



Onderwerp Strategisch Informatiebeveiligings- en
Privacybeleid Nieuwegein 2026–2030

Datum juli 2026

Raadsvoorstel

2026-230

Afdeling Support
E-mailadres opsteller s.lee@nieuwgein.nl
Portefeuillehouder Marijke van Beukering-
Huijbregts

Onderwerp

Strategisch Informatiebeveiligings- en Privacybeleid Nieuwegein 2026–2030

Gevraagd besluit

1. Het Strategisch Informatiebeveiligings- en Privacybeleid Nieuwegein 2026–2030 vast te stellen, met daarin de volgende aandachtspunten:
 - a. Het in samenhang aansturen van informatiebeveiliging en privacy vanuit één strategisch beleidskader.
 - b. Het baseren van het informatiebeveiligingsbeleid op het landelijke normenkader Baseline Informatiebeveiliging Overheid, versie 2 (BIO2), waarbij risicogestuurd werken centraal staat.
 - c. Het hanteren van een volwassenheidsmodel voor informatiebeveiliging om de ontwikkeling en het gewenste volwassenheidsniveau van de organisatie te bepalen.
 - d. De inrichting van rollen, taken en verantwoordelijkheden voor informatiebeveiliging en privacy binnen de organisatie, waarbij het management verantwoordelijk is voor de borging binnen de eigen processen.
2. Het Strategisch Informatiebeveiligingsbeleid 2021–2025 met ingang van de inwerkingtreding van het Strategisch Informatiebeveiligings- en Privacybeleid Nieuwegein 2026–2030 te vervangen.

Inleiding

De gemeente opereert in een samenleving waarin digitalisering een steeds grotere rol speelt in dienstverlening, samenwerking en besluitvorming. Tegelijkertijd nemen digitale dreigingen en risico's rondom gegevensverwerking toe. Een zorgvuldige en veilige omgang met informatie en persoonsgegevens is daarom een randvoorwaarde voor betrouwbare gemeentelijke dienstverlening.

Het huidige strategisch informatiebeveiligingsbeleid loopt af en sluit niet meer volledig aan bij recente ontwikkelingen in wet- en regelgeving, landelijke normenkaders en het actuele dreigingsbeeld. Daarbij gaat het onder meer om de verdere ontwikkeling van BIO2, de ontwikkelingen rond de Cyberbeveiligingswet als nationale uitwerking van de NIS2-richtlijn, toenemende digitale ketenafhankelijkheden en de wens om

informatiebeveiliging en privacy bestuurlijk meer in samenhang te beschouwen. Het vigerende beleid uit 2021 is destijds door het college vastgesteld. De hiervoor benoemde ontwikkelingen maken dat het inmiddels een strategisch beleidskader is dat beter door de Gemeenteraad kan worden vastgesteld. Met het Strategisch Informatiebeveiligings- en Privacybeleid 2026–2030 wordt een geactualiseerd bestuurlijk kader voorgesteld voor de bescherming van informatie en persoonsgegevens binnen de gemeente.

Het beleid sluit aan bij landelijke normenkaders en relevante wetgeving, waaronder de Baseline Informatiebeveiliging Overheid, versie 2 (BIO2), de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de ontwikkelingen rond de Cyberbeveiligingswet (NIS2). Daarnaast geeft het beleid richting aan risicogestuurd werken en de bestuurlijke sturing op informatiebeveiliging en privacy binnen de organisatie.

Wat er aan vooraf ging

Op 15 januari 2026 bent u als raad tijdens een informatieavond geïnformeerd over het rekenkamerrapport "Rapport onderzoek Informatiebeveiliging". In dit rapport zijn meerdere aanbevelingen gedaan. Eén van deze aanbevelingen was het herzien van het strategisch informatiebeveiligings- en privacybeleid. Die herziening was al in voorbereiding en met dit voorgestelde besluit geven wij volledig invulling aan die aanbeveling.

Daarnaast is aanbevolen om een bewustwordingsplan voor informatieveiligheid en privacy op te stellen en vast te stellen. Ook dat herziene bewustwordingsplan was al in voorbereiding. Het bewustwordingsplan is vastgesteld op 1 juni 2026 door het directieteam van de organisatie. Hiermee geven wij volledig invulling aan deze aanbeveling en kan een toezegging die op die avond genoteerd is (2025-379) worden afgehandeld.

