Gemeentelijk Informatiebeveiligingsbeleid Nijmegen 2025

Versiebeheer
Het versiebeheer van dit document ligt bij de CISO.

Kenmerk:	E25.002350
Versie:	1.0
Versiedatum:	16 december 2025
Portefeuillehouder	Tobias van Elferen
Goedgekeurd door:	CISO

1. Inleiding

Hoe zorgen we ervoor dat onze informatie niet op straat komt te liggen? In een wereld die steeds meer digitaal wordt, is informatiebeveiliging steeds belangrijker. Daarom heeft de gemeente beleid voor de beveiliging van informatie. Het bestaande beleid is verouderd. Daarom is het tijd voor een nieuw informatiebeveiligingsbeleid. Dit document beschrijft het informatiebeveiligingsbeleid van de gemeente Nijmegen voor de jaren 2025 tot 2028 en vervangt het in 2022 vastgestelde informatiebeveiligingsbeleid. Dit document is richtinggevend en kaderstellend en wordt aangevuld met een uitwerkingsdocument op tactisch niveau en werkinstructies op operationeel niveau.

Met dit gemeentelijk informatiebeveiligingsbeleid zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te bouwen op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit beleid is de Baseline Informatie Overheid (BIO) versie 2 op basis van de industrie standaard NEN-ISO/IEC 27002:2022. Deze vormen het normenkader bij de Cyberbeveiligingswet. Het informatiebeveiligingsbeleid geeft uitvoering aan onze doelen om ethisch en in lijn met wet- en regelgeving te handelen, en bovendien de identiteit van de Nijmegenaar te registreren en te beschermen.

1.1. Leeswijzer

In hoofdstuk 2 wordt de kern van het gemeentelijk beleid uiteengezet. Dit beleid wordt aangevuld met specifieke tactische beleidsregels op onderwerpen zoals fysieke- en logische toegang, kunstmatige intelligentie, bedrijfscontinuïteit, enzovoorts, in het uitwerkingsdocument. Dit wordt gedaan op basis van input van ambtelijk opdrachtgevers, de CISO, de ISO, de privacy functionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de Informatiebeveiligingsdienst (IBD) en de uitkomsten van risicoanalyses en DPIA's. In het ISMS staan de acties en planning vermeld om de praktijk in overeenstemming te brengen met het beleid. Hoofdstuk 3 beschrijft hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2. Wat is informatiebeveiliging?

Informatiebeveiliging gaat over het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening (werkprocessen, gebruikte applicaties en opgeslagen gegevens) aantoonbaar te garanderen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot Informatie Technologie

en Operationele Technologie (IT en OT) en het heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

De meeste incidenten komen niet voort uit een gebrekkige techniek, maar door menselijk handelen en tekortschietende procesorganisatie. Maatregelen op het gebied van informatiebeveiliging beperken zich dan ook niet alleen tot technische maatregelen maar gaan ook over verantwoord en bewust gedrag van medewerkers. Bewustzijn, kennis, integriteit en de bescherming van onze informatiestromen gaan hand in hand.

1.3. Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke taken goed uit te kunnen voeren. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of publiekszaken.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat. Vanuit de AVG hebben wij de plicht om persoonsgegevens zorgvuldig te beveiligen.

2. Gemeentelijk beleid

2.1 Doel

Het doel van het ‘Gemeentelijk informatiebeveiligingsbeleid Nijmegen 2025’ is het voldoen aan relevante wet en regelgeving, richting geven aan de organisatie op het vlak van informatiebeveiliging en het stellen van kaders. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in risicogerichte plannen en draagt bij aan de beschikbaarheid, integriteit en vertrouwelijkheid van onze dienstverlening. Het beleid op informatiebeveiliging dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van een informatieveilige gemeente.

2.2. Ontwikkelingen

Er zijn diverse ontwikkelingen op gebied van informatiebeveiliging. Deze ontwikkelingen krijgen een plek in het nieuwe beleid. De ontwikkelingen die van belang zijn voor de actualisering van het infomatiebeveiligingsbeleid zijn de volgende:

2.2.1. De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van de BIO2 is gericht op risicomanagement. Dat wil zeggen dat proces eigenaren nu meer dan vroeger werken volgens de aanpak van de ISO 27001(industrie standaard waarin beschreven wordt hoe een informatiebeveiligingsmanagementsysteem in elkaar zit)[1] . Dit houdt voor het management in dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Daarbij wordt de aanpak bepaald aan de hand van het risico dat de organisatie loopt. In dit strategisch beleid sorteren we voor richting de BIO2.

2.2.2. De WPG

De gemeente heeft BOA's in dienst die gegevens verwerken die onder de wet Politiegegevens (WPG) vallen, evenals medewerkers leerplicht en sociaal rechercheurs waar hetzelfde voor geldt. Hiervoor moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

Er is een belangrijke overlap met privacy als het gaat om de beheerstructuren en de juiste organisatorische en technische maatregelen ter bescherming van persoonsgegevens, zoals bedoeld door de AVG. Voor aanvullingen op het vlak van privacy wordt verwezen naar het privacy beleid van gemeente Nijmegen zoals vastgesteld door het college van Burgemeester en Wethouders.

