

Strategisch
Informatiebeveiligings-
en
Privacybeleid
Nieuwegein



2026 – 2030

Versiebeheer

Versie	Datum	Door	Wijzigingen
1.0	19-05-2026	S. Lee	Definitief

Inhoudsopgave

VERSIEBEHEER.....	2
1. INLEIDING.....	4
1.1 Leeswijzer.....	5
1.2 Reikwijdte van het beleid.....	5
2. WETTELIJKE EN NORMATIEVE KADERS.....	6
3. VISIE EN UITGANGSPUNTEN.....	7
3.1 Visie op informatiebeveiliging en privacy.....	7
3.2 Uitgangspunten.....	8
4. AMBITIE 2026-2030.....	8
5. STRATEGISCHE THEMATISCHE ACCENTEN.....	9
5.1 Risicogestuurd werken.....	10
5.2 Privacy en gegevensbescherming.....	10
5.3 Continuïteitmanagement van digitale dienstverlening.....	10
5.4 Weerbare organisatie en bewust handelen.....	11
5.5 Verantwoording.....	11
6. BESTUURLIJKE STURING, ROLLEN EN VERANTWOORDELIJKHEDEN.....	11
6.1 Gemeenteraad en college.....	11
6.2 Governance en verantwoordingsstructuur.....	12
6.3 Directie en afdelingshoofden.....	12
6.4 Ondersteunende en toezichhoudende rollen.....	13
6.5 Medewerkers.....	13
7. BORGING EN HERZIENING.....	14

1. Inleiding

De gemeente werkt in een samenleving die in toenemende mate digitaliseert. Inwoners, ondernemers en maatschappelijke partners verwachten een overheid die betrouwbaar, toegankelijk en zorgvuldig handelt. Digitale dienstverlening en het gebruik van gegevens zijn onlosmakelijk verbonden met het functioneren van de gemeente.

Tegelijkertijd nemen digitale dreigingen en risico's voor informatie en persoonsgegevens toe. Een zorgvuldige omgang met informatie en persoonsgegevens is daarom een randvoorwaarde voor betrouwbare en rechtmatige gemeentelijke dienstverlening en voor de bescherming van publieke waarden, zoals transparantie, betrouwbaarheid en de bescherming van inwoners.

Informatiebeveiliging en privacy raken alle onderdelen van de organisatie en maken integraal onderdeel uit van digitale ontwikkelingen, datagedreven werken en het gebruik van nieuwe technologieën.

Dit strategisch informatiebeveiligings- en privacybeleid 2026–2030 beschrijft het bestuurlijke kader waarbinnen de gemeente verantwoordelijkheid draagt voor de bescherming van informatie en persoonsgegevens. Het beleid geeft richting aan bestuurlijke keuzes, benoemt uitgangspunten en verduidelijkt de rol van informatiebeveiliging en privacy binnen de gemeentelijke organisatie.

De nadere uitwerking vindt plaats in onderliggende tactische beleidsdocumenten en binnen de planning- en controlcyclus.

Het beleid sluit aan bij de iVisie en het coalitieakkoord, waarin digitalisering wordt ingezet om publieke waarde te creëren. Daarbij staat een zorgvuldige balans tussen digitale mogelijkheden en de bescherming van publieke waarden centraal. Betrouwbare omgang met informatie en persoonsgegevens vormt hiervoor een belangrijke randvoorwaarde.

Het beleid sluit aan bij geldende wet- en regelgeving en relevante landelijke normen voor informatiebeveiliging en gegevensbescherming.

Met dit strategisch beleid legt de gemeenteraad het fundament voor een samenhangende en toekomstbestendige benadering van informatiebeveiliging en privacy binnen de gemeente voor de periode 2026–2030.

1.1 Leeswijzer

Het *Strategisch Informatiebeveiligings- en Privacybeleid 2026–2030* geeft het bestuurlijke kader waarbinnen de gemeente verantwoord omgaat met digitalisering, informatiebeveiliging en privacy. Het document is bedoeld om bestuur en management te ondersteunen bij bewuste, uitlegbare en risicogestuurde keuzes in een samenleving waarin digitale dienstverlening, gegevensverwerking en digitale dreigingen steeds complexer worden.

Het beleid heeft drie hoofddoelen:

1. **Richting geven aan bestuurlijke afwegingen** over digitale risico's, privacy en beveiliging, inclusief het gewenste volwassenheidsniveau voor kritische en niet-kritische processen.
2. **Publieke waarden borgen**, zoals betrouwbaarheid, continuïteit van dienstverlening, transparantie en bescherming van persoonsgegevens.
3. **Het fundament vormen voor tactisch beleid en uitvoering**, via onderliggende beleidsdocumenten en de planning- en controlcyclus.

