



Raadsvoorstel

Datum 11 november 2025

Onderwerp Rekenkamerrapport "Zwolle dataveilig?" - onderzoek naar informatieveiligheid binnen de gemeente Zwolle.

Versienummer 1

Samenvatting

Gemeenten beheren een enorme hoeveelheid (vertrouwelijke) gegevens. Inwoners moeten erop kunnen vertrouwen dat deze gegevens goed worden beschermd. Daarom gelden strenge wetten en regels voor de informatieveiligheid van gemeenten. De rekenkamer Zwolle deed onderzoek hoe de gemeente Zwolle er voor staat op dit gebied.

De rekenkamer stelt vast dat de gemeente zich in toenemende mate bewust is van het belang van informatiebeveiliging. In de afgelopen jaren zijn al goede stappen gezet. Op onderdelen is echter nog verbetering nodig. In het rapport doet de Rekenkamer hiervoor zeven gerichte aanbevelingen. Aan de gemeenteraad wordt voorgesteld deze aanbevelingen over te nemen.

Financiële gevolgen

Betreft doel 6.4.3 Informatievoorziening

Begroting wijzigen Nee

Budgetnummer -

Bijlagen

1. Rekenkamer Zwolle - Eindrapport 'Zwolle dataveilig?' - Onderzoek naar informatieveiligheid binnen de gemeente Zwolle'.
2. Infographic bij rapport 'Zwolle dataveilig?'

Openbaarheid

- ☒ Openbaar
- ☐ Geheim



Datum

11 november 2025

De raad wordt voorgesteld te besluiten om:

1. Kennis te nemen van het rekenkamerrapport "Zwolle dataveilig? Onderzoek naar informatieveiligheid binnen de gemeente Zwolle" en de aanbevelingen in het rapport over te nemen:
 1. Actualiseer en completeer het beleid op tactisch en operationeel niveau en informeer de raad hierover in het kader van de jaarlijkse ENSIA-rapportage.
 2. Benut de aanwezige systemen beter en informeer de raad hierover in het kader van de jaarlijkse ENSIA-rapportage.
 3. Waardeer de functie van CISO op naar 1,0 fte en positioneer de functie zodanig dat de CISO onafhankelijk van de lijn functioneert en een directe lijn met directie en bestuurders heeft.
 4. Versterk het risicobewustzijn en het eigenaarschap van de medewerkers op het gebied van informatieveiligheid, onder andere door e-learningen verplicht te maken.
 5. Ga met de bevindingen uit de testen aan de slag, stel hiervoor een verbeterplan (met deadlines en actiehouders) op en informeer de raad over de opvolging van de verbetermaatregelen.
 6. Voor periodiek diepgaande en fysieke testen uit op de uitwijk- en bedrijfscontinuïteitsplannen, zo nodig in samenwerking met SSC ONS.
 7. Bespreek de ambities, opzet en uitvoering van het beleid op informatieveiligheid geregeld (minimaal één keer per jaar) met elkaar. Agendeer de ENSIA-rapportage voor een vergadering van de auditcommissie en bespreek deze gelijktijdig met de boardletter van de accountant, waarin gerapporteerd wordt over de IT-audit.
2. Het college van burgemeester en wethouders opdracht te geven uitvoering te geven aan de aanbevelingen.

Datum 11 november 2025

Inleiding

De samenleving is in transitie naar een informatiesamenleving. Deze transitie brengt nieuwe kansen, maar ook een groeiend aantal risico's met zich mee. Steeds meer systemen en processen zijn gedigitaliseerd en de samenleving is hier in toenemende mate afhankelijk van geworden. Dit maakt dat informatieveiligheid een beleidsterrein is dat volop in beweging en ontwikkeling is. De accountant van Zwolle heeft in de afgelopen jaren verschillende malen gewezen op de risico's. Daarbij is vastgesteld dat in de afgelopen jaren weliswaar verbeterstappen zijn gerealiseerd, maar dat er nog veel stappen te zetten zijn om tot een kwalitatief goede beheersing van IT-risico's.

Tegen deze achtergronden heeft de rekenkamer onderzoek gedaan naar de informatieveiligheid binnen de gemeente Zwolle. Het doel van het onderzoek was inzicht te geven in de manier waarop Zwolle invulling geeft aan informatiebeveiliging en in beeld te brengen hoe het is gesteld met de informatieveiligheid van de gemeente Zwolle. Een daarvan afgeleid doel is de raad in staat te stellen zijn kaderstellende en controlerende rol op het gebied van informatiebeveiliging te kunnen uitvoeren. Het onderzoek is uitgevoerd aan de hand van de volgende onderzoeksvraag: "Hoe is het gesteld met de informatiebeveiliging van de gemeente Zwolle, wat zijn de zwakke plekken en hoe kunnen deze worden verholpen?"