2.2.3. De 10 principes voor informatiebeveiliging[2]

De 10 principes voor informatiebeveiliging, opgesteld door de VNG, zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.

[1] NEN-EN-ISO/IEC 27001:2023 nl

[2] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

Deze principes zijn onderdeel van ons huidige beleid. We nemen ze opnieuw op als uitgangspunt in deze beleidsherziening omdat ze ook nu van toepassing zijn. De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.4. Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

Het dreigingsbeeld informatiebeveiliging Nederlandse gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee belangrijk om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.5. Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie over onze kwetsbaarheden. Daarom zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3. Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2022. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2023 genomen. Dit normenkader ligt ook onder de Baseline Informatiebeveiliging Overheid (BIO2). Het implementeren van deze baseline is voor gemeenten noodzakelijk om te voldoen aan de Cyberbeveiligingswet (Cbw). De Cyberbeveiligingswet (Cbw) is de Nederlandse omzetting van de Europese Network and Information Security Directive (NIS2). Deze is ontwikkeld om de weerbaarheid van overheidsorganisaties en vitale sectoren tegen cyberdreigingen te vergroten. De BIO2 sluit aan bij actuele dreigingsbeelden, technologische ontwikkelingen en internationale normen.
De NIS2-richtlijn, vastgesteld door de Europese Unie in 2023, heeft als doel de cyberweerbaarheid van essentiële en belangrijke entiteiten binnen de lidstaten te harmoniseren en te versterken. Gemeenten die publieke taken uitvoeren en persoonsgegevens verwerken, vallen als essentiële entiteiten binnen het toepassingsbereik van de NIS2.

Binnen de gemeente wordt naast IT ook OT ingezet. Met OT worden systemen bedoeld voor de besturing, bewaking en beheer van fysieke processen. Denk aan technologie die nodig is om verkeerslichten of een gemaal te bedienen. Als norm voor het beschermen van OT wordt verwezen naar de Cybersecurity Implementatie Richtlijn (CSIR)[3] versie 3.0. Daarnaast hanteert gemeente Nijmegen ook meer gespecialiseerde normen zoals voor DigiD, waardedocumenten, SUWI en voor veilig mailen (NEN7516).

2.4. Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord. Dit gebruik is in scope ongeacht de uitingsvorm van de informatie, locatie, tijdstip en gebruikte apparatuur. Binnen de scope valt ook alle operationele technologie (OT) die gebruikt wordt binnen de gemeentegebouwen en in de publieke ruimte van de gemeente, en die eigendom is van de gemeente, zoals gebouwbeheersystemen, cameratechnologie, pompen en gemalen.

2.6. Uitgangspunten

De bestuurlijke principes leiden, met de hierboven genoemde standaarden, tot de uitgangspunten die we hierna beschrijven. De rollen en verantwoordelijkheden worden beschreven in hoofdstuk 3.

2.6.1. Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het inrichten en beheren van een structuur voor informatiebeveiliging, inclusief het beleggen van verantwoordelijkheden en de inbedding in een planning en control cyclus. Hiermee bereiken wij volwassenheidsniveau 3 van het Capability Maturity Model (CMM).
- Het bewerkstelligen van een veilige cultuur voor het werken met informatie. Onderdeel hier van is scholing, oefening en leren van incidenten. Hiermee wordt informatiebeveiliging effectief.
- Het op elke laag toepassen van maatregelen op basis van risico, van dataminimalisatie tot continuïteit, door de gehele organisatie. Hiermee wordt informatiebeveiliging efficiënt.
- Het samenwerken met en toezien op de maatregelen in de (keten)samenwerking. Hiermee nemen wij onze verantwoordelijkheid en zijn wij een sterke schakel.

[3] https://www.cert-wm.nl/csir

2.6.2. Randvoorwaarden

Onderstaande randvoorwaarden zijn van belang om risico`s inzichtelijk te kunnen krijgen en verantwoording af te kunnen leggen. Belangrijke randvoorwaarden zijn:

- De informatiebeveiligingseisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging binnen de organisatie dient actief bevorderd en geborgd te worden.
- Maatregelen worden gestructureerd geïmplementeerd op basis van urgentie en haalbaarheid.
- Om uitvoering te kunnen geven aan dit gemeentelijk beleid en het informatiebeveiligingsplan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

2.6.3 Informatiebeveiliging wordt ondersteund door architectuur

Informatiebeveiliging is een basisprincipe van de informatiearchitectuur van gemeente Nijmegen en is uitgewerkt als onderdeel van die architectuur. De architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie). Dit is de uitwerking van principes als Privacy by Design en Privacy by Default.
De toewijzing van algoritmes, applicaties en gegevensverzamelingen die onder de verantwoordelijkheid van de concernmanager vallen, zijn gebaseerd op risicomanagement. Dat heeft gevolgen voor de beschermende maatregelen, maar ook voor de registratie in het verwerkingsregister en de te volgen inzageprocedure.

3. Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek die wij toepassen staat bekend als het Three Lines of Defense Model (3LD) model. In dit model is het management verantwoordelijk voor het realiseren van informatiebeveiliging binnen de eigen processen. De tweede lijn (SO, PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door interne toetsing van een objectief oordeel voorzien met mogelijkheden tot verbetering. Zowel het gemeentelijk beleid als de uitwerking informatiebeveiligingsbeleid Nijmegen 2025 zijn, na vaststelling, te vinden in Team Digitaal informatiebeleid.

Het bestuur, de directie en het GMT spelen een cruciale rol bij het uitvoeren van dit gemeentelijk IB beleid. Het college is eindverantwoordelijke voor de informatiebeveiliging. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het beleid is in lijn met de relevante landelijke en Europese wet- en regelgeving.

3.1. Verantwoordelijkheid: bestuur

Het college stelt als eindverantwoordelijke het gemeentelijk informatiebeveiligingsbeleid Nijmegen 2025 vast. College en raad zorgen er voor dat zij op de hoogte zijn van ontwikkelingen die de risico`s voor de gemeente op het vlak van informatiebeveiliging beïnvloeden. Zij laten zich informeren over de stand van zaken rond informatiebeveiliging bij de gemeente.

3.2. Aansturing: directieteam

De aansturing vindt plaats door de directie. Zij zorgt er met het gemeentelijk managementteam (GMT) voor dat alle processen, systemen en middelen altijd onder de verantwoordelijkheid vallen van een concernmanager. De directie spreekt de eigenaren aan op de beveiliging van de informatie die onder hen berust. Zij stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie zorgt er met de CISO en de CIO voor dat de relevante portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de stand van zaken rond de beveiliging van informatie in de bedrijfsvoering. Het bestuur kan op die manier haar richtinggevende rol vervullen.
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek en de bijbehorende collegeverklaring en rapportage. De raad wordt geïnformeerd over ENSIA en de stand van zaken op het vlak van informatiebeveiliging door middel van periodieke raadsbrieven.

3.2. Uitvoering: GMT/ambtelijk opdrachtgevers

Informatiebeveiliging is een verantwoordelijkheid van concernmanagers als eigenaren van processen en de bijbehorende systemen. Zij is ook een verantwoordelijkheid van alle ambtelijk opdrachtgevers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Alle processen, systemen, (persoons)gegevens, applicaties hebben 1 eigenaar; er is dus altijd iemand verantwoordelijk. Het GMT en ambtelijk opdrachtgevers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten.

Concernmanagers worden bij deze activiteiten ondersteund door adviserende functies op het vlak van informatie en automatisering, P&O, financiën en facilitair. Informatiebeveiliging is ook een verantwoordelijkheid van alle medewerkers. Het raakt de werkzaamheden van iedereen omdat alle ambtenaren toegang hebben tot systemen en informatie. Voor een verdere uitwerking van rollen en verantwoordelijkheden zie de uitwerking van het informatiebeveiligingsbeleid.

3.2.1 Medewerkers

Informatiebeveiliging is een verantwoordelijkheid van iedereen. Dit geldt ook voor alle medewerkers. Daarom neemt iedereen deel aan trainingen in het gebruik van beveiligingsprocedures, het signaleren van risicovolle situaties en de juiste omgang met bedrijfsmiddelen. Alle medewerkers hebben basiskennis van de privacywetgeving en weten deze toe te passen in hun dagelijks werk.

3.3. Controle en verantwoording

Dit informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de gemeente Nijmegen. Zij geven sturing aan het onderwerp informatiebeveiliging door het tonen van voorbeeldgedrag en het vragen om informatie.

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit gemeentelijke beleid.

De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. Jaarlijks rapporteert zij de resultaten van de interne toetsing aan diverse toezichthouders alsook aan de directie en het bestuur.

De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren aan het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin zij haar bevindingen en aanbevelingen vastlegt.

3.4.1. ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de Eenduidige Normatiek Single Information Audit (ENSIA). Deze systematiek wordt door de Rijksoverheid gebruikt voor de verantwoording aan de stelselhouders voor DIGID/WOZ/BAG/SUWI in plaats van de separate verantwoording per stelsel. De ENSIA coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke ambtelijk opdrachtgevers. De ambtelijk opdrachtgevers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA vragenlijsten.

De verantwoording over de informatiebeveiliging komt in de jaarlijkse rapportage informatiebeveiliging tot uitdrukking in de in control verklaring. Met deze verklaring geeft het college aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente zal treffen. In dit proces wordt ook verantwoording afgelegd per brief aan de raad.

4. Rechten van betrokkenen

De gemeente honoreert wettelijk gezien in beginsel alle rechten van betrokkenen op basis van de AVG. Hierbij moet het verzoek op basis van een recht van betrokkenen in evenredigheid staan met de belasting van de gemeentelijke organisatie. Het excessief opvragen van persoonsgegevens kan bestempeld worden als misbruik van recht. De gemeente voert een registratie van alle verzoeken.

5. Inwerkingtreding

Het gemeentelijk informatiebeveiligingsbeleid Nijmegen 2025 treedt in werking op de dag na bekendmaking, onder gelijktijdige intrekking van het Informatiebeveiligingsbeleid 2022.