Nijmegen

GEMEENTEBLAD

Officiële uitgave van de gemeente Nijmegen

Nr. 57565

10 februari

2022

Informatiebeveiligingsbeleid 2022 gemeente Nijmegen

Versiebeheer
Het versiebeheer van dit document ligt bij de CISO.
Kenmerk: E22.000031
Versie: 1.0
Versiedatum: 8 februari 2022
Portefeuillehouder Petra Molenaar
Goedgekeurd door: CISO
Classificatie: openbaar

Waarom is de veiligheid van onze informatie van belang?

Informatie in al zijn vormen is één van de belangrijkste bedrijfsmiddelen als gemeente. De toegankelijkheid, vertrouwelijkheid en betrouwbaarheid ervan zijn absolute raadvoorwaarden om onze gemeentelijke taken zo goed mogelijk en met zo min mogelijk middelen te kunnen uitvoeren. Daarbij mag van ons verwacht worden dat we verantwoord handelen, daarop aanspreekbaar zijn en transparant en proactief verantwoording afleggen naar burgers en raadsleden.
Denk aan de gevolgen wanneer:

- vertrouwelijke persoonsgegevens ‘op straat’ liggen
- ICT-systemen uitvallen
- informatie voor vitale maatschappelijke functies niet beschikbaar is (zoals voor verkeer, vervoer, openbare orde en veiligheid)
- politiek gevoelige informatie uitlekt
- partijen handelen met voorkennis op inkooptrajecten of speculeren op grondtransacties

Dit zijn incidenten met ernstige gevolgen. Niet alleen voor onze eigen bedrijfsvoering, maar ook voor burgers, bedrijven en onze partners. Gevolgen zijn mogelijk imagoschade, politieke consequenties maar ook financieel verlies en juridische consequenties.
Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is de manier waarop we dit realiseren. We moeten de informatie waarover we als gemeente beschikken goed beschermen. Hoe waardevoller de informatie, hoe strenger de te treffen maatregelen. Tegelijkertijd zien we de mogelijkheden van nieuwe technieken (bijv. data-analyses), die vragen om kaders om deze verantwoord te benutten.

Waar gaat informatiebeveiliging over?

Informatiebeveiliging gaat over het treffen van maatregelen om de betrouwbaarheid van werkprocessen, gebruikte applicaties en de daarin opgeslagen gegevens te garanderen, en te beschermen tegen bedreigingen van buitenaf.
Specifieker gaat het om ervoor te zorgen dat:

- beschikbaarheid/continuïteit: informatie op de juiste tijd en plaats beschikbaar is voor gebruikers.
- vertrouwelijkheid (privacy): informatie alleen toegankelijk is voor bevoegden en onbevoegden vertrouwelijke informatie niet kunnen inzien of aanpassen.
- betrouwbaarheid: informatie juist, volledig, tijdig en de verwerking controleerbaar is
- duurzaamheid: informatie tijdig gearchiveerd wordt zodat ook in de toekomst verantwoording en geschiedschrijving mogelijk blijft (bron: archiefwet)

Het gaat niet alleen over ICT. Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. (Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor een organisatie verricht.) Integriteit en de bescherming van onze informatiestromen gaan hand in hand.
Op dit gebied zijn best practices beschreven. Deze standaarden zijn vastgelegd in normen. De bekendste norm op dit terrein is de ISO 27001/2 norm. De BIO is het normenkader voor de Nederlandse overheid, gebaseerd op de ISO 27001/2 norm.

Wat is de reikwijdte van informatiebeveiliging?

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om:
- alle uitingsvormen van informatie (in woord, beeld of geluid)
- alle mogelijke informatiedragers (op papier of elektronisch)
- alle informatie verwerkende systemen (hardware en software)

Maar vóóral ook om mensen en processen.
Uit onderzoek blijkt dat de meeste incidenten niet voortkomen uit een gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie. Maatregelen op het gebied van informatiebeveiliging beperken zich dan ook niet alleen tot technische maatregelen. Denk bijvoorbeeld aan:
- het invoeren van een 'clean desk'-beleid. Immers, een opgeruimd bureau vermindert de kans dat gevoelige en officiële documenten rondslingeren en daardoor in verkeerde handen terechtkomen.
- het opstellen van regels over de omgang met mobiele devices (laptops, telefoons), om er voor te zorgen dat de informatie die medewerkers bij zich dragen net zo goed beschermd is als die in het stadhuis.
- het geven van aanwijzingen voor telewerken, over bijvoorbeeld het delen van informatie tijdens online vergaderingen.

Waarom formuleren we beleid over informatiebeveiliging?

Met dit beleid willen we uitgangspunten en regels vaststellen op basis waarvan we als gemeente keuzes maken op het gebied van informatiebeveiliging. We baseren ons hierbij op het normenkader van de landelijke Baseline Informatiebeveiliging Overheid (hierna: BIO) omdat dit leidt tot het best passende beleid voor Nijmegen.