Het beleid sluit aan bij actuele wetgeving (o.a. AVG, NIS2/Cyberbeveiligingswet, BIO2), technologische ontwikkelingen en landelijke kaders. Daarnaast geldt dat op basis van de vastgestelde iVisie digitalisering een strategisch vraagstuk is voor de gemeente. Informatiebeveiliging en privacy zijn hierin kaderstellend en moeten daarom vanaf het begin meegewogen worden bij besluitvorming, beleidsontwikkeling en organisatieverandering.

De bestuurlijke verantwoordelijkheden zijn duidelijk belegd: de **gemeenteraad** stelt het strategische kader vast en vervult een kaderstellende en controlerende rol. Het **college** is bestuurlijk verantwoordelijk voor uitvoering, sturing en verantwoording. **Directie en afdelingshoofden** zorgen voor vertaling, samenhang en toepassing in de organisatie. **Medewerkers** handelen binnen de vastgestelde kaders. ENSIA en de planning- en controlcyclus vormen het structurele kader voor verantwoording.

Het document biedt richting **voor risicogestuurd werken** en voor het maken van bewuste keuzes in digitaliseringsprojecten, ketensamenwerkingen en inzet van nieuwe technologieën. Het vraagt om een organisatiecultuur waarin bewust handelen, voorbeeldgedrag en structurele aandacht voor informatiebeveiliging en privacy centraal staan.

1.2 Reikwijdte van het beleid

Dit beleid heeft betrekking op de bescherming van informatie en persoonsgegevens binnen alle taken en verantwoordelijkheden van de gemeente. Het beleid benadert informatiebeveiliging en privacy in samenhang en geldt voor de gehele organisatie.

Het beleid geldt voor alle vormen van informatieverwerking tijdens de volledige levenscyclus van informatie, van ontstaan en gebruik tot opslag, uitwisseling, archivering en vernietiging. Dit geldt voor zowel digitale als niet-digitale informatie, ongeacht de manier waarop deze wordt vastgelegd.

Het beleid is van toepassing op het college, de gemeenteraad, medewerkers en andere personen die onder verantwoordelijkheid van de gemeente werken. Daarnaast geldt het beleid voor externe partijen en samenwerkingsverbanden voor zover zij namens of in opdracht van de gemeente informatie verwerken of onder de bestuurlijke verantwoordelijkheid van de gemeente vallen.

Dit beleid bevat geen uitvoerende maatregelen of projecten. De nadere uitwerking vindt plaats in tactisch beleid en binnen de planning- en controlcyclus.

Dit beleid helpt bestuur en management om op een samenhangende, uitlegbare en toekomstbestendige manier sturing te geven aan digitale veiligheid, privacy en betrouwbare dienstverlening.

2. Wettelijke en normatieve kaders

Dit beleid is opgesteld binnen een samenhangend geheel van wettelijke, normatieve en bestuurlijke kaders. Deze kaders bepalen de ruimte waarbinnen de gemeente haar verantwoordelijkheid neemt voor informatiebeveiliging en privacy en vormen het fundament onder bestuurlijke keuzes en sturing.

Voor de verwerking en bescherming van persoonsgegevens handelt de gemeente volgens de geldende wet- en regelgeving voor gegevensbescherming, waaronder de Algemene verordening gegevensbescherming en nationale uitvoeringswetgeving. Bij taken waarbij politiegegevens worden verwerkt, zoals binnen toezicht en handhaving, is aanvullend de Wet politiegegevens van toepassing. Deze wet stelt specifieke eisen aan de bescherming, verwerking en het toezicht op politiegegevens en vormt binnen dit beleid een aanvullend wettelijk kader.

De gemeente handelt binnen de geldende en in ontwikkeling zijnde wet- en regelgeving op het gebied van digitale veiligheid, waaronder de Cyberbeveiligingswet als nationale uitwerking van de NIS2-richtlijn. Deze regelgeving benadrukt de bestuurlijke verantwoordelijkheid voor informatiebeveiliging, risicomanagement en toezicht en vormt een belangrijk kader voor dit strategisch beleid. Gemeenten worden onder deze wet van rechtswege aangemerkt als essentiële entiteit.

