

# Informatiebeveiligingsbeleid 2017-2020

---



# Management samenvatting

## Achtergrond

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties voor gemeenten van groot belang. Uitval van informatiesystemen of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennismaken dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering. Een betrouwbare, beschikbare en correcte informatiehuishouding (integer) is essentieel voor de dienstverlening van gemeenten. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeente en daarmee van de overheid in het algemeen wordt geschaad, wanneer dit onvoldoende op orde is.

In november 2013 is tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de Vereniging van Nederlandse Gemeenten (VNG) de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' bekrachtigd. Deze Resolutie, die is opgesteld door de Vereniging van Nederlandse Gemeenten (VNG) in samenwerking met de Informatiebeveiligingsdienst voor gemeenten (IBD) en de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Dit houdt in dat iedere gemeente het informatiebeveiligingsbeleid vaststelt aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die is opgesteld door de IBD. Tevens zullen gemeenten informatieveiligheid zowel bestuurlijk als ambtelijk borgen en maken ze de invulling op informatieveiligheid transparant voor burgers, bedrijven en ketenpartners.

## Doel

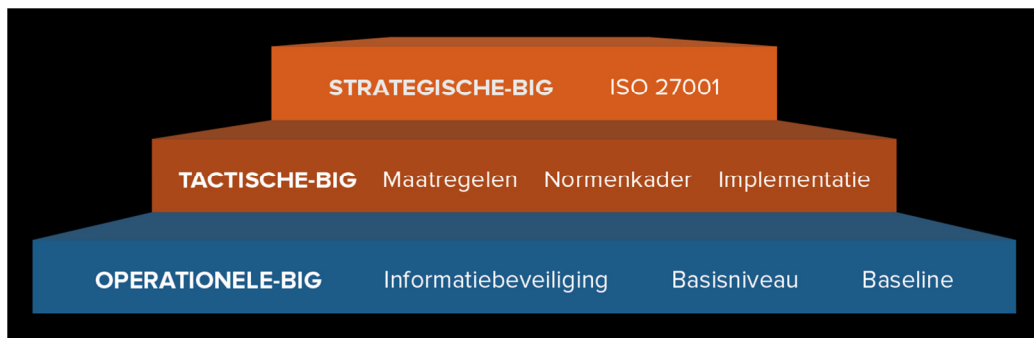
Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten) partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit voortgezet kunnen worden. Het informatiebeveiligingsbeleid wordt minimaal één keer in de 3 jaar geëvalueerd en de rapportage over het functioneren van de informatiebeveiliging wordt conform de P&C cyclus aangeboden aan het DT.

## De Baseline

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De BIG bestaat uit twee delen:

- BIG – Strategische Baseline  
Dit is de “kapstok” of het strategisch beleid waaraan de elementen van de informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente.
- BIG – Tactische Baseline  
Dit beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. Gebaseerd op de beveiligingsnorm ISO/IEC 27002:2007.

Deze twee baselines is de basis voor de informatiebeveiliging binnen onze gemeente.



De BIG bestaat uit 103 Controls (hoofdcategorieën) en 303 maatregelen (sub-categorieën) waaraan moet worden voldaan of wordt uitgelegd waarom de maatregel niet wordt getroffen. Dit is het principe “pas toe of leg uit”. Als voorbeeld wordt in control 9.1.1. (Fysieke beveiliging van de omgeving) gesproken over 24 uur, 7 dagen per week bewaking (maatregel 9.1.1.5) en dat beveiligingspersoneel toezicht houdt (maatregel 9.1.1.7). Bij deze maatregelen zal zeer waarschijnlijk worden uitgelegd dit in onze gemeente anders wordt aangepakt.

# Inhoudsopgave

Management samenvatting .....	2
Achtergrond.....	2
Doel .....	2
De Baseline .....	3
1    Informatiebeleid.....	5
1.1    Doel .....	5
1.2    Scope .....	5
1.3    Uitgangspunten .....	5
1.4    Randvoorwaarden .....	6
1.5    Beveiligingscaterorieën.....	6
2    Hoofdbeveiligingscategorieën.....	7
2.1    Organisatie .....	7
2.2    Beheer van bedrijfsmiddelen .....	7
2.3    Personele beveiliging.....	7
2.4    Fysieke beveiliging.....	8
2.5    Communicatie- en bedieningsprocessen .....	9
2.6    Toegangsbeveiliging .....	9
2.7    Nieuw of onderhoud op informatiesystemen.....	10
2.8    Informatiebeveiligingsincidenten.....	10
2.9    Continuïteitsbeheer.....	10
2.10    Naleving.....	11
3    Slotbepaling.....	12
3.1    Verdere uitwerking.....	12
3.2    Vaststelling .....	12

# 1 Informatiebeleid

Dit informatiebeveiligingsbeleid is gebaseerd op de Strategische Baseline en deze sluit aan bij de organisatie van informatiebeveiliging binnen de Rijksdienst. Dit omdat processen en ondersteunende informatiesystemen door de overheid breed worden gebruikt en daarmee de verankering en verantwoording op eenzelfde manier dient plaats te vinden.

## 1.1 Doel

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij de gemeente. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, maar het is bittere noodzaak geworden.

Op de Buitengewone Algemene Ledenvergadering van de VNG hebben eind november 2013 de gemeenten ingestemd met de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeenten”. Dit is bedoeld om:

- Gemeenten op een vergelijkbare manier efficiënt te laten samenwerken met informatiebeveiliging.
- Gemeenten een hulpmiddel te geven op aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
- De auditlast bij gemeenten te verminderen (ENSIA).
- Gemeenten een aantoonbare betrouwbare partner te laten zijn.

## 1.2 Scope

De scope van dit beleid omvat de bedrijfsvoering processen, onderliggende informatiesystemen, de informatie van de gemeente en het gebruik ervan door de medewerkers in de meest brede zin van het woord. Dit beleid is ook van toepassing op alle ruimten van het gemeentehuis en aanverwante gebouwen, en op de apparatuur die gebruikt worden bij de uitoefening van taken op de diverse locaties. Als informatiesystemen niet fysiek binnen de gemeente (Clouddiensten zoals SAAS, PAAS enz) draaien is dit beleid niet van toepassing. Hiervoor gelden andere richtlijnen, die opgenomen worden in het Cloudcontract of SLA.

## 1.3 Uitgangspunten

- Binnen de gemeente is het College van B&W integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Informatiebeveiliging gaat over informatie in alle verschijningsvormen binnen de organisatie. Het gaat niet alleen over ICT.
- Het beleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten.
- In dit beleid wordt het “Schengen-principe” gehanteerd. Dit houdt in, dat organisatieonderdelen van de overheid elkaar beschouwen als vertrouwd partner en niet als on-vertrouwde buitenwereld. Het gevolg hiervan is dat iedere overheidsorganisatie afzonderlijk zijn omgeving beveiligt en “schoon” houdt en dat anderen hierop kunnen vertrouwen.

- Het beveiligingsniveau is in lagen opgebouwd. Er wordt een basisbeveiligingsniveau vastