Nijmegen

GEMEENTEBLAD

Officiële uitgave van de gemeente Nijmegen

Nr. 270559

7 november 2019

Informatiebeveiligingsbeleid 2019 gemeente Nijmegen

Gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO)
Versiebeheer
Het versiebeheer van dit document ligt bij de CISO.
Kenmerk:
Versie: 1.0
Versiedatum: september 2019
Beheersmaatregel: 5.1.2
Documentnaam: 5.1.2 Informatiebeveiligingsbeleid Uitgangspunten
Gemaakt door:
Portefeuillehouder Burgemeester
Goedgekeurd door: CISO
Classificatie:

Inleiding

Waarom Informatiebeveiliging?
Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie is essentieel voor een gemeente omdat het de basis is voor juist en efficiënt handelen. Gemeente Nijmegen wil zich verantwoordelijk gedragen, aanspreekbaar en servicegericht zijn. Gemeente Nijmegen wil bovenal transparant en proactief verantwoording afleggen aan burgers en raadsleden en met minimale middelen maximale resultaten behalen. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe stringenter de maatregelen die getroffen moeten worden. Waarde van informatie kan bestaan uit de schade die verlies oplevert voor een burger op het moment dat persoonsinformatie niet meer onder controle staat van de gemeente. Maar waarde kan ook bestaan uit de impact van een politiek gevoelig lek, of financieel gewin door voorkennis op inkoop trajecten of speculaties op grond transacties.

Wat is Informatiebeveiliging?
Informatiebeveiliging is de verzamelnaam voor een pakket aan maatregelen, die getroffen worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te garanderen, en te beschermen tegen bedreigingen. De best practices op dit terrein zijn beschreven in de ISO 27001/2 norm. Het begrip ‘informatiebeveiliging’ heeft te maken met:

- beschikbaarheid / continuïteit: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- exclusiviteit / vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- integriteit / betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- duurzaamheid: het zorg dragen voor de tijdige archivering van informatie zodat ook in de toekomst verantwoording en geschiedschrijving mogelijk blijft. Dit aspect komt voort uit de archiefwet.

Reikwijdte en afbakening Informatiebeveiliging
Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, SD kaart, beeldscherm et cetera) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: het implementeren van een clean desk beleid of het opstellen van regels aangaande de omgang met mobiele devices (laptops, telefoons) en het geven van aanwijzingen voor telewerken.

Waarom dit document?
Dit document is een algemene beschrijving van beleid op het vlak van informatiebeveiliging. De uitwerking levert uitgangspunten op en regels die de keuzes van gemeente Nijmegen weergeven op het vlak van informatiebeveiliging. Deze keuzes zijn gebaseerd op de Baseline Informatiebeveiliging

Gemeenten (BIG), die opgevolgd wordt door de Baseline Informatiebeveiliging Overheid (BIO). Zij leiden tot het best passende beleid voor Nijmegen.
In dit document zijn de beleidsuitgangspunten weergegeven. In de uitwerking worden deze verder beschreven. Ook zijn er beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden. 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 (kwaliteits¬handhaving 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 AVG. De beheerstructuren overlappen daarom met elkaar. Voor aanvullingen op het vlak van privacy, zie het geldende Privacy Beleid van gemeente Nijmegen zoals vastgesteld door het college van Burgemeester en Wethouders.

De informatiebeveiligingsmaatregelen worden per ISO hoofdstuk verder uitgewerkt in het document Uitwerking Informatiebeveiligingsmaatregelen, dat tegelijk met het Informatiebeveiligingsbeleid door het GMT is vastgesteld. Dit informatiebeveiligingsbeleid omvat tevens het beveiligingsplan voor Suwinet.

Informatiebeveiligingsbeleid van de gemeente Nijmegen
Het bestuur en (lijn)management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Deze rol wordt nader uitgewerkt in het “3 lines of defense” model zoals dat beschreven wordt in de Uitwerking Informatiebeveiligingsmaatregelen.

Het management geeft een duidelijke richting aan informatiebeveiliging en laat zien dat zij informatiebeveiliging belangrijk vindt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, 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. Hierbij geldt:

- Er is wetgeving waar aan voldaan moet worden, zoals (niet uitputtend) bijvoorbeeld BRP, SUWI, BSN, BAG/BGT/BRO en PUN, maar ook de archiefwet, en Europese wetgeving zoals de GDPR.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), opgevolgd door 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.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:20017) en de BIG/BIO:

1. De rol en verantwoordelijkheid van het College van B&W inclusief de expliciete eindverantwoordelijkheid, worden in de toepasselijke modellen uitgewerkt in bijlage 1.
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 ISMS (Information Security Management System) de basis onder een betrouwbare informatievoorziening. In het ISMS wordt de verbetering van de betrouwbaarheid van de informatievoorziening gemeentebreed benaderd. De planning in het ISMS wordt bijgesteld op basis van nieuwe ontwikkelingen.
3. Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het management systeem van informatiebeveiliging.
4. Het sturen en rapporteren over de voortgang en de kwaliteit van de informatiebeveiliging gebeurt op basis van KPI`s.
5. We kennen de volgende functies in de informatiebeveiliging,