Na inwerkingtreding brengt de Cyberbeveiligingswet voor de gemeente concrete verplichtingen met zich mee. Dit betreft in ieder geval de zorgplicht om passende en evenredige maatregelen te treffen, de meldplicht voor significante incidenten, de registratieplicht en de plicht om risico's aantoonbaar te beheersen. Voor de invulling van de zorgplicht geldt de Baseline Informatiebeveiliging Overheid als nadere uitwerking. De meldplicht loopt via het voor de gemeentelijke sector aangewezen Computer Security Incident Response Team, dat is belegd bij de Informatiebeveiligingsdienst voor gemeenten (IBD). Het externe toezicht op de naleving van de wet berust bij de daartoe aangewezen rijksinspectie en staat los van de horizontale verantwoording via ENSIA en de planning- en controlcyclus.

De wet legt daarnaast een verantwoordelijkheid bij het bestuur voor het goedkeuren van en toezien op de maatregelen voor risicobeheersing. In dat verband geldt voor de leden van het college en voor de ambtelijke leiding een kennis- en scholingsverplichting, zodat zij digitale risico's kunnen herkennen en de maatregelen en gevolgen daarvan kunnen beoordelen. Deze kennis wordt actueel gehouden en is aantoonbaar.

Voor informatiebeveiliging hanteert de gemeente de Baseline Informatiebeveiliging Overheid, versie 2, als leidend normenkader. De BIO2 gaat uit van een risicogestuurde en passende benadering en sluit aan bij landelijk geldende afspraken voor informatiebeveiliging binnen de overheid. De BIO2 is daarbij mede gebaseerd op internationaal erkende normen voor informatiebeveiliging en risicomanagement, waaronder ISO 27001, ISO 27002 en ISO 27005. Deze normen fungeren als referentiekader voor de inrichting en beoordeling van informatiebeveiliging. Wanneer van BIO2-maatregelen wordt afgeweken, gebeurt dit uitsluitend op basis van een expliciete risicoafweging. De acceptatie van dergelijke restrisico's wordt bestuurlijk vastgesteld.

Voor de bestuurlijke verantwoording over informatiebeveiliging en privacy maakt de gemeente gebruik van de ENSIA-systematiek. ENSIA vormt het samenhangende kader waarbinnen het college verantwoording aflegt over de naleving van relevante normen en wettelijke verplichtingen en ondersteunt de controlerende rol van de gemeenteraad.

Bij het bepalen van accenten en prioriteiten betreft de gemeente het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten, zoals opgesteld door de IBD. Dit dreigingsbeeld biedt inzicht in actuele ontwikkelingen en dreigingen en vormt een belangrijke bron voor risicogestuurde

beleidsvorming. De gemeente weegt deze inzichten steeds in samenhang met de eigen context, risico's, afhankelijkheden en bestuurlijke prioriteiten.

De gemeente maakt waar mogelijk gebruik van het ondersteuningsaanbod en de collectieve kennis van de IBD. Dit draagt bij aan een eenduidige toepassing van normen en aan aansluiting bij landelijke ontwikkelingen en toezicht.

Informatiebeveiliging binnen de gemeente heeft betrekking op zowel informatie en communicatietechnologie als operationele technologie. Onder operationele technologie vallen systemen die fysieke processen in de buitenwereld en gebouwen aansturen, zoals klimaatbeheersing in gebouwen, verkeerslichten, en het openen van bruggen en gemalen. Voor de bescherming van deze systemen sluit de gemeente aan bij de door de IBD ontwikkelde aanpak, gebaseerd op de Cybersecurity Implementatie Richtlijn, als aanvullend kader binnen dit beleid.

Voor specifieke vormen van gegevensverwerking kunnen aanvullende sectorale normen van toepassing zijn. Welke normen in een concreet geval relevant zijn, wordt bepaald op basis van de aard van de verwerking, de wet- en regelgeving en de risico's die zijn geconstateerd. Een voorbeeld hiervan is de wettelijke verplichte norm NEN 7510 voor partijen die gezondheidsinformatie verwerken.

Technologische ontwikkelingen, waaronder het gebruik van kunstmatige intelligentie, beïnvloeden de verwerking van informatie en de risico's die daaruit voortvloeien. Deze ontwikkelingen worden beschouwd binnen de bestaande kaders voor informatiebeveiliging en privacy, waarbij zorgvuldigheid, uitlegbaarheid en bescherming van persoonsgegevens richtinggevend zijn. Nadere uitwerking vindt plaats in afzonderlijk beleid en in tactische plannen, waarin onder meer aandacht wordt besteed aan de zorgvuldige, uitlegbare en verantwoorde toepassing van nieuwe technologieën.

