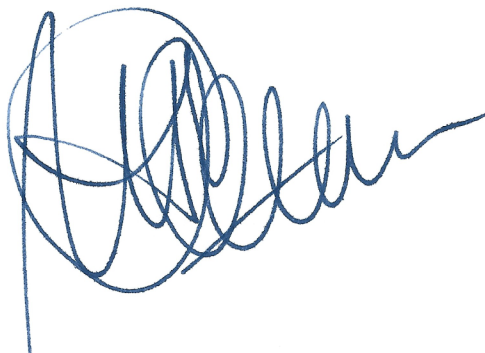
Wij danken alle betrokken bestuurders, medewerkers en overige gesprekspartners voor hun openheid en medewerking aan dit onderzoek.

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 Steenwijkerland

Herman Odink
Voorzitter



Bijlage:

- Rekenkameronderzoek Informatiebeveiliging Gemeente Steenwijkerland
- Bestuurlijke reactie conceptrapport college Steenwijkerland d.d. 17.02.2026