# VOORSTEL AAN B&W: Collegevergadering B&W d.d. 26 mei 2026

**NR.: BW-26-06061**

| **Onderwerp:** Strategisch informatiebeveiligings- & privacybeleid 2026-2030 | Openbaar volgens WOO<br><br>**Ja** |
|---|---|

## Voorstel:

1. Het Strategisch Informatiebeveiligings- en privacybeleid gemeente Nederweert 2026 tot 2030 vast te stellen.
2. Het Strategisch Informatiebeveiligingsbeleid 2025, het Informatiebeveiligingsbeleid Governance 2025 en het Privacybeleid 2025–2027 in te trekken.
3. De tactische en operationele uitwerking van dit beleid, conform de AVG, het IBD-format en de BIO (en opvolgende BIO2.0), NIS2 en de Cyberbeveiligingswet, uit te voeren binnen de bestaande budgetten voor informatiebeveiliging en privacy, en deze waar nodig via de P&C-cyclus en separate besluiten te intensiveren.
4. De CISO, Privacy Officer en Functionaris Gegevensbescherming te mandateren om, binnen dit strategisch kader, de governance- en taakbeschrijvingen op het gebied van informatiebeveiliging en privacy waar nodig te actualiseren en aan te passen.

| | | | |
|---|---|---|---|
| Portefeuillehouder(s) | : Burgemeester Op de Laak | Datum | : 26 mei 2026 |
| | | Kopie aan | : |
| Team | : Informatievoorziening | Overlegd met | : F. Robben |
| Auteur | : D Jacobs | | |

## Vervolgbehandeling:

| | | | |
|---|---|---|---|
| ☐ Raadsvergadering | : Nee | d.d. | : |

## Externe boodschap:

De gemeente Nederweert heeft het Strategisch Informatiebeveiligings- en privacybeleid 2026-2030 opgesteld. Dit beleid geeft richting aan hoe wij omgaan met persoonsgegevens van inwoners, ondernemers en partners, en hoe we de digitale veiligheid van onze organisatie versterken. Ook maken we duidelijk wie waarvoor verantwoordelijk is. Het beleid sluit aan op de AVG en op de geldende regels voor privacy en digitale veiligheid. Daarmee leggen we de basis voor een betrouwbare, veilige en toekomstbestendige dienstverlening. Zo beperken we digitale risico's en houden we het vertrouwen van inwoners en ondernemers hoog.

**Rapportage bij B&W-voorstel BW-26-06061** Collegevergadering B&W d.d. 26 mei 2026

**Voorstel**
1. Het Strategisch Informatiebeveiligings- en privacybeleid gemeente Nederweert 2026 tot 2030 vast te stellen.
2. Het Strategisch Informatiebeveiligingsbeleid 2025, het Informatiebeveiligingsbeleid Governance 2025 en het Privacybeleid 2025–2027 in te trekken.
3. De tactische en operationele uitwerking van dit beleid, conform de AVG, het IBD-format en de BIO (en opvolgende BIO2.0), NIS2 en de Cyberbeveiligingswet, uit te voeren binnen de bestaande budgetten voor informatiebeveiliging en privacy, en deze waar nodig via de P&C-cyclus en separate besluiten te intensiveren.
4. De CISO, Privacy Officer en Functionaris Gegevensbescherming te mandateren om, binnen dit strategisch kader, de governance- en taakbeschrijvingen op het gebied van informatiebeveiliging en privacy waar nodig te actualiseren en aan te passen.

**Inleiding**
De gemeente Nederweert werkt steeds meer digitaal en verwerkt daarbij veel (persoons)gegevens van inwoners, ondernemers en partners. Tegelijkertijd nemen de eisen vanuit wet- en regelgeving en de dreiging van cyberincidenten toe. De Algemene Verordening Gegevensbescherming (AVG), Baseline Informatiebeveiliging Overheid (BIO), de NIS2-richtlijn en de Cyberbeveiligingswet vragen om een actueel, integraal en aantoonbaar beleid voor informatiebeveiliging en privacy. Het bestaande strategisch informatiebeveiligingsbeleid 2025, het governance beleid en het privacybeleid 2025–2027 sluiten hier niet meer voldoende op aan. Daarom is een nieuw Strategisch Informatiebeveiligings- en privacybeleid 2026–2030 opgesteld, waarin informatiebeveiliging, privacy en governance in één document zijn samengebracht. De kernfuncties CISO, PO en FG spelen hierbij een centrale rol en krijgen mandaat om de bijbehorende governance- en taakbeschrijvingen actueel te houden.