3. Visie en uitgangspunten

3.1 Visie op informatiebeveiliging en privacy

De gemeente wil een betrouwbare en zorgvuldige overheid zijn die het vertrouwen van inwoners, ondernemers en medewerkers verdient en behoudt. Informatiebeveiliging en privacy vormen daarbij een noodzakelijke voorwaarde voor het uitvoeren van gemeentelijke taken en voor het bieden van betrouwbare, toegankelijke en zorgvuldige dienstverlening in een digitale samenleving.

Informatiebeveiliging en privacy worden beschouwd als een integraal onderdeel van goed bestuur. Zij maken onderdeel uit van de manier waarop de gemeente werkt, besluiten neemt en verantwoording aflegt. Digitale veiligheid en een zorgvuldige omgang met gegevens zijn daarmee een gezamenlijke verantwoordelijkheid van bestuur, management en organisatie.

Deze visie sluit aan bij de leidende principes voor digitalisering binnen de gemeente, zoals verwoord in het Manifest Digitaal Nieuwegein. Daarbij staat een zorgvuldige omgang met gegevens, bescherming van privacy en veilige digitale dienstverlening centraal.

De gemeente kiest voor een samenhangende benadering waarin de bescherming van informatie en persoonsgegevens hand in hand gaat met het benutten van digitale mogelijkheden. Informatiebeveiliging en privacy ondersteunen betrouwbare dienstverlening, maatschappelijke opgaven en een zorgvuldige inzet van digitale middelen en data.

Informatiebeveiliging en privacy worden daarom tijdig betrokken bij nieuwe ontwikkelingen, beleidskeuzes en veranderingen binnen de organisatie. Door deze onderwerpen vanaf het begin mee te nemen in besluitvorming worden risico's beter beheerst en wordt het vertrouwen in het gemeentelijk handelen versterkt.

3.2 Uitgangspunten

Vanuit deze visie hanteert de gemeente de volgende uitgangspunten voor informatiebeveiliging en privacy. Deze uitgangspunten geven richting aan bestuurlijke keuzes en vormen het kader voor de verdere inrichting van informatiebeveiliging en privacy binnen de organisatie.

Mensgericht en passend

De gemeente hanteert een mensgerichte en passende benadering bij informatiebeveiliging en privacy. Daarbij wordt rekening gehouden met de belangen, mogelijkheden en verantwoordelijkheden van inwoners, medewerkers en samenwerkingspartners.

Met passend wordt bedoeld dat keuzes en maatregelen worden afgestemd op de aard van processen, de bijbehorende risico's en de maatschappelijke impact, in verhouding tot wat nodig en uitvoerbaar is.

Betrouwbare dienstverlening

Informatiebeveiliging en privacy vormen een basis voor een betrouwbare dienstverlening. Een zorgvuldige omgang met informatie en persoonsgegevens draagt bij aan de continuïteit en kwaliteit van dienstverlening.

Risicogestuurd

De gemeente werkt risicogestuurd. Keuzes over informatiebeveiliging en privacy worden gebaseerd op inzicht in risico's en worden bewust en uitlegbaar gemaakt op bestuurlijk niveau, in samenhang met maatschappelijke belangen en publieke waarden.

Transparant en verantwoord

De gemeente handelt transparant en legt verantwoording af over de wijze waarop informatiebeveiliging en privacy zijn ingericht en toegepast. Bestuurlijke keuzes zijn uitlegbaar en toetsbaar en passen binnen geldende wet- en regelgeving en vastgestelde kaders.

Security en privacy by design

Informatiebeveiliging en privacy worden vanaf het begin betrokken bij de ontwikkeling van beleid, processen, systemen en dienstverlening. Door deze uitgangspunten vroegtijdig toe te passen worden risico's beter onderkend en beheerst.

4. Ambitie 2026-2030

De gemeente versterkt in de periode 2026–2030 informatiebeveiliging en privacy als onderdeel van de bestuurlijke sturing op digitalisering, dienstverlening en informatiemanagement. Digitale risico's worden daarbij bewust en uitlegbaar afgewogen in samenhang met maatschappelijke belangen en publieke waarden.

De gemeente bepaalt het gewenste volwassenheidsniveau van informatiebeveiliging en privacy op basis van een risicogestuurde en passende benadering. Daarbij wordt onderscheid gemaakt tussen kritische processen en overige processen. Kritische processen zijn processen waarvan uitval, misbruik of datalekken directe gevolgen kunnen hebben voor de continuïteit van dienstverlening, de veiligheid van inwoners of het vertrouwen in het gemeentelijk handelen.