Op 15 september 2025 heeft de voorzitter van de rekenkamer het rapport "Zwolle dataveilig?" aangeboden aan de gemeenteraad. Op 10 november 2025 vond het raadsdebat plaats. Aan de raad wordt voorgesteld een besluit te nemen over de opvolging van de aanbevelingen.

Kader

Niet van toepassing.

Beoogd effect

Met dit besluit geeft de raad aan hoe opvolging en uitvoering wordt gegeven aan de aanbevelingen die de rekenkamer doet in het rapport "Zwolle dataveilig?".

Argumenten

1.1 Het rapport geeft inzicht in de mate waarin de gemeente Zwolle bewust is van het belang van informatieveiligheid.

Uit het rapport blijkt dat de gemeente Zwolle zich in toenemende mate bewust is van het belang van informatiebeveiliging om zo weerbaar te zijn tegen cyberaanvallen. Er zijn in de afgelopen jaren stappen gezet op het gebied van informatieveiligheid. Er is strategisch beleid gemaakt en verantwoordelijkheden zijn goed vastgelegd. Het college en de directie dragen het belang van informatieveiligheid uit. Ook aan risicobewustzijn in de organisatie wordt aandacht besteed.

Op verschillende onderdelen is echter nog verbetering nodig om op informatiebeveiliging en privacy te kunnen voldoen aan de wettelijke verplichtingen en zo voldoende weerbaar te zijn. Dat geldt zowel voor de nu geldende als voor de binnenkort verhoogde eisen met betrekking tot de cybersecurity. De rekenkamer constateert dat het risicobewustzijn in de organisatie aanwezig is en er steeds meer inspanning wordt gepleegd om 'in control' te komen. Volledig alle risico's uitsluiten is wensdenken, maar bewust zijn van de risico's die de organisatie loopt en daarop acteren moet het streven zijn.



Datum

11 november 2025

1.2 De rekenkamer stelt vast dat verbetering nodig is om op informatiebeveiliging en privacy te kunnen voldoen aan de wettelijke verplichtingen om voldoende weerbaar te zijn.

De rekenkamer constateert dat het risicobewustzijn in de organisatie aanwezig is en er steeds meer inspanningen worden gepleegd om deze risico's te beheersen. Om op informatieveiligheid 'in control' te raken en te voldoen aan Europese en landelijke wet- en regelgeving is extra inzet en aandacht nodig. Op tactisch en operationeel niveau zijn nog lacunes aanwezig op het gebied van informatieveiligheid. Ook worden de 'tools' die op tactisch en operationeel niveau aanwezig zijn nog niet optimaal gebruikt, waardoor risico's buiten beeld blijven of niet goed vastgelegd worden.

1.3 De aanbevelingen kunnen bijdragen aan een doelmatigere en doeltreffendere uitvoering van het informatieveiligheidsbeleid.

De rekenkamer adviseert het risicobewustzijn en het eigenaarschap van de medewerkers op het gebied van informatieveiligheid te versterken. Ook kunnen de uitwijk- en bedrijfscontinuïteitsplannen voor calamiteiten beter en meer periodiek worden getest.

1.4 De aanbevelingen kunnen bijdragen aan betere grip op het proces door de raad.

De raad is nog niet goed aangesloten op beleid en uitvoering van de thema's informatieveiligheid en privacy. Bespreking van de ambities, opzet en uitvoering van het beleid en agendering van de ENSIA-rapportage voor bijvoorbeeld een vergadering van de auditcommissie kan dit inzicht vergroten.

2.1 Het is aan het college om opvolging en uitvoering te geven aan de aanbevelingen.

Met dit beslispunt wordt de opvolging van de aanbevelingen geformaliseerd.

Alternatieve mogelijkheden

De raad kan besluiten één of meer aanbevelingen niet over te nemen.

Maatschappelijk draagvlak & participatie

Niet van toepassing.

Communicatie

Bij publicatie van het rapport in september 2025 heeft de rekenkamer een persbericht verspreid. Het besluit van de raad geeft geen aanleiding voor nadere communicatie over het onderzoek.

Financiën

Dit voorstel heeft geen financiële consequenties.

Risico's

Niet van toepassing.

Vervolg

Het college geeft opvolging en uitvoering aan de aanbevelingen.

Openbaarheid

Dit raadsvoorstel en het rekenkamerrapport zijn openbaar.