**Beoogd effect**
In 2030 beschikt de gemeente Nederweert over een aantoonbaar veilige, weerbare en privacy bewuste informatiehuishouding, die voldoet aan de BIO (en BIO2.0), AVG, NIS2 en de Cyberbeveiligingswet en het vertrouwen van inwoners en ondernemers versterkt.

**Argumenten**
*1.1 Het nieuwe beleid borgt naleving van actuele wet- en regelgeving voor informatiebeveiliging en privacy.*
Het Strategisch Informatiebeveiligings- en privacybeleid is expliciet gebaseerd op de AVG, BIO en de doorontwikkeling naar BIO2.0, de NIS2-richtlijn en de Cyberbeveiligingswet. Hierdoor sluit het beleid aan op de Europese en landelijke kaders voor informatiebeveiliging en privacy binnen de overheid. Door informatiebeveiliging en privacy in één strategisch document op te nemen, wordt de samenhang tussen de AVG, de BIO en andere relevante normen duidelijker. Dit maakt het eenvoudiger om aantoonbaar te voldoen aan de eisen van toezichthouders en auditors. Ook wordt hiermee de basis gelegd voor een structurele cyclus van planning, uitvoering, monitoring en verantwoording. Dit helpt het college om zijn verantwoordelijkheid voor rechtmatige en zorgvuldige gegevensverwerking goed in te vullen.

*1.2 Informatiebeveiliging en privacy zijn samengebracht in één integraal beleidskader, wat zorgt voor duidelijkheid en samenhang.*
In het nieuwe beleid zijn het eerdere informatiebeveiligingsbeleid en privacybeleid geïntegreerd tot één strategische lijn. Dit voorkomt dat er tegenstrijdige of overlappende beleidsdocumenten bestaan. Medewerkers en management krijgen zo één helder kader waarbinnen zij hun keuzes kunnen maken. Ook wordt de governance voor informatiebeveiliging en privacy in dit document beschreven, waardoor rollen, taken en verantwoordelijkheden beter op elkaar aansluiten. Dit ondersteunt een integrale benadering van risico's, maatregelen en controles. De samenvoeging draagt bij aan een efficiëntere beleidsvoering en vermindert de kans op hiaten in de bescherming van informatie en persoonsgegevens.

*1.3 De governance voor informatiebeveiliging en privacy is in het beleid verankerd, wat de bestuurlijke en ambtelijke sturing versterkt.*

In het beleid zijn de belangrijkste functies en rollen op het gebied van informatiebeveiliging en privacy benoemd, zoals het college van B&W, de gemeentesecretaris, strategisch management, CISO, FG, Privacy Officer, proceseigenaren en lijnmanagement. Hiermee wordt duidelijk wie waarvoor verantwoordelijk is en wie welke besluiten neemt. Dit maakt het mogelijk om bestuurlijke prioriteiten gericht te vertalen naar concrete acties in de organisatie. Aanvullende rollen kunnen per proces of project worden vastgelegd in aparte documenten, zodat er ruimte blijft voor maatwerk. Door in het besluit de CISO, Privacy Officer en FG te mandateren om governance- en taakbeschrijvingen te actualiseren, kan de organisatie deze rollen snel laten meebewegen met nieuwe eisen en inzichten. Zo blijft de governance actueel, zonder dat voor elke wijziging een nieuw bestuurlijk besluit nodig is.

*1.4 Het beleid sluit aan op de producten en werkwijze van de Informatiebeveiligingsdienst (IBD), waardoor de gemeente gebruikmaakt van landelijke expertise.*
Het strategisch beleid is opgesteld volgens het IBD-format, met een duidelijke scheiding tussen strategisch, tactisch en operationeel niveau. Dit betekent dat tactische en operationele producten, zoals onderwerp specifiek beleid, risicoanalyses, maatregelenoverzichten, incidentprocedures en bewustwordingsprogramma's, logisch onder dit beleid hangen. Door deze aansluiting kan de gemeente efficiënter gebruikmaken van de hulpmiddelen, handreikingen en best practices van de IBD. Dit voorkomt dat de gemeente zelf alles hoeft te ontwikkelen en bevordert uniformiteit met andere gemeenten. Bovendien maakt dit het makkelijker om mee te bewegen met landelijke ontwikkelingen en updates van de AVG, BIO en BIO2.0. Dit draagt bij aan een toekomstbestendige inrichting van informatiebeveiliging en privacy.