Voor kritische processen is de ambitie gericht op het realiseren en in stand houden van een aantoonbaar volwassenheidsniveau dat past bij geldende wetgeving, landelijke kaders en de maatschappelijke impact van deze processen. Voor overige processen streeft de gemeente naar een passend volwassenheidsniveau, afgestemd op de aard van het proces, de risico's en de uitvoerbaarheid binnen de organisatie.

Om de ontwikkeling van informatiebeveiliging in lijn met deze risicogestuurde benadering te kunnen volgen en duiden, hanteert de gemeente een volwassenheidsmodel, gebaseerd op gangbare modellen zoals het Capability Maturity Model Integration (CMMI). Dit model ondersteunt het bestuur en de organisatie bij het inzichtelijk maken van de ontwikkeling van informatiebeveiliging, het bepalen van prioriteiten en het onderscheiden van passende niveaus voor kritische en overige processen.

De gemeente hanteert daarbij als bestuurlijke ambitie een volwassenheidsniveau dat minimaal overeenkomt met niveau 3 van het gehanteerde model. Dit niveau staat voor een organisatiebrede en gestandaardiseerde inrichting van processen voor informatiebeveiliging en ondersteunt een consistente toepassing van beleid, risicomanagement en bestuurlijke verantwoording.

Het realiseren en in stand houden van dit ambitieniveau vraagt om een reële verhouding tussen ambitie, capaciteit en middelen. De gemeente bepaalt daarom op basis van een nulmeting het huidige volwassenheidsniveau, stelt een realistisch groeipad vast en verbindt hieraan de benodigde personele en financiële middelen. Het college betreft deze samenhang bij de planning- en controlcyclus en legt hierover verantwoording af aan de gemeenteraad, zodat de vastgestelde ambitie en de beschikbare middelen met elkaar in evenwicht blijven.

De vertaling van deze ambitie naar prioriteiten en activiteiten vindt plaats in onderliggende tactische beleidsdocumenten en binnen de planning- en controlcyclus.

5. Strategische thematische accenten

Dit hoofdstuk beschrijft de strategische thema's voor informatiebeveiliging en privacy in de periode 2026–2030. Deze thema's geven richting aan bestuurlijke keuzes en vormen het kader voor verdere uitwerking in tactisch beleid en de planning- en controlcyclus.

Binnen deze thema's wordt gestuurd op een samenhangend geheel van beveiligingsdoelen. Deze doelen geven richting aan de bescherming van informatie en persoonsgegevens en ondersteunen de bestuurlijke afwegingen die voortvloeien uit de visie, uitgangspunten en ambitie van dit beleid.

De gemeente past informatieclassificatie toe om de bescherming van informatie en persoonsgegevens af te stemmen op de aard, gevoeligheid en het risico van de betreffende informatie.

De volgende beveiligingsdoelen vormen hiervoor het uitgangspunt.

Vertrouwelijkheid

Informatie en persoonsgegevens zijn uitsluitend toegankelijk voor personen die daarvoor geautoriseerd zijn.

Integriteit

Informatie is juist, volledig en aantoonbaar betrouwbaar gedurende de gehele levenscyclus van informatie.

Beschikbaarheid

Informatie en digitale dienstverlening zijn tijdig beschikbaar, passend bij de behoeften van de organisatie en de afspraken met inwoners, ondernemers en partners.

Controleerbaarheid en transparantie

De gemeente waarborgt dat de werking van maatregelen, de naleving van kaders en de bestuurlijke verantwoording voldoende inzichtelijk en toetsbaar zijn.

Veerkracht

De organisatie is in staat digitale verstoringen en incidenten te voorkomen, op te vangen, te herstellen en hiervan te leren.

5.1 Risicogestuurd werken

Risicogestuurd werken is een strategisch uitgangspunt voor informatiebeveiliging en privacy binnen de gemeente. Inzicht in risico's geeft richting aan bestuurlijke keuzes, prioriteiten en de afweging tussen bescherming, uitvoerbaarheid en maatschappelijke impact.

Binnen dit beleid is risicomanagement gericht op inzicht in risico's die de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en persoonsgegevens kunnen beïnvloeden. Daarbij wordt onderkend dat niet alle risico's volledig kunnen of hoeven te worden weggenomen.