Daarnaast wordt binnen gemeentelijk verband, onder meer via de VNG, samengewerkt aan de versterking van informatieveiligheid en privacy. Deze landelijke ontwikkelingen, gezamenlijke inzichten en gemeentelijke samenwerkingsverbanden zijn betrokken bij de actualisatie van het strategisch kader.

Gewenst effect

Door vaststelling van het Strategisch Informatiebeveiligings- en Privacybeleid 2026–2030 beschikt de gemeente over een actueel bestuurlijk kader voor de bescherming van informatie en persoonsgegevens.

Argumenten

1.a.1 Informatiebeveiliging en privacy vragen om samenhangende bestuurlijke sturing.

Informatiebeveiliging en privacy raken de gehele organisatie en zijn onlosmakelijk verbonden met betrouwbare en rechtmatige gemeentelijke

dienstverlening. Door beide onderwerpen vanuit één strategisch kader aan te sturen, ontstaat samenhang in bestuurlijke keuzes, risicobeheersing, gegevensbescherming en verantwoording.

Het beleid bevat daarbij meerdere uitgangspunten die richting geven aan bestuur en organisatie. Het gaat om een mensgerichte en passende benadering, betrouwbare dienstverlening, risicogestuurd werken, transparant en verantwoord handelen en security en privacy by design.

1.b.1 Het beleid sluit aan bij actuele wet- en regelgeving en landelijke normenkaders.

Gemeenten moeten voldoen aan verschillende wettelijke verplichtingen op het gebied van informatiebeveiliging en gegevensbescherming, waaronder de Algemene verordening gegevensbescherming en de Wet politiegegevens. Daarnaast wordt de Europese NIS2-richtlijn in Nederland geïmplementeerd via de Cyberbeveiligingswet. Het beleid sluit hierop aan en hanteert de Baseline Informatiebeveiliging Overheid, versie 2 (BIO2), als leidend normenkader.

1.b.2 Digitale weerbaarheid vraagt om risicogestuurd werken.

De afhankelijkheid van digitale systemen, gegevens, leveranciers en ketenpartners neemt toe. Verstoring van systemen of verlies van gegevens kan gevolgen hebben voor dienstverlening, veiligheid en het vertrouwen van inwoners. Het beleid ondersteunt een risicogestuurde aanpak, waarbij bestuurlijke keuzes bewust en uitlegbaar worden gemaakt in samenhang met maatschappelijke belangen en publieke waarden.

1.c.1 Het volwassenheidsmodel maakt ontwikkeling en sturing inzichtelijk.

Met het volwassenheidsmodel kan de gemeente de ontwikkeling van informatiebeveiliging volgen en prioriteiten bepalen. Dit ondersteunt bestuurlijke sturing, verbetering en verantwoording. De gemeente hanteert daarbij als bestuurlijke ambitie een volwassenheidsniveau dat minimaal overeenkomt met niveau 3 van het gehanteerde model.

1.d.1 Het beleid verduidelijkt rollen, verantwoordelijkheden en bestuurlijke sturing.

Informatiebeveiliging en privacy raken bestuur, directie, management, medewerkers en ondersteunende rollen. Het beleid beschrijft hoe verantwoordelijkheden zijn belegd en hoe informatiebeveiliging en privacy worden aangestuurd, geborgd en verantwoord binnen de gemeentelijke organisatie.

2.1 Het eerdere strategische informatiebeveiligingsbeleid wordt vervangen door een geactualiseerd beleidskader.

Met de vaststelling van het Strategisch Informatiebeveiligings- en Privacybeleid Nieuwegein 2026–2030 wordt het Strategisch Informatiebeveiligingsbeleid 2021–2025 vanaf de inwerkingtreding van het nieuwe beleid vervangen. Daarmee beschikt de gemeente over één actueel en samenhangend strategisch kader dat aansluit bij de huidige bestuurlijke, maatschappelijke en wettelijke context.

