



Aan de Personele unie van rekenkamers Meppel, Staphorst, Steenwijkerland, Westerveld (MSSW)
t.a.v. 5.1.2e voorzitter
PER E-MAIL
In cc: per e-mail: ambtelijk secretaris rekenkamer

Datum
17 februari 2026

Ons kenmerk
2026-002756

Uw brief/kenmerk

Onderwerp
Bestuurlijke reactie Rapport Rekenkameronderzoek Informatiebeveiliging Gemeente Westerveld
d.d. 27-1-2026 (v1.0)

Geachte 5.1.2e

Op vrijdag 30 januari 2026 ontvingen wij van u het Rapport Rekenkameronderzoek Informatiebeveiliging Gemeente Westerveld. Allereerst willen wij u danken voor de uitgebreide evaluatie die de Rekenkamer heeft uitgevoerd. Graag geven wij onze bestuurlijke reactie op het rapport.

Algemene conclusie:

Als wij het rapport beschouwen vanuit de vier hoofdthema's van de BIO2, te weten: organisatorisch, menselijk, fysiek en technologisch, zijn wij blij dat dit - met een aantal kanttekeningen - een overwegend positief beeld geeft en (deels) voor ons herkenbaar is.

U schrijft dat het rapport is ingestoken op basis van feiten en bevindingen. Hierbij merken wij op dat bevindingen doorgaans geconstateerd worden vanuit een toetsingskader. Aangezien het toetsingskader onvoldoende in het onderzoek is gedefinieerd - althans geeft het rapport daar geen duidelijkheid over - is het naar onze mening niet mogelijk een normgerichte beoordeling te doen. Daarnaast ontbreekt in het rapport een onderbouwing voor het al dan niet relevant zijn van geconstateerde feiten en observaties.

Door het ontbreken van een vooraf gestelde norm of ander richtinggevend kader kunnen wij geen duidelijke en eenduidige conclusies trekken uit de antwoorden op de gestelde onderzoeksvragen (hoofd- en deelvragen). Wij missen daarnaast een benchmarkvergelijking, waardoor de gegeven antwoorden niet leiden tot een concreet en toetsbaar antwoord en handelingsperspectief. Daarnaast ontbreekt in de meeste gegeven antwoorden een onderbouwing voor het belang en relevantie van het onderwerp.

In uw uitvraag van bestuurlijke wederhoor schrijft u dat om een ambtelijke reactie is gevraagd. Navraag leert dat u deze ambtelijke reactie op 14 januari 2026 heeft ontvangen. In uw rapport is niet terug te lezen of en zo ja in hoeverre de opmerkingen uit de ambtelijke reactie zijn overgenomen. Voor de volledigheid zijn de opmerkingen uit de ambtelijke reactie (op v0.9 van het rapport) als bijlage toegevoegd.

Zoals hierboven aangegeven herkennen wij (deels) de bevindingen en onderschrijven de noodzaak om onze digitale weerbaarheid verder te versterken, mede gezien de eisen uit de Cyberbeveiligingswet en het toenemende cyberdreigingsbeeld. Het rapport laat zien dat er binnen onze organisatie veel inzet en bewustzijn aanwezig is, maar dat verdere professionalisering noodzakelijk is op het gebied van governance, risicobeheer, continuïteit en samenwerking met SSC-Ons. Het rapport geeft helaas geen advies over hoe daarin voorzien kan worden. Vanwege het ontbreken van concrete oplossingen en een handelingsperspectief, hebben wij op basis van de aanbevelingen onderstaande punten geformuleerd.

Opvolging van de aanbevelingen

1. Governance en managementsysteem

Het college neemt de aanbeveling over om het managementsysteem voor informatiebeveiliging verder in te richten conform ISO 27001. Wij zullen de 'check'- en 'act'-fasen structureel versterken, tussentijdse verantwoording borgen en risicobeheer professionaliseren. De status hiervan zal worden opgenomen in onze P&C cyclus en in het jaarverslag.

2. Risicobeheer en continuïteit

Wij stellen de kritieke processen en systemen formeel vast en blijven werken aan, en verbeteren van, onze draaiboeken voor continuïteit. Samen met SSC-Ons zullen wij de continuïteitsplannen afstemmen en gezamenlijke crisisoefeningen organiseren. Ook wordt gewerkt aan een integraal risicobeeld.