Bij het bepalen van risico's wordt ook rekening gehouden met de afhankelijkheid van externe partijen, leveranciers en samenwerkingsverbanden. De continuïteit en veiligheid van gemeentelijke dienstverlening zijn mede afhankelijk van deze ketens. Dit vraagt om bestuurlijke aandacht voor risico's, verantwoordelijkheden en onderlinge afspraken.

Bestuurlijke keuzes over risico's worden expliciet en uitlegbaar gemaakt in samenhang met maatschappelijke belangen en publieke waarden. De verdere uitwerking vindt plaats in onderliggende tactische beleidsdocumenten.

5.2 Privacy en gegevensbescherming

De gemeente hecht belang aan een zorgvuldige en rechtmatige verwerking van persoonsgegevens. Privacy en gegevensbescherming maken onderdeel uit van goed bestuur en dragen bij aan het vertrouwen van inwoners, ondernemers en samenwerkingspartners.

Bij de verwerking van persoonsgegevens handelt de gemeente volgens geldende wet- en regelgeving. Daarbij staan de bescherming van rechten en vrijheden van betrokkenen en het voorkomen van onnodige risico's centraal.

Privacybescherming wordt in samenhang met informatiebeveiliging vormgegeven. Daarbij staat de bescherming van rechten en vrijheden van betrokkenen centraal.

5.3 Continuïteitmanagement van digitale dienstverlening

Digitale dienstverlening is essentieel voor het functioneren van de gemeente en de uitvoering van haar taken. Verstoringen kunnen directe gevolgen hebben voor dienstverlening, veiligheid en vertrouwen.

De continuïteit van digitale dienstverlening is daarom een strategisch aandachtspunt. Dit beleid stelt kaders voor weerbaarheid, voorbereiding op verstoringen, bestuurlijke escalatie en herstel van dienstverlening. Binnen deze kaders zorgt het college voor uitvoering, sturing en verantwoording, zodat de beschikbaarheid van informatie en systemen, en de zorgvuldige omgang met persoonsgegevens ook onder versturende omstandigheden zo goed mogelijk geborgd blijven.

Binnen deze kaders zorgt de organisatie voor een passende inrichting van respons, samenwerking en herstelvermogen, zodat bij digitale verstoringen beheerst kan worden gehandeld en de continuïteit van dienstverlening zo veel mogelijk behouden blijft.

5.4 Weerbare organisatie en bewust handelen

Informatiebeveiliging en privacy zijn niet alleen afhankelijk van systemen en processen, maar ook van het handelen van medewerkers binnen de organisatie. Een organisatie waarin medewerkers zich bewust zijn van hun verantwoordelijkheid draagt bij aan het beperken van risico's en het versterken van digitale weerbaarheid.

Binnen deze kaders stimuleert het college een organisatiecultuur waarin informatiebeveiliging en privacy onderdeel zijn van professioneel handelen en dagelijks werk. Duidelijke verwachtingen, voorbeeldgedrag van bestuur en leidinggevend en aandacht voor bewustwording dragen bij aan een organisatie die risico's tijdig herkent, zorgvuldig handelt en passend kan reageren op incidenten en verstoringen.

5.5 Verantwoording

Het college legt binnen de reguliere planning- en controlcyclus verantwoording af aan de gemeenteraad over informatiebeveiliging en privacy. Daarbij wordt periodiek inzicht gegeven in risico's, relevante ontwikkelingen, naleving van kaders en de mate waarin informatiebeveiliging en privacy binnen de organisatie zijn geborgd.

6. Bestuurlijke sturing, rollen en verantwoordelijkheden

Binnen de gemeente is een samenhangende inrichting van sturing, verantwoordelijkheden en verantwoording voor informatiebeveiliging en privacy aanwezig. De gemeenteraad stelt met dit beleid het strategische kader vast en vervult een kaderstellende en controlerende rol.

Het college van burgemeester en wethouders is bestuurlijk verantwoordelijk voor uitvoering, sturing en verantwoording binnen dit kader. Het college bepaalt bestuurlijke prioriteiten, maakt bewuste en uitlegbare keuzes over digitale risico's en legt hierover verantwoording af aan de gemeenteraad.

De directie, het management en overige functionarissen zijn binnen de organisatie verantwoordelijk voor de vertaling van dit kader naar sturing, uitwerking, uitvoering, beheersing en advisering, ieder vanuit de eigen rol. Dit beleid richt zich daarmee op de samenhang tussen kaderstelling, bestuurlijke verantwoordelijkheid, politieke aanspreekbaarheid en organisatorische verantwoording.

