GEMEENTE HILVERSUM
POSTBUS 9900
1201 GM HILVERSUM

BEZOEKADRES:
RAADHUIS
DUDOKPARK 1
TELEFOONNUMMER: 14 035
HILVERSUM.NL

Aan de rekenkamercommissie van de gemeente Hilversum

DATUM	September 2026
ZAAKNUMMER	1957328
BEHANDELD DOOR	Ferdi Struijs
TELEFOON (035)	629 2178
UW KENMERK	
BIJLAGEN	
BETREFT	Bestuurlijke reactie rekenkameronderzoek Informatieveiligheid 2025-2026

Geachte heer Derks,

Met bijzondere aandacht heeft het college kennisgenomen van het rapport van de Rekenkamer Hilversum over de informatiebeveiliging binnen onze gemeente. Het college waardeert de uitgebreide analyse, de kritische blik en de aanbevelingen die in het rapport zijn opgenomen. Digitalisering en gegevensbescherming vormen essentiële pijlers voor de gemeentelijke dienstverlening. We dragen immers in grote mate de verantwoordelijkheid voor belangrijke gegevens die we op een veilige manier moeten verwerken. Alle maatregelen die we nemen op het gebied van informatiebeveiliging zijn gericht op een ononderbroken dienstverlening aan inwoners, bedrijven en ketenpartners. Het is voor gemeenten in steeds grotere mate een uitdaging om daaraan te voldoen. Dit onderzoek helpt bij het verder inzichtelijk krijgen van de risico's en het nemen van maatregelen door het College van B en W.

Algemene reflecties

Het rapport laat zien dat de gemeente de afgelopen jaren stappen heeft gezet, en dat er tegelijk nog verschillende verbetermogelijkheden zijn om aan de vereisten rondom informatiebeveiliging te voldoen. Waaronder de Baseline Informatiebeveiliging Overheid (de nieuwe BIO2) die sinds 15 augustus 2026 wettelijk verankerd is via de Cyberbeveiligingswet (Cbw).

Reflectie op de aanbevelingen van de Rekenkamer aan het college

1. Zorg voor een volledig informatiebeveiligingsbeleid, dat aan de geldende wettelijke normen voldoet en is uitgewerkt in werkprocessen

Op 5 maart 2025 heeft de gemeenteraad het Strategisch gegevensbescherming en informatiebeveiligingsbeleid 2025-2029 vastgesteld. Dit is het bestuurlijk kader om voor de komende

periode de uitwerking te kunnen maken naar de tactische en operationele laag binnen de gemeentelijke organisatie, inclusief de vertaling naar werkprocessen en –instructies.

De onderzoeker constateert dat op sommige thema's beleid ontbreekt, met daarbij als belangrijke kanttekening dat het wel aannemelijk wordt geacht dat deze in de organisatie als werkproces aanwezig zijn c.q. in de operatie geborgd zijn. In deze gevallen zal de gemeente de uitvoeringspraktijk in beleid gaan borgen. Het doel is om de komende jaren (binnen de termijn van de werkingsduur van het strategisch beleidskader) het beleid te actualiseren en verder in lijn te brengen met de vereisten uit de BIO, Cbw en Wwke[1]. Hierbij wordt geprioriteerd op basis van reële risico's.

2. Zorg dat het informatiebeveiligingsbeleid is toegerust voor de overgang naar toekomstige wetgeving.

Het signaleren, beoordelen en vertalen van wijzigingen in wet- en regelgeving is onderdeel van het reguliere takenpakket van de chief information security officer (CISO), in samenspraak met de chief information officer (CIO). Sinds 15 augustus 2026 is de Cbw van kracht. De organisatie is begin 2026 gestart met een verdere impactanalyse van de invoering van deze wet om te bepalen welke aanvullende maatregelen er nodig zijn ten opzichte van de huidige situatie.

Onderdeel van de aanpak is het verder in beeld brengen en beheersen van de belangrijkste informatiebeveiligingsrisico's en het risico gestuurd prioriteren van de benodigde maatregelen vanuit de Cbw. Zo is voldaan aan de registratieplicht en er kan voldaan worden aan de meldplicht. De organisatie zet stappen om op de volle breedte aan de eisen van de Cbw te voldoen. Het zwaartepunt van de implementatie en borging ligt in 2027. Verankering in processen, werkwijze en governance vindt gefaseerd plaats.

Net als Hilversum bevinden alle gemeenten zich op dit moment in de verdere implementatie van BIO2 en Cbw. Wat wel specifiek is voor Hilversum is dat de fusie met Wijdemeren vanuit informatiebeveiliging nog een hoge mate van betrokkenheid bij een zorgvuldige en ordentelijke overdracht van gegevens vraagt.