*1.5 Het beleid versterkt de digitale weerbaarheid van de gemeente tegen cyberdreigingen.*
Met de komst van NIS2 en de Cyberbeveiligingswet wordt van overheden verwacht dat zij hun digitale weerbaarheid aantoonbaar op orde hebben. In het strategisch beleid is expliciet aandacht voor risicomanagement, continuïteit van dienstverlening (business continuity management), incident- en crisismanagement en auditing. Hiermee wordt de basis gelegd voor structurele verbeteringen in detectie, respons en herstel na een incident. Ook wordt ruimte geboden om gericht te investeren in aanvullende expertise en inhuur, bijvoorbeeld voor NIS2-compliance en onafhankelijke audits. Door deze onderwerpen strategisch te verankeren, kan de gemeente gerichter prioriteren en investeren in maatregelen die de grootste risico's verkleinen. Dit verkleint de kans op ernstige verstoringen van de dienstverlening aan inwoners en ondernemers.

*1.6 Het beleid draagt bij aan het vertrouwen van inwoners en ondernemers in de gemeente.*
Inwoners en ondernemers verwachten dat de gemeente zorgvuldig omgaat met hun gegevens en dat digitale dienstverlening veilig is. Door informatiebeveiliging en privacy expliciet en integraal te regelen, laat de gemeente zien dat zij deze verantwoordelijkheid serieus neemt. Het beleid beschrijft hoe de gemeente omgaat met vertrouwelijkheid, integriteit en beschikbaarheid van informatie, maar ook met transparantie, rechten van betrokkenen en privacy by design. Dit sluit aan bij de ambities van het coalitieakkoord om een betrouwbare en toegankelijke overheid te zijn. Een helder beleidskader maakt het bovendien makkelijker om hierover duidelijk te communiceren, bijvoorbeeld bij datalekken of vragen van inwoners. Zo wordt het vertrouwen in de gemeentelijke organisatie en dienstverlening versterkt.

*1.7 De looptijd 2026–2030 biedt stabiliteit én ruimte om in te spelen op nieuwe ontwikkelingen.*
Door te kiezen voor een strategische horizon van 2026 tot 2030 krijgt de organisatie voldoende tijd om de gewenste veranderingen door te voeren. Tegelijkertijd blijft de periode overzichtelijk en passend bij de verwachte ontwikkelingen in wet- en regelgeving. In het beleid is ruimte opgenomen voor periodieke evaluatie en bijstelling, zodat nieuwe eisen uit bijvoorbeeld BIO2.0 of nadere uitwerking van de Cyberbeveiligingswet kunnen worden verwerkt. Dit voorkomt dat het beleid snel veroudert en steeds volledig herschreven moet worden. De combinatie van een meerjarige horizon en een cyclische aanpak zorgt voor continuïteit én wendbaarheid. Dit sluit aan bij de behoefte van zowel bestuur als organisatie aan voorspelbaarheid en flexibiliteit.

*2.1 Het intrekken van de bestaande beleidsdocumenten voorkomt onduidelijkheid en dubbele kaders.*
Op dit moment bestaan er meerdere beleidsdocumenten: het Informatiebeveiligingsbeleid 2025, het Informatiebeveiligingsbeleid Governance 2025, Privacybeleid 2023 en het Privacybeleid 2025–2027. Deze documenten zijn niet volledig afgestemd op de nieuwste ontwikkelingen en overlappen deels met elkaar. Door deze documenten expliciet in te trekken, is voor iedereen duidelijk dat het Strategisch Informatiebeveiligings- en privacybeleid 2026–2030 leidend is. Dit vermindert de kans dat

medewerkers of auditors zich op verouderde kaders baseren. Ook wordt zo voorkomen dat er tegenstrijdige eisen of definities in omloop blijven. Het intrekken van de oude documenten is daarmee een noodzakelijke stap om de nieuwe lijn helder en eenduidig te maken. Dit draagt bij aan een betere naleving en uitvoerbaarheid van het beleid.