6.1 Gemeenteraad en college

De gemeenteraad stelt het strategische kader voor informatiebeveiliging en privacy vast en vervult een kaderstellende en controlerende rol. Op basis van dit beleid en de bestuurlijke verantwoording kan de raad het college aanspreken op gemaakte keuzes, gestelde prioriteiten, beschikbare middelen en de mate waarin informatiebeveiliging en privacy binnen de gemeente zijn geborgd.

Het college van burgemeester en wethouders is bestuurlijk verantwoordelijk voor uitvoering, sturing en verantwoording. Binnen de vastgestelde kaders bepaalt het college bestuurlijke prioriteiten en maakt het bewuste en uitlegbare keuzes over digitale risico's in samenhang met publieke waarden, continuïteit van dienstverlening en rechtmatige verwerking van persoonsgegevens.

Het college laat zich periodiek informeren over risico's, relevante ontwikkelingen, naleving van kaders en de mate waarin informatiebeveiliging en privacy binnen de organisatie zijn geborgd. Op basis daarvan kan het college bestuurlijk bijsturen en, waar nodig, aanvullende maatregelen treffen of voorstellen aan de gemeenteraad voorleggen.

De vaststelling van dit strategisch kader door de gemeenteraad laat de wettelijke verantwoordelijkheid van het college onverlet. Op grond van de Cyberbeveiligingswet rusten de zorgplicht, de meldplicht, de registratieplicht en de daaruit voortvloeiende bestuurlijke verantwoordelijkheid voor informatiebeveiliging op het college van burgemeester en wethouders. De kaderstellende vaststelling door de gemeenteraad geeft hieraan bestuurlijke legitimiteit en richting, maar verplaatst deze wettelijke verantwoordelijkheid niet naar de gemeenteraad.

6.2 Governance en verantwoordingsstructuur

De verantwoording over informatiebeveiliging en privacy vindt plaats binnen de bestaande bestuurlijke verantwoordingsstructuren. De ENSIA-verantwoording en de planning- en controlcyclus bieden periodiek inzicht in risico's, relevante ontwikkelingen, naleving van vastgestelde kaders en de mate van borging.

Deze informatie ondersteunt het college in zijn bestuurlijke verantwoordelijkheid en stelt de gemeenteraad in staat zijn kaderstellende en controlerende rol te vervullen. Daarmee wordt aangesloten bij de reguliere wijze waarop de gemeente stuurt, verantwoordt en bijstuurt.

ENSIA en de planning- en controlcyclus vormen het kader voor de horizontale verantwoording binnen de gemeente. Daarnaast kent de Cyberbeveiligingswet een vorm van extern, verticaal toezicht dat hiervan losstaat. Dit toezicht wordt uitgeoefend door de daartoe aangewezen rijksinspectie en richt zich op de naleving van de wettelijke zorg-, meld- en registratieplicht. De gemeente richt haar verantwoording zo in dat zij zowel de horizontale verantwoording als het externe toezicht op samenhangende en aantoonbare wijze kan bedienen.

6.3 Directie en afdelingshoofden

Directie

De directie is verantwoordelijk voor de vertaling van het strategisch informatiebeveiligings- en privacybeleid naar tactisch niveau. De directie zorgt voor de verdere uitwerking binnen de planning- en controlcyclus en, waar nodig, in onderliggende beleidsdocumenten. Daarbij bewaakt de directie de samenhang tussen informatiebeveiliging, privacy en andere relevante beleidsdomeinen en ondersteunt zij het college in de bestuurlijke sturing, monitoring en verantwoording.

De directie en de ambtelijke leiding beschikken daarbij over de kennis en vaardigheden die nodig zijn om digitale risico's te herkennen en de maatregelen en gevolgen daarvan te beoordelen, in lijn met de eisen die de Cyberbeveiligingswet aan de leiding van de organisatie stelt.

Afdelingshoofden

Afdelingshoofden zijn verantwoordelijk voor de toepassing en bewaking van de vastgestelde kaders binnen hun eigen verantwoordelijkheidsgebied. Zij zorgen ervoor dat informatiebeveiliging en privacy binnen de afdeling tijdig worden betrokken bij regulier management, beleidsvorming, besluitvorming en veranderingen. Afdelingshoofden signaleren risico's en relevante ontwikkelingen, bereiden vraagstukken vanuit de afdeling voor en brengen deze in via de reguliere sturingslijnen, zodat de directie in staat wordt gesteld om samenhangend en integraal te sturen op informatiebeveiliging en privacy.