Het College van B en W constateert dat de gemeentelijk organisatie – mede naar aanleiding van het eindrapport van de rekenkamer - belangrijke stappen heeft gezet om de positie van de gemeentelijke organisatie qua informatiebeveiliging verder te versterken.

Direct na de eerste bevindingen zijn technische kwetsbaarheden met hoge prioriteit opgepakt en waar mogelijk direct opgelost. Daarnaast heeft de raad in de Voorjaarsnota jaarlijks structureel een bedrag van € 150.000 beschikbaar gesteld, waarmee op korte termijn reeds de voorbereidende werkzaamheden gestart zijn om te komen tot een centrale voorziening voor monitoring en analyse van beveiligingsmeldingen. Daarmee wordt het technische fundament van de organisatie versterkt en kunnen signalen sneller worden herkend, opgevolgd en waar nodig direct worden vertaald naar actie.

Tegelijkertijd vraagt informatiebeveiliging meer dan techniek alleen. Een goed ingerichte monitoring en respons oplossing ondersteunt medewerkers en het management bij het tijdig signaleren en afhandelen van risico’s, maar vervangt niet de menselijke alertheid, deskundigheid en verantwoordelijkheid voor opvolging van de meldingen in de organisatie. Juist de combinatie van technische monitoring, processen

[1] Onder de Wet weerbaarheid kritieke entiteiten (Wwke) worden we als gemeente aangewezen als kritieke entiteit die onder de eisen van de Cbw valt. Daarbij gaat om weerbaarheid tegen relevante door de natuur of door de mens veroorzaakte dreigingen, die dienstverlening aanzienlijk zou kunnen verstoren.

waarin gegevensbescherming en informatiebeveiliging geborgd zijn, bewust en veilig gedrag van alle betrokkenen en blijvende bestuurlijke aandacht maakt dat de gemeente stap voor stap kan toewerken naar een robuustere informatiebeveiliging en naleving van de Cyberbeveiligingswet (Cbw).

Het college onderschrijft dat informatiebeveiliging een organisatiebrede en tevens bestuurlijke verantwoordelijkheid is. Van medewerkers en bestuurders wordt verwacht dat zij zorgvuldig omgaan met informatie en de geldende beveiligingsprocedures naleven. De raad is verantwoordelijk voor het stellen van kaders en het beschikbaar stellen van middelen. Het college voert deze kaders uit en zorgt voor de verdere organisatorische inbedding en uitvoering binnen de gemeentelijke organisatie. Juist deze samenhang tussen verantwoordelijkheid, kaderstelling, middelen en uitvoering is noodzakelijk om de beveiliging van de gegevens van inwoners, bedrijven en ketenpartners duurzaam te versterken.

3. **Versterk de fundamenten van informatiebeveiliging door een volledig en risico gestuurd ISMS in te richten conform de BIO2, in samenhang met het bredere risicomanagement binnen de organisatie.**
Het college onderschrijft uw aanbeveling om risico gestuurd werken verder te versterken. In het kader van de BIO2-implementatie wordt (in nauw samenspel met de concerncontroller) het bestaande stelsel verder ontwikkeld. Daarbij zetten we in op een nadrukkelijker samenhang tussen beleid, risicoanalyses, maatregelen, planning en verantwoording. Met een Information Security Management System (ISMS) verbeteren we de bestuurbaarheid en de weerbaarheid van onze organisatie op het gebied van informatiebeveiliging.

Hierbij plaatst het college de kanttekening dat er in 2026 en in een deel van 2027 twee afzonderlijke P&C cycli ambtelijk ondersteund moeten worden. Hierdoor zal het zwaartepunt voor de verdere ontwikkeling van breed risicomanagement in 2027 en verder liggen. Ook tijdens de integratie- en fusiewerkzaamheden spannen we ons uiteraard in om de risico's voor de gehele omgeving (Wijdemeren en Hilversum) te reduceren. In security termen: elke integratie verkleint het aanvalsoppervlak.