Kanttekeningen

1.1. De uitvoering van het beleid vraagt blijvende inzet van de organisatie.

Informatiebeveiliging en privacy raken de gehele organisatie. Het realiseren van de ambities uit het beleid vraagt inzet van het college, de directie, het management en medewerkers, met structurele aandacht voor bewustwording, risicomanagement en naleving van afspraken. De raad heeft hierbij een kaderstellende en controlerende rol. De verdere uitwerking vindt plaats via tactische plannen, de reguliere bedrijfsvoering en de planning en controlcyclus.

Financiële aspecten

Het vaststellen van het Strategisch Informatiebeveiligings- en Privacybeleid 2026–2030 heeft op zichzelf geen directe financiële consequenties. Met dit besluit wordt het bestuurlijke kader vastgesteld.

De uitvoering van het beleid vindt plaats via onderliggende tactische plannen en binnen de reguliere bedrijfsvoering. Daarbij kan de komende jaren aanvullende inzet nodig zijn voor onder meer de voorbereiding op nieuwe wetgeving, de verdere implementatie van landelijke normenkaders en het versterken van bewustwording binnen de organisatie.

Eventuele aanvullende middelen worden uitgewerkt in onderliggende uitvoeringsplannen en, indien nodig, via de reguliere planning- en controlcyclus aan het de gemeenteraad voorgelegd. Hiermee wordt tevens invulling gegeven aan de andere toezegging bij de bespreking van het rekenkamerrapport T 2026-379 waarbij de integraliteit van de afweging ziet op de toedeling van financiële middelen en niet het totale informatieveiligheidsbeleid. Dat laatste is niet beoogd toe te zeggen en ook niet uitvoerbaar.

Communicatie aspecten

Het Strategisch Informatiebeveiligings- en Privacybeleid 2026–2030 wordt na vaststelling binnen de organisatie onder de aandacht gebracht via de reguliere managementlijn. Afdelingshoofden en teamleiders worden geïnformeerd over de uitgangspunten, rollen en verantwoordelijkheden, zodat zij deze kunnen vertalen naar hun eigen processen en werkzaamheden.

Voor medewerkers betekent dit dat zij bij hun dagelijkse werkzaamheden zorgvuldig omgaan met informatie en persoonsgegevens, vastgestelde

werkwijzen volgen, incidenten en datalekken tijdig melden en informatiebeveiliging en privacy tijdig betrekken bij nieuwe processen, systemen, samenwerkingen en veranderingen.

Het beleid wordt gepubliceerd volgens de geldende publicatievereisten, waaronder, indien van toepassing, publicatie via overheid.nl.

Uitvoering

De uitvoering van dit beleid ligt bij de directie en de lijnorganisatie. De directie zorgt voor de verdere uitwerking in tactische kaders en bewaakt de samenhang.

Het beleid wordt in de hele organisatie toegepast. Informatiebeveiliging en privacy hebben een vaste plek in processen, projecten en ontwikkelingen. Proceseigenaren en afdelingsmanagers zijn hiervoor verantwoordelijk binnen hun eigen domein. Informatiebeveiliging en privacy maken een vast onderdeel uit van de sturing en verantwoording binnen de organisatie.

De voortgang en naleving worden periodiek gemonitord en gerapporteerd binnen de planning- en controlcyclus. Hierbij wordt inzicht gegeven in risico's en afwijkingen. Als er sprake is van afwijkingen of restrisico's, stuurt de directie bij. Waar nodig worden deze aan het college voorgelegd.

Waar relevant sluit de gemeente in de uitvoering aan bij landelijke gemeentelijke ontwikkelingen en samenwerking binnen VNG-verband, waaronder Common Ground. Daarbij gelden informatiebeveiliging en privacy als randvoorwaarden voor zorgvuldige, veilige en betrouwbare digitale dienstverlening.

Bijlagen

1. Strategisch Informatiebeveiligings- en Privacybeleid Nieuwegein 2026–2030
2. Beleidsstructuur informatiebeveiliging en privacy
3. Volwassenheidsmodel informatiebeveiliging
4. Bestuurlijke verantwoordelijkheden informatiebeveiliging en privacy

burgemeester en wethouders,

Ellie Liebregts
secretaris

Marijke van Beukering-Huijbregts
burgemeester