3. Samenwerking met SSC-Ons

Het college zal in het Bedrijfsvoeringsberaad nadrukkelijker sturen op de belangrijkste beveiligingsrisico's voor Westerveld. Wij gaan met SSC-Ons in gesprek over betere communicatie bij wijzigingen en incidenten. Daarnaast wordt toegewerkt naar duidelijke referentieprofielen voor autorisatiebeheer.

4. Privacy en gegevensbescherming

We herkennen de achterstand in het uitvoeren van DPIA's. De achterstand in DPIA's en verwerkersovereenkomsten wordt risicogebaseerd weggewerkt. Wij onderzoeken de inzet van extra capaciteit en samenwerking binnen de regio. Ook zal het register van verwerkingen periodiek worden geactualiseerd en bijgehouden.

5. Mensgerichte maatregelen

Het college onderschrijft de noodzaak van doelgroepgerichte trainingen en structurele aandacht voor veilig gedrag. Wij zullen het management nadrukkelijker betrekken bij dit onderwerp en zorgen voor heldere communicatie over rollen, verantwoordelijkheden en beschikbare ondersteuning.

6. Fysieke en technische beveiliging

Wij zullen de maatregelen treffen om onze fysieke veiligheid te waarborgen en de maatregelen verder te verbeteren en om samen met SSC-Ons te werken aan consistentie in technische beveiligingsmaatregelen, monitoring en incidentvoorbereiding.

17 februari 2026

3 / 5

Vervolgstappen

Wij zullen als college:

- een uitvoeringsplan laten opstellen waarin alle aanbevelingen zijn uitgewerkt in concrete acties, termijnen en verantwoordelijken;
- de gemeenteraad periodiek informeren over de voortgang;
- informatiebeveiliging structureel agenderen binnen het managementteam en de P&C-cyclus.

Tenslotte

Wij zien het rapport als een waardevolle stimulans om onze informatiebeveiliging verder te versterken. Wij danken de Rekenkamer voor de analyse en de constructieve aanbevelingen en wij zetten ons in om de digitale weerbaarheid van Westerveld duurzaam te verbeteren.

5.1.2e

5.1.2e

Bijlage

Ambtelijke reactie op Rekenkamerrapport (nota van bevindingen) bevindingen.

Rekenkameronderzoek Informatiebeveiliging Westerveld, conceptversie 0.9 d.d. 2 januari 2026.

De reactie betreft de correctheid van het feitenonderzoek. Onderstaand is de ambtelijke reactie uit Westerveld weergegeven.

Pagina 4

Onjuist, er is geen wekelijkse microlearning.

Pagina 11

Punt 5 is onjuist er is een directe escalatielijn naar de directeur.

Punt 7 is onvolledig onvolledig, ieder kwartaal worden alle autorisaties gecontroleerd, wekelijks wordt het IDU (In/Doorstroom/Ui dienst) proces gecontroleerd, dit ter bescherming van ongeautoriseerde toegang.

Punt 10 is onjuist en onvolledig; er is procesmatig afgesproken dat informatiebeveiliging in projecten aan de orde komen. Er is periodiek overleg tussen het team privacy en informatiemanagement die projecten in portefeuille hebben.

Punt 12 is onjuist en onvolledig, we maken gebruik van alle functionaliteiten van de GRC tooling. Het is een weloverwogen besluit van het MT geweest om de implementatie van de tool gefaseerd uit te voeren.

Punt 13 is onjuist, de huidige ontwikkelingen geven juist meer structuur aan de samenwerking en regie in de nieuwe opzet. De term “zoekende” is feitelijk onjuist.

Pagina 12

Punt 19 is onjuist, de aanvulling “in de praktijk leidt dit weleens tot wrijving” is feitelijk niet onderbouwd. Er is met beide veiligheidsregio’s een warm contact. Feitelijk is de situatie wel zo dat in het geval van incidenten, afhankelijk van de aard en impact, we te maken kunnen krijgen met twee veiligheidsregio’s.

Punt 21 is juist, dit in tegenstelling hetgeen in punt 10 is geconstateerd.

Punt 23 is onvolledig, in het wijzigingsproces wordt de CISO niet door SSC ONS geïnformeerd.