*3.1 De financiële ruimte wordt flexibel ingericht, zodat de gemeente gericht kan investeren waar dat nodig is.*
De exacte kosten van de uitvoering van het strategisch beleid zijn vooraf niet volledig te bepalen, onder andere door de doorontwikkeling van BIO2.0, de implementatie van NIS2 en de Cyberbeveiligingswet. Door in het besluit op te nemen dat uitvoering in principe binnen de bestaande budgetten plaatsvindt, blijft er financiële discipline. Tegelijkertijd wordt expliciet ruimte gelaten om waar nodig via de P&C-cyclus en separate besluiten extra middelen vrij te maken. Dit geldt bijvoorbeeld voor business continuity management, specialistische inhuur voor NIS2-compliance en auditing. Deze aanpak voorkomt dat nu een te grove raming wordt vastgesteld die niet aansluit op de werkelijke behoefte. Tegelijkertijd erkent het dat aanvullende investeringen noodzakelijk kunnen zijn om de wettelijke verplichtingen en de gewenste weerbaarheid te realiseren.

*4.1 De mandatering maakt het mogelijk om taken en rollen snel bij te werken.*
De CISO, Privacy Officer en Functionaris Gegevensbescherming zitten dicht op de praktijk. Zij zien daardoor snel wanneer aanpassing van governance- of taakbeschrijvingen nodig is. Door hen hiervoor mandaat te geven, kan de organisatie sneller inspelen op veranderingen in wet- en regelgeving of in de manier van werken. Dat voorkomt onnodige vertraging en houdt de verantwoordelijkheden helder. Zo blijft het beleid werkbaar en actueel.

**Kanttekeningen**

*1.1 Er is een risico dat de beschikbare middelen en capaciteit onvoldoende zijn om alle ambities uit het beleid tijdig te realiseren.*
De opgave op het gebied van informatiebeveiliging en privacy is groot en groeit door nieuwe wet- en regelgeving. Dit vraagt om structurele aandacht, tijd en specialistische kennis. Het is mogelijk dat de huidige formatie en budgetten niet toereikend zijn om alle maatregelen in het gewenste tempo uit te voeren. Dit risico wordt ondervangen door in het besluit expliciet ruimte te laten voor intensivering via de P&C-cyclus en separate besluiten. Daarnaast wordt in de uitwerking prioriteit gegeven aan de grootste risico's en wettelijke verplichtingen. Door periodiek te rapporteren over voortgang en knelpunten kan het college tijdig besluiten tot bijsturing. Zo blijft het risico beheersbaar en kan gericht worden geïnvesteerd waar dat het meest nodig is.

*1.2 De wet- en regelgeving rondom informatiebeveiliging en privacy is in beweging, waardoor het beleid mogelijk tussentijds moet worden aangepast.*
BIO2.0, NIS2 en de Cyberbeveiligingswet zijn nog in ontwikkeling of worden de komende jaren verder uitgewerkt. Dit kan betekenen dat aanvullende eisen ontstaan die nu nog niet volledig zijn te overzien. In het strategisch beleid is daarom gekozen voor een kader stellende benadering, met ruimte voor periodieke herijking. De tactische en operationele producten worden zo ingericht dat zij relatief eenvoudig kunnen worden aangepast aan nieuwe eisen. Ook wordt aangesloten bij de producten en updates van de IBD, zodat de gemeente niet alles zelf hoeft te ontwikkelen. Daarmee wordt het risico van veroudering beperkt en blijft het beleid wendbaar. Het strategisch besluit nu is nodig om richting te geven, ook al zijn nog niet alle details bekend.

*1.3 De integratie van informatiebeveiliging en privacy in één document kan in de organisatie tijd vragen om te wennen aan de nieuwe structuur.*
Medewerkers zijn gewend aan aparte documenten voor informatiebeveiliging, governance en privacy. De overgang naar één integraal beleidsdocument kan in eerste instantie vragen oproepen. Dit wordt ondervangen door heldere communicatie en toelichting bij de introductie van het nieuwe beleid. In de tactische en operationele uitwerking worden concrete handreikingen, formats en procesbeschrijvingen aangeboden. Ook wordt ingezet op bewustwording en training, zodat medewerkers weten wat er van hen wordt verwacht. Door de voordelen van de integrale aanpak te benadrukken – minder versnippering, meer duidelijkheid wordt de acceptatie vergroot. Zo wordt de tijdelijke verwarring omgezet in een duurzamere en overzichtelijke werkwijze.

