

Kenmerk	: 3578282	Memo
Aan	: Gemeenteraad Meppel	
Van	: College van B&W	
Datum	: 19 Mei 2026	
Onderwerp	: Informatiebeveiliging & Privacy	
Bijlage	: IB&P Beleid 2026-2029	
Afschriften voor	: Griffie	

Algemeen

Het College van B&W heeft het geactualiseerde informatiebeveiligings- en privacybeleid vastgesteld. In het kader van transparantie en de kader stellende en controlerende rol van de gemeenteraad wordt dit beleid ter kennisname met u gedeeld.

Aanleiding

De actualisatie van het beleid is noodzakelijk door nieuwe en aangescherpte wet- en regelgeving, zoals de Cyberbeveiligingswet (op basis van de Europese NIS2-richtlijn) en de Baseline Informatiebeveiliging Overheid (BIO2).

Deze ontwikkeling betekent dat informatiebeveiliging niet langer een interne richtlijn is, maar een wettelijke verplichting waarbij het bestuur aantoonbaar verantwoordelijk is voor digitale veiligheid en risicobeheersing. Tegelijkertijd neemt de afhankelijkheid van digitale systemen toe en worden cyberdreigingen complexer, met directe impact op de continuïteit van gemeentelijke dienstverlening en het vertrouwen van inwoners.

Dit geactualiseerde beleid sluit aan bij een recent onderzoek van de Rekenkamer naar informatiebeveiliging en privacy, dat inzicht geeft in de wijze waarop deze onderwerpen binnen de gemeente Meppel zijn georganiseerd. Het rekenkameronderzoeksrapport is op dit moment nog niet gepubliceerd, maar zal binnenkort met de raad worden gedeeld. Eén van de aanbevelingen uit het onderzoek is dat het periodiek bijstellen van beleid, risicoanalyses en beheersmaatregelen bijdraagt aan verdere versterking van informatiebeveiliging en privacy. De in dit geactualiseerde beleid opgenomen aanpassingen zijn hiervan een concreet voorbeeld.

Relatie met P&C-cyclus en sturing

Met het nieuwe beleid wordt informatiebeveiliging nadrukkelijk onderdeel van de reguliere planning- en control cyclus. Dit betekent dat beleid, uitvoering en verantwoording niet los staan, maar structureel worden verbonden via een continue verbetercyclus (plannen, uitvoeren, controleren en bijstellen). Hiermee wordt geborgd dat:

- Periodiek wordt gerapporteerd over risico's en voortgang
- Bijsturing plaatsvindt op basis van audits, ENSIA en actuele dreigingen
- Informatiebeveiliging onderdeel is van reguliere bestuurlijke afwegingen

Voor de raad betekent dit dat informatiebeveiliging transparanter en beter toetsbaar wordt binnen bestaande verantwoordingsmomenten.

Wat is er inhoudelijk veranderd

Het nieuwe beleid bouwt voort op de bestaande basis, maar brengt een aantal wezenlijke veranderingen aan:

- Van richtlijn naar aantoonbare naleving
Waar eerdere kaders richtinggevend waren, ligt de nadruk nu op aantoonbaar “in control” zijn en het kunnen verantwoorden van gemaakte keuzes.
- Van losse maatregelen naar samenhang
Informatiebeveiliging is ingericht als een samenhangend geheel van beleid, uitvoering, risicoanalyse en verantwoording, in plaats van afzonderlijke maatregelen.
- Risico gestuurd werken centraal
Niet alle maatregelen worden generiek toegepast, maar afgestemd op de risico's voor dienstverlening, gegevens en inwoners. Dit maakt de aanpak doelgerichter en beter uitlegbaar.
- Versterkte bestuurlijke verantwoordelijkheid
Het beleid maakt expliciet dat het college en de directie sturen op risico's en prioriteiten, en dat deze afwegingen onderdeel zijn van reguliere besluitvorming.
- Organisatie brede verantwoordelijkheid
Informatiebeveiliging is niet alleen een technische aangelegenheid, maar een verantwoordelijkheid van de gehele organisatie, inclusief management en medewerkers.
- Meer aandacht voor continuïteit en weerbaarheid
De focus ligt niet alleen op het voorkomen van incidenten, maar ook op het kunnen blijven functioneren bij verstoringen en het beperken van schade.
- Strakkere sturing op leveranciers en ketens
Door afhankelijkheid van externe partijen zijn de eisen aan beveiliging, toezicht en samenwerking aangescherpt.

Ten opzichte van het beleid uit 2023 is het nieuwe beleid dus:

- Beter afgestemd op wettelijke verplichtingen (BIO2 en Cyberbeveiligingswet)
- Duidelijker verankerd in bestuurlijke sturing en verantwoordelijkheid
- Sterker verbonden met de P&C-cyclus en reguliere verantwoording
- Meer gericht op risico's en doelmatige inzet van maatregelen
- Beter in staat om aantoonbaar “in control” te zijn

Daarmee wordt de ontwikkeling gemaakt van een situatie waarin de basis op orde is, naar een organisatie waarin informatiebeveiliging structureel, bestuurbaar en aantoonbaar is geborgd.

Afsluitend

Met dit beleid zijn de kaders voor informatiebeveiliging en privacy geactualiseerd en sluit de gemeente aan bij de geldende wettelijke eisen. Het beleid versterkt de mogelijkheden voor de raad om haar kade stellende en controlerende rol uit te oefenen, doordat risico's, maatregelen en voortgang structureel inzichtelijk gemaakt kunnen worden via de bestaande bestuurlijke verantwoordingscyclus.