Punt 27 is feitelijk onvolledig, er is geen duiding wat de interactie is en wat onder “beperkt” verstaan wordt.

Pagina 13

Punt 34 is onvolledig, risicobeheer is onderdeel van de P&C cyclus, feit is wel dat Informatiebeveiligingsrisico’s niet integraal in dit proces is opgenomen.

Punt 35 is onduidelijk geformuleerd, onduidelijk is welke SMART doelstellingen hiermee worden bedoeld.

Punt 36 is onvolledig en feitelijk onjuist; er wordt verantwoording afgelegd over een beperkt van de applicaties waarover verantwoording moet worden afgelegd en onder toezicht staat van een toezichthouder.

Punt 40 is onduidelijk geformuleerd, er is zeker een actueel beeld van gebruik van “decentrale” applicaties. Wel is er beperkt zicht op de aanwezigheid van “Shadow IT”.

Punt 41 is onvolledig; er vindt geen formele verantwoording over geïmplementeerde maatregelen, en de effectiviteit ervan, door ONS plaats.

Punt 42 is onjuist, ONS voert technische projecten uit of implementeert maatregelen waarbij iedere deelnemer soms de keuze heeft om hieraan mee te doen.

Pagina 14

Punt 47 is feitelijk onjuist, hier is sprake van een toekomstige situatie.

Punt 51 is onvolledig, er is niet geduid door wie (ONS of de partner) analyses van incidenten worden uitgevoerd. In geval van datalekken wordt er altijd een oorzaakanalyse uitgevoerd.

Punt 52 is onvolledig, in geval van een grootschalig incident worden de demand manager, het MT en de CISO geïnformeerd, allen zijn deelnemer in de chatgroep.

Punt 62 is feitelijk onjuist, de bevinding is feitelijk niet onderbouwd maar een conclusie.

17 februari 2026

5 / 5

Pagina 16

Punt 3 is feitelijk onjuist, er zijn specifieke trainingen binnen Leerveld aanwezig.

Punt 5 is feitelijk onjuist en suggestief in BIO 1.04 staat dat er een VOG kan worden gevraagd. Voor specifieke functies is er wel een VOG aangevraagd.

Pagina 17

Punt 9 is feitelijk onjuist, er staan iedere maand introductiebijeenkomsten gepland.

Punt 15 is onvolledig er staat niet beschreven hoe hoog het verloop feitelijk is.

Pagina 19

Punt 14 is feitelijk onjuist, zowel in de verplichte training als ook in de introductie en het personeelshandboek is het onderwerp fysieke toegangsbeveiliging als op het Intranet is dit onderwerp benoemd.

Punt 17 is onjuist, er is een protocol Aggressie en Geweld.

Punt 22 is een conclusie, feit is dat er een deugdelijke CO2 handblusser voorhanden is.

Punt 23 onvolledig, er zijn meer maatregelen getroffen om de apparatuur te beschermen.

Pagina 20

Aanbevelingen Punt 3 is overbodig, er is al een protocol Aggressie en geweld.

Bevindingen punt 3 is feitelijk onvolledig; het is onduidelijk wat onder het "meerendeel" verstaan wordt.

Punt 4 is onjuist het zaaksysteem is niet vanuit het Internet benaderbaar.

Punt 5 is onvolledig, Westerveld geeft geen apparaten uit. ONS verstrekt de middelen.

Punt 7 is onvolledig, aangezien dit een lopend project is, is de bevinding dat "bij Westerveld onbekend is welke bronnen hierop zijn aangesloten" een conclusie. Westerveld heeft een actieve rol in de stuurgroep.

Punt 9 is een toekomstige situatie, geen feitelijke situatie.

Punt 11 is onvolledig en beschreven als een toekomstige situatie.

Punt 12 is feitelijk onjuist, het betreft een toekomstige situatie.

Punt 13 is onvolledig en niet feitelijk beschreven.

Punt 15 is feitelijk niet volledig beschreven, de bevinding bevat tevens een conclusie

Pagina 23 "Achtervang voor de FG" is feitelijk onjuist, er is geen "Extern bureau".

Bijlage B Overzicht van geïnterviewden onvolledig

Er ontbreken in het overzicht 5.1.2e Gemeentesecretaris, 5.1.2e Privacy officer en 5.1.2e

5.1.2e Functionaris gegevensbescherming.

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	1, 3, 5