*1.4 De nadruk op governance en rollen kan de indruk wekken dat het vooral om structuur gaat en minder om cultuur en gedrag.*
Informatiebeveiliging en privacy staan of vallen niet alleen met rollen en procedures, maar ook met het dagelijks handelen van medewerkers en leidinggevenden. Het risico bestaat dat het beleid als "papieren werkelijkheid" wordt gezien als de aandacht zich vooral richt op formele rollen. Dit wordt tegengegaan door in de uitwerking nadrukkelijk in te zetten op bewustwording, voorbeeldgedrag en integratie in bestaande werkprocessen. Het strategisch beleid benoemt expliciet het belang van een veilige en open meldcultuur rondom incidenten en datalekken. Ook wordt aangesloten bij P&O-instrumenten, zoals introductieprogramma's en periodieke trainingen. Zo wordt governance niet een doel op zich, maar een middel om gewenst gedrag te ondersteunen.

*4.1 Het mandaat vraagt om duidelijke grenzen en goede afstemming.*
Als de CISO, Privacy Officer en Functionaris Gegevensbescherming aanpassingen mogen doen, moet voor iedereen helder zijn wat zij wel en niet mogen wijzigen. Zonder duidelijke grenzen kan onduidelijkheid ontstaan over de rol van het college en de organisatie. Daarom is het belangrijk dat de aanpassingen alleen binnen het vastgestelde strategische kader plaatsvinden. Zij kunnen dus niet zelfstandig afwijken van het beleid of daar nieuwe keuzes in maken. Daarmee blijft de bevoegdheid beperkt tot de uitvoering en actualisatie van bestaande afspraken. Ook moet hierover goed worden afgestemd met betrokken collega's. Zo blijft het mandaat praktisch en bestuurlijk goed beheersbaar.

**Uitvoering**
Na vaststelling van het strategisch beleid wordt een uitvoeringsplan opgesteld op tactisch niveau, waarin de prioriteiten, planning en verantwoordelijkheden per jaar worden uitgewerkt. Dit plan sluit aan op de producten en werkwijze van de IBD en de BIO/BIO2.0, en bevat onder andere een actualisatie van de risicoanalyse, een maatregelenplan, een plan voor business continuity management en een audit- en monitoringskalender. De betrokken functies, zoals CISO, FG, Privacy Officer, gemeentesecretaris, strategisch management en proceseigenaren, werken hierin samen.

**Communicatie en participatie**
Voor de communicatie wordt een interne campagne opgezet gericht op management en medewerkers, met heldere uitleg van het nieuwe beleid, de belangrijkste wijzigingen en de verwachtingen richting de organisatie. Hierbij wordt gebruikgemaakt van intranet, Bij relevante trajecten, zoals de implementatie van NIS2-maatregelen of BCM, worden betrokken teams actief meegenomen in de uitwerking. Externe partners en leveranciers worden waar nodig geïnformeerd over de aangescherpte eisen op het gebied van informatiebeveiliging en privacy, bijvoorbeeld via contracten en verwerkersovereenkomsten. Zo wordt het strategisch beleid vertaald naar concreet handelen in de hele keten.

**Financiële gevolgen**
De exacte kosten voor de uitvoering van het Strategisch Informatiebeveiligings- en privacybeleid 2026 tot 2030 zijn op voorhand niet volledig vast te stellen, mede door de doorontwikkeling van BIO2.0, de implementatie van NIS2 en de Cyberbeveiligingswet. De uitvoering vindt in principe plaats binnen de bestaande budgetten voor informatiebeveiliging, privacy en aanpalende domeinen (zoals ICT en organisatieontwikkeling). Voor specifieke intensiveringen, zoals de verdere inrichting van business continuity management, specialistische inhuur ten behoeve van NIS2-compliance en onafhankelijke auditing, kunnen aanvullende middelen noodzakelijk zijn. Deze worden, indien aan de orde, via de reguliere P&C-cyclus of separate voorstellen aan het college voorgelegd. In de jaarlijkse rapportages over de uitvoering van het beleid wordt ook inzicht gegeven in de besteding van middelen en eventuele aanvullende financiële behoefte.

**Bijlagen**
Bijlage 1: Strategisch informatiebeveiligings- & privacybeleid gemeente Nederweert 2026 tot 2030