4. **Intensiveer activiteiten om kennis van en bewustzijn over informatiebeveiliging en -risico's onder medewerkers te bevorderen.**
De phishing test onder medewerkers liet helaas zien dat er nog wat te winnen is in de alertheid van de organisatie met betrekking tot zulke gebeurtenissen. Er ligt een belangrijke rol voor de hele organisatie en het management om toe te zien op training van medewerkers in het gebruik van beveiligingsprocedures en deelname aan verplichte relevante trainingen. Daarnaast wijzen we onze medewerkers op hun eigen verantwoordelijkheid om hier serieus mee om te gaan. We maken daarbij gebruik van e-learning modules via de Hilversum Academie en verder gebruiken we de actualiteiten om berichten te plaatsen op Hilvert (het intranet van de gemeente Hilversum) om zo bewustzijn te vergroten.
Het Privacy en Informatieveiligheid Team (PIT) voorziet de organisatie van advies en ondersteuning op het gebied van bewustwording over informatiebeveiliging, privacy en veilig gedrag in gebouwen van de gemeente. Als onderdeel van de verdere bewustwording en verdere professionalisering onderzoekt de organisatie hoe phishing simulaties, incidentscenario's en crisisoefeningen hieraan een bijdrage gaan leveren. Het uitgangspunt is dat de frequentie van de inzet van deze middelen verhoogd wordt, waarbij het maximale leereffect van de organisatie een belangrijk doel is.

5. **Versterk de fysieke beveiliging van vertrouwelijke gegevens van de gemeente.**
De bevindingen uit de inlooptest en penetratietest worden actief opgevolgd. Daarbij wordt een onderscheid gemaakt in de aanpak tussen wat we op korte termijn (moeten) doen en welke verbeterpunten logischer kunnen landen in de strategische huisvestingsvisie. Er is daarnaast een onderscheid te maken tussen snelle maatregelen die we kunnen nemen en acties, bijvoorbeeld om bewustwording te vergroten, die een langere adem zullen vragen.

   U schrijft dat de bevindingen uit de inloop- en penetratietest '*vooralsnog*' enkel met de organisatie gedeeld worden. We dringen er bij u op aan om deze bevindingen ook in de toekomst niet buiten de gemeentelijke organisatie te delen om de veiligheid en beveiliging van onze bestuurders, medewerkers, bezoekers, gebouwen en de gegevens die zich daarin bevinden te kunnen blijven borgen.

6. **Vergroot de interne digitale weerbaarheid van de gemeente.**
Bevindingen uit de technische bijlage met hoge prioriteit zijn begin 2026 opgevolgd en voor zover mogelijk direct opgelost. De punten die nog open staan kennen een afhankelijkheid met andere interne ontwikkelingen, te denken valt aan beperkingen in de huidige netwerkapparatuur waarvan de vervanging op het projectportfolio van ICT staat. Een ander voorbeeld is de implementatie van Identity Access Management (IAM). Dit project is gestart, maar vraagt meer tijd en de resultaten worden in 2027 verwacht.

   Het college constateert verder, op basis van de onderzoeksresultaten, dat onze ICT-systemen zo zijn ingericht dat calamiteiten die vanuit de buitenwereld op ons netwerk en systemen worden gestuurd nu kunnen worden opgevangen. Echter, nieuwe cyberdreigingen, de toenemende digitalisering en maatschappelijke afhankelijkheid hiervan vragen om continue doorontwikkeling van de robuuste IT-omgeving om onze weerbaarheid te behouden en versterken. Het vergroten en versterken van de digitale weerbaarheid is ook onderdeel van de Nederlandse Digitaliseringsstrategie waar ook Hilversum zich toe te verhouden heeft.

   Het zal nodig blijven om te investeren in het ICT-fundament van de organisatie, zowel in techniek als in personeel. In de Voorjaarsnota 2026 is daarom een structurele investering in ICT-security van 150.000 euro toegekend. Daarmee kunnen we monitoring en incidentopvolging verbeteren die direct en 24/7 actie kunnen ondernemen bij beveiligingsincidenten. Met die verbetering maken we verdere stappen om te voldoen aan de eisen uit de Cbw op het gebied van logging, monitoring, incidentbeheersing en onze zorgplicht.

7. **Toets periodiek of het toezicht van de derde lijn voldoende aansluit bij de gewenste diepgang en effectiviteit, en voer waar nodig gerichte verbeteringen door.**
Het college onderschrijft het belang van een heldere invulling van rollen, verantwoordelijkheden en (toezicht)functies binnen de keten van informatiebeveiliging. De verschillende rollen, taken en verantwoordelijkheden zijn beschreven voor alle bestuurslagen in hoofdstuk 3 – Governance van het vastgestelde Strategisch gegevensbescherming en informatiebeveiligingsbeleid 2025-2029. Het beleid biedt voldoende aanknopingspunten om de gevraagde diepgang en effectiviteit van de derde lijn vorm te geven zoals de Cyberbeveiligingswet (Cbw) dat van ons vraagt.