6.4 Ondersteunende en toezichthoudende rollen

Ondersteunende en toezichthoudende rollen ondersteunen het college, de directie en het management bij de invulling van hun verantwoordelijkheden. Zij adviseren, signaleren risico's en dragen ieder vanuit hun eigen rol en wettelijke positie bij aan toezicht, samenhang en verantwoording.

De **Chief Information Security Officer** heeft een onafhankelijke adviesrol ten aanzien van informatiebeveiliging en ondersteunt het college, de directie en het management bij risicovraagstukken, sturing en verantwoording.

De **Functionaris Gegevensbescherming** houdt vanuit een onafhankelijke toezichthoudende rol toezicht op de naleving van privacywetgeving en adviseert over de bescherming van persoonsgegevens.

De **Privacy Officer** ondersteunt de organisatie bij de toepassing van het privacybeleid en draagt bij aan samenhang en consistentie in de omgang met persoonsgegevens.

De **concerncontroller** ondersteunt het college, de directie en het management bij de samenhang tussen risicomanagement, planning en control en bestuurlijke verantwoording. Vanuit deze rol draagt de concerncontroller bij aan de toetsbaarheid en beheersing van informatiebeveiliging en privacy binnen de organisatie.

De **ENSIA-coördinator** ondersteunt de gemeente bij de samenhangende verantwoording over informatiebeveiliging en privacy richting toezicht en audit.

Deze rollen hebben een adviserende, ondersteunende of toezichthoudende functie en zijn niet verantwoordelijk voor bestuurlijke besluitvorming.

6.5 Medewerkers

Medewerkers en andere personen die onder verantwoordelijkheid van de gemeente werkzaamheden verrichten, gaan zorgvuldig om met informatie en persoonsgegevens binnen de kaders van dit strategisch beleid en de daarop gebaseerde tactische uitwerkingen.

Van medewerkers wordt verwacht dat zij handelen in overeenstemming met vastgestelde beleidskaders en dat zij informatiebeveiliging en privacy betrekken bij de uitvoering van hun werkzaamheden.

Het management ondersteunt medewerkers door informatiebeveiliging en privacy onderdeel te laten zijn van reguliere werkprocessen, communicatie en bewustwording, zodat het gewenste gedrag structureel wordt geborgd binnen de organisatie.

Als onderliggende ambtelijke uitwerking bij dit beleid wordt een RASCI-tabel gebruikt. Daarin is de verdeling van rollen en verantwoordelijkheden voor informatiebeveiliging en privacy nader uitgewerkt ten behoeve van governance, beheersing en uitvoering.

7. Borging en herziening

De borging van dit beleid vindt plaats via onderliggende tactische beleidsdocumenten, de planning- en controlcyclus en de periodieke verantwoording van het college aan de gemeenteraad.

Binnen deze cyclus wordt periodiek inzicht gegeven in risico's, ontwikkelingen en de naleving van de vastgestelde kaders voor informatiebeveiliging en privacy. Deze informatie ondersteunt het college bij uitvoering, sturing en verantwoording en ondersteunt de gemeenteraad bij zijn kaderstellende en controlerende rol.

De ontwikkeling van het volwassenheidsniveau van informatiebeveiliging wordt daarbij gevolgd met behulp van het gehanteerde volwassenheidsmodel. De uitkomsten worden betrokken bij bestuurlijke afwegingen, prioriteiten en de verdere ontwikkeling van informatiebeveiliging en privacy binnen de organisatie.

Ontwikkelingen in wetgeving, technologie, dreigingen en organisatie worden periodiek meegenomen bij de beoordeling van dit beleid.

Herziening van dit strategisch beleid is een bevoegdheid van de gemeenteraad. Wanneer zich tussentijds wezenlijke wijzigingen voordoen die van invloed zijn op de visie, uitgangspunten of bestuurlijke sturing, wordt het beleid herzien. In alle andere gevallen vindt herziening plaats aan het einde van de beleidsperiode.

De onderliggende tactische beleidskaders en uitvoeringsdocumenten worden door het college en de directie vastgesteld en waar nodig tussentijds geactualiseerd, zonder dat hiervoor een nieuw besluit van de gemeenteraad nodig is. Zo blijft de organisatie in staat om tijdig in te spelen op ontwikkelingen in wetgeving, technologie en dreigingen, terwijl het strategische kader stabiel blijft gedurende de beleidsperiode.

Vastgesteld door de gemeenteraad van Nieuwegein op 17 september 2026