Beleidsuitgangspunten met nadere uitwerking
Dit document bevat de beleidsuitgangspunten, die in de Informatiebeveiligingsbeleid Uitwerking 2022 nader zijn uitgewerkt. Ook zijn daar in beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden. De informatiebeveiligingsmaatregelen worden per ISO hoofdstuk verder uitgewerkt in het document Informatiebeveiligingsbeleid Uitwerking 2022, dat tegelijk met dit Informatiebeveiligingsbeleid ambtelijk is vastgesteld. De Informatiebeveiligingsbeleid Uitwerking 2022 omvat tevens het beveiligingsplan voor Suwinet en dat voor waardedocumenten, zoals rijbewijzen en reisdocumenten.

Overlap met privacy
Onderdeel van het informatiebeveiligingsbeleid is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de (kwaliteitshandhaving van de) bedrijfsvoering. Ook voor **privacy** is een dergelijke beheerstructuur van belang. De **overlap** bevindt zich op het vlak van de juiste organisatorische en technische maatregelen ter bescherming van de persoonsgegevens, zoals bedoeld door de Algemene verordening gegevensbescherming (AVG). De beheerstructuren overlappen daarom met elkaar. Voor aanvullingen op het vlak van privacy, wordt verwezen naar het privacybeleid van gemeente Nijmegen zoals vastgesteld door het college van Burgemeester en Wethouders.

Waar willen we naartoe met informatiebeveiliging?

Als vertrekpunt voor de ontwikkeling van informatiebeveiliging binnen de gemeente hebben we onze visie als volgt verwoord:
De komende jaren zet de gemeente Nijmegen in op het verhogen van informatieveiligheid en een verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van de identiteit en democratische rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Door het treffen van technische en organisatorische maatregelen willen we onze informatie beschermen en de kwaliteit waarborgen. We willen ons volwassenheidsniveau als gemeente verhogen en tegelijkertijd voldoen aan wet- en regelgeving rondom informatiebeveiliging.
In ons streven om "in control" te zijn en te blijven leggen we jaarlijks verantwoording af via de 'rapportage Informatiebeveiliging'. 'In control' betekent in dit verband dat we weten welke risico's we lopen, we weloverwogen hier (al dan niet) maatregelen voor treffen en de voortgang daarvan bewaken. Een randvoorwaarde is dat de getroffen maatregelen aantoonbaar bijdragen aan het voldoen aan relevante wet- en regelgeving. Dit betekent onder andere dat verantwoordelijkheden vastgelegd zijn en de naleving (zichtbaar) getoetst wordt. Vastgelegde verantwoordelijkheden moeten bijdragen aan een verhoogd bewustzijn bij medewerkers van hun rollen en taken op het gebied van informatiebeveiliging, zodat zij deze ook waar kunnen maken. Toetsing maakt het mogelijk om lering te trekken uit resultaten en systematisch verbetering tot stand te brengen. Hiermee kunnen ook voor de langere termijn uitspraken gedaan worden over de kwaliteit en de continuïteit van de ICT-omgeving van gemeente Nijmegen.

Wat zijn de pijlers onder ons informatiebeveiligingsbeleid?

Het bestuur en (lijn)management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid (Deze rol wordt nader uitgewerkt in het zogeheten "three lines of defense'-model zoals dat beschreven wordt in de Informatiebeveiligingsbeleid Uitwerking 2022.) Het bestuur weegt bij het nemen van besluiten het goed beschermen van gevoelige informatie zodanig mee dat de privacy van de burger gewaarborgd is. Het management geeft richting aan informatiebeveiliging door het opstellen en handhaven van een informatiebeveiligingsbeleid. Het management laat hiermee zien dat informatiebeveiliging belangrijk is en zij zich hierbij betrokken voelt. Dit beleid is van toepassing op de gehele organisatie: alle processen, organisatieonderdelen, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving.
De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Met de volgende randvoorwaarden:

- Wetgeving waar aan voldaan moet worden bijvoorbeeld op het vlak van registraties van gegevens van inwoners en topografie. Maar ook privacy wetgeving. (Denk bijvoorbeeld aan BRP, SUWI, BSN, BAG/BGT/BRO en PUN, maar ook de archiefwet. En Europese wetgeving zoals de GDPR.)
- We hebben landelijk als basis een gemeenschappelijk normenkader: de Baseline Informatiebeveiliging Overheid (BIO). De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering bij het maken van risico-analyses.
- Daarnaast werken we met de tien bestuurlijke principes voor informatiebeveiliging (opgesteld door de VNG) in aanvulling op de Baseline.