CISO: Chief Information Security Officer, gemeentebreed informatiebeveiligingsfunctionaris
FG: gemeentebreed Functionaris Gegevensbescherming
Voor Suwinet: Security Officer
Voor de BRP: beveiligingsbeheerder BRP
Voor de reisdocumenten: beveiligingsfunctionaris Reisdocumenten
Voor de rijbewijzen: beveiligingsfunctionaris Rijbewijzen
In de Uitwerking Informatiebeveiligingsmaatregelen worden de rollen nader uitgewerkt.

6. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen zoals beschreven wordt in dit beleid.
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 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.

Uitgangspunten informatiebeveiliging

Het belang van informatie(veiligheid)
Informatie is één van de voornaamste bedrijfsmiddelen van Nijmegen. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is de manier waarop we dit realiseren.
Visie
De komende jaren zet de gemeente Nijmegen in op het verhogen van informatieveiligheid en 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 rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is vooral gericht op bescherming van informatie, maar tegelijkertijd maakt het nieuwe manieren van werken mogelijk door kaders te geven voor gefundeerde besluiten over bijvoorbeeld data analyse. Zo zorgt het voor een verantwoorde manier van elektronische dienstverlening. De focus is informatie uitwisselen in alle verschijningsvormen, zowel digitaal, op papier als mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. Integriteit en de bescherming van onze informatiestromen gaan hand in hand.

Doelstelling
Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen, zoals bedoeld in artikel 32 van de AVG, om informatie te beschermen en te waarborgen. Hiermee voldoet de gemeente aan relevante wet- en regelgeving. De gemeente Nijmegen wil haar volwassenheidsniveau verhogen. Zij streeft er naar om “in control” te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen via de Rapportage Informatiebeveiliging. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn, dat er een controleerbare planning is van de maatregelen die nog niet genomen zijn, en die bewaakt moeten worden. De genomen maatregelen dragen aantoonbaar bij aan het voldoen aan de relevante wet- en regelgeving. Aantoonbaar betekent dat verantwoordelijkheden vastgelegd zijn en naleving zichtbaar getoetst wordt. Vastgelegde verantwoordelijkheden gaan gepaard met bewustzijn bij de medewerkers van hun rollen en taken op het vlak 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.

Uitgangspunten
- Het informatiebeveiligingsbeleid van de gemeente Nijmegen is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de BIG/BIO.
- Het beleid sluit aan op het Privacy Beleid van de gemeente Nijmegen.
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College van B&W van de gemeente Nijmegen. Het College van B&W herijkt periodiek het Informatiebeveiligingsbeleid.
- De werking van het Informatiebeveiligingsbeleid wordt getoetst.
- Het College van B&W van de gemeente Nijmegen is volgens de Algemene Verordening Gegevensbescherming de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. Het college ziet hier op toe.

Risicobenadering

- De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in Nijmegen kent een risico gedreven insteek.. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de baseline informatiebeveiliging, die gebaseerd is op de hier boven genoemde ISO 27002 norm. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. De proceseigenaar onderzoekt dan de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident. Er wordt rekening gehouden met de beveiligingseisen van de informatie. Deze eisen blijken uit de classificatie van de informatie op het gebied van beschikbaarheid, integriteit, volledigheid en duurzaamheid. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: risico = kans x impact.
- Bedreigingen worden gevormd door menselijk falen zoals niet expliciet belegde verantwoordelijkheid, te kort schietende kennis, gebrekkig bewustzijn van risico`s, een vals gevoel van veiligheid en nadelige prioritering.
- Kwetsbaarheid van het werkproces kan 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, onduidelijkheid over regie en over normen waaraan voldaan moet worden.

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

Scope
- De scope 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.

Privacy
- Met ingang van 2018 heeft gemeente Nijmegen een Functionaris Gegevensbescherming aangesteld. Ook is er een apart Privacy beleid 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.

Informatiebeveiligingsbeleid en architectuur
- Informatiebeveiliging is onderdeel van de informatiearchitectuur en zal worden uitgewerkt als onderdeel van die architectuur. Deze is gebaseerd op het DIB (Digitaal Informatie Beleid). De architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie)
- 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 dit Informatiebeveiligingsbeleid is op de dag na publicatie in het gemeenteblad. Bij inwerkingtreding van deze beleidsregels vervalt het tot nu toe gehanteerde informatiebeveiligingsbeleid.

Aldus vastgesteld in de vergadering van 5 november 2019
De Gemeentesecretaris,
mr. drs. A.H. van Hout
De Burgemeester,

drs. H.M.F. Bruls