8. **Verbeter de periodieke informatievoorziening.**
De rekenkamer beveelt aan om de raad te informeren over actuele risico's, relevante regels, incidenten en ontwikkelingen op het gebied van informatieveiligheid. Zodat de raad structureel en consistent kan

sturen en controleren op risico's, voortgang en naleving van de wettelijke zorgplicht. Het college van B en W begrijpt de informatiebehoefte van de raad bij het thema informatiebeveiliging goed. Het college ziet twee logische invalshoeken waarlangs het gesprek over informatiebeveiliging gevoerd kan worden.

- De jaarlijkse ENSIA-rapportage van de gemeentelijke organisatie aan de raad is een bestaand middel om u te informeren over de stand van zaken van de datakwaliteit binnen de basisstelsels en de beschermingsmaatregelen rondom DigiD en Suwinet-Inkijk. Voor een beeld van de stand van zaken rondom informatiebeveiliging biedt de CISO standaard een rapportage als apart onderdeel in de geheime bijlagen.
- Het college biedt aan om het actuele dreigingsbeeld zoals dat door de Informatiebeveiligingsdienst van de VNG gemaakt wordt met de raad te delen zodra dat beschikbaar komt. Waar opportuun wordt dit gebundeld met de ENSIA-rapportage, zodat de informatie integraal gepresenteerd wordt aan de raad.

Reflectie op de aanbevelingen van de Rekenkamer aan de raad

Het college van B en W onderschrijft de constatering van de Rekenkamer van een actieve rol van de raad bij het thema informatiebeveiliging. De investering die we de komende jaren moeten doen om informatiebeveiliging (en daarmee ook gegevensbescherming) te laten voldoen aan de eisen uit de Cyberbeveiligingswet zullen keuzes van de raad vragen. Een belangrijke manier waarop de raad invulling kan geven aan haar rol binnen de Cbw is door er de komende jaren voor te zorgen dat er voldoende middelen beschikbaar zijn voor het realiseren van maatregelen binnen de organisatie die bijdragen aan informatiebeveiliging. Dan gaat het ook over voldoende budget voor ICT en functioneel beheer om medewerkers aan te trekken die technisch onze systemen en applicaties veilig kunnen houden. Het is nodig om kennis en kunde in huis te hebben om beveiliging technisch optimaal voor elkaar te hebben. En het gaat ook over versterking van de eerste en tweede lijn op het gebied van informatiebeveiliging.

Investeringskeuzes die de raad feitelijk alleen kan maken door een breed begrip van de materie. Het college onderschrijft dan ook de constatering dat er voor de ambtenaren, raads- en commissieleden en burgemeester en wethouders verschillende rollen, rechten en plichten gelden. Voor een goede invulling van die rol is opleiding en training op alle niveaus noodzakelijk. Voor het college zelf geldt dat zij de schakel vormt tussen de ambtelijke organisatie en de raad wanneer het gaat om informatievoorziening aan de raad. Daarbij is het van belang te onderkennen dat kennis over informatiebeveiliging op alle functies een vereiste is vanuit de Cbw. Voor raads- en commissieleden stelt het college voor om bij aanvang van de komende raadsperiode stil te staan bij de eigen rol, behoeften (rechten) en plichten als het gaat om informatiebeveiliging, waarbij de manier van werken van de raad ook onder de aandacht kan en moet komen.

Tezamen met themasessies, het (vertrouwelijk) bespreken van relevante rapportages en mogelijke informatiebeveiligingsrisico's en e te nemen maatregelen vormt dit waardevolle instrumenten voor toezicht en controle.

Tot slot

Het is de wens van het College van B en W om het onderwerp met zoveel mogelijk transparantie met de raad te bespreken waarbij we in ogenschouw moeten houden dat er bepaalde zaken niet in openbaarheid gedeeld kunnen worden om malafide personen en organisaties niet wijzer te maken.

Wij danken de Rekenkamer voor het waardevolle onderzoek en de aanbevelingen. Met deze reactie en de vervolgacties willen wij de informatiebeveiliging in Hilversum naar een hoger niveau brengen en het vertrouwen van de raad en de inwoners in onze digitale dienstverlening versterken.

Hilversum, september 2026

Hoogachtend,

Burgemeester en wethouders van Hilversum,

de gemeentesecretaris,	de burgemeester,
mr. C.P. Torres Barrera	dr. ir. G.M. van den Top

Evidence sheet iBabs digital signature

Top, van den, Gerhard
g.vandentop@hilversum.nl
09-24-2026 14:40
a33b522894ec8b120ce952025ee62f981994511b654c9c108d7b8d41571ad9dc



Torres Barrera, Pilar
p.torresbarrera@hilversum.nl
09-27-2026 11:13
f641a54be3cf0198b4412fc21d69b1e0570ffbe5a1a8ded613abd559f1f1c2a6