Dit leidt tot de volgende uitgangspunten waar onder dit kader meer over wordt toegelicht:

1. De eindverantwoordelijkheid voor de informatiebeveiliging ligt bij het College van B&W. Het bestuur geeft het goede voorbeeld door te zorgen voor een cultuur waarin iedereen dreigingen kan melden en door verantwoordelijk om te gaan met informatie.
2. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt, samen met het systeem waarin de ontwikkeling en de planning van de maatregelen wordt beheerd (het ISMS), de basis voor een betrouwbare informatievoorziening. De prioriteit in het ISMS wordt oa bijgesteld op basis van risico management.
3. Informatiebeveiliging is een continu verbeterproces dat zich steeds aanpast aan veranderende omstandigheden. De plan-do-check-act-cyclus vormen samen het managementsysteem van informatiebeveiliging.
4. Het sturen en rapporteren over de voortgang en de kwaliteit van de informatiebeveiliging gebeurt op basis van Kritieke Prestatie Indicatoren (KPI`s). Het bestuur neemt dreigingen en risico`s voor informatieveiligheid mee in hun vragen over voorstellen zodat zij deze mee kunnen wegen bij het nemen van beslissingen.
5. We kennen de volgende functies rondom informatiebeveiliging,

- CISO: Chief Information Security Officer, informatiebeveiligingsfunctionaris (gemeentebreed)
- FG: Functionaris Gegevensbescherming (gemeente breed)
- Security Officer Suwinet
- Voor de basisregistratie personen (BRP): beveiligingsbeheerder BRP
- Voor de reisdocumenten: beveiligingsfunctionaris Reisdocumenten
- Voor de rijbewijzen: beveiligingsfunctionaris Rijbewijzen
  In de Uitwerking Informatiebeveiligingsmaatregelen worden deze nader omschreven.

6. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen. Informatiebeveiliging kost geld.
7. Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden getraind in het gebruik van de voor hen relevante procedures.
8. Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken bij de CISO. Informatiebeveiliging is van iedereen.
9. Onze informatiebeveiliging heeft invloed op en wordt ook geraakt door die van onze ketenpartners.
10. Wij registreren onze incidenten en leren daarvan zodat onze ervaringen ons weerbaarder maken.

Informatiebeveiliging met aandacht voor risico`s

- De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in Nijmegen is gebaseerd op risicoanalyse. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets die gebaseerd is op de norm. Als een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. De verantwoordelijke onderzoekt dan hoe kwetsbaar het werkproces is en de dreigingen die kunnen leiden tot een beveiligingsincident. Er wordt rekening gehouden met de beveiligingseisen van de informatie. Alle informatie heeft een classificatie waarmee wordt aangegeven hoe gevoelig de informatie is. Het risico is de kans op beveiligingsincidenten maal de gevolgen daarvan voor het werkproces.
- Bedreigingen kunnen worden gevormd door menselijk falen zoals het niet duidelijk bepalen van verantwoordelijkheid, te kort schietende kennis, gebrekkig bewustzijn van risico`s, een vals gevoel van veiligheid en nadelige prioritering. Een belangrijke factor hierin is de onzekerheid die ontstaat doordat ontwikkelingen in het verleden maar beperkt de digitale toekomst kunnen voorspellen.
- Kwetsbaarheid van het werkproces kan onder andere veroorzaakt worden door het niet controleren op input en/of output, onbekendheid met de classificatie van de gegevens, onduidelijkheid over toegangsrechten, het niet aanwezig zijn van goede procedures.
- Een cultuur waarin wij kunnen leren van incidenten zorgt er voor dat verbeterpunten gevonden worden en de organisatie deze ook aanpakt.

Informatiebeveiliging is van iedereen

Het Informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers van de gemeente. Voor een overzicht van de doelgroepen zie de Uitwerking Informatiebeveiligingsmaatregelen.

Informatiebeveiliging gaat ook over ketenpartners

- Het bereik van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
- Dit informatiebeveiligingsbeleid is een algemene basis. Dit normenkader geldt dus expliciet ook voor de bedrijfsprocessen waar de audits en/of zelfevaluaties DigiD assessment, BAG/BGT inspectie, Suwinet, BRP, reisdocument en rijbewijzen (al dan niet afgedekt door ENSIA) zich op richten.

Informatiebeveiliging in relatie tot privacy

- Met ingang van 2018 heeft gemeente Nijmegen een Functionaris Gegevensbescherming aangesteld. Ook is er een apart privacybeleid opgesteld dat laat zien, binnen de kaders van de AVG, hoe de gemeente Nijmegen onder andere omgaat met de uitwisseling van persoonsgegevens en het gebruik van data.
- Informatiebeveiliging zorgt er voor dat persoonsgegevens en gevoelige data in alle omstandigheden afdoende beschermd zijn.

Informatiebeveiliging wordt ondersteund door architectuur

- Informatiebeveiliging is een basisprincipe van de informatiearchitectuur van gemeente Nijmegen en zal worden 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 applicaties en gegevensverzamelingen aan bepaalde classificatie niveaus heeft gevolgen voor de beschermende maatregelen, maar ook voor de registratie in het verwerkingsregister en de te volgen inzageprocedure.

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 wel 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.

Inwerkingtreding

De inwerkingtreding van het Informatiebeveiligingsbeleid 2022 gemeente Nijmegen is op de dag na publicatie onder gelijktijdige intrekking van Informatiebeveiligingsbeleid 2019 gemeente Nijmegen.

Aldus vastgesteld in de vergadering van 8 februari 2022
De Gemeentesecretaris,
mr. drs. A.H. van Hout
De Burgemeester,
drs. H.M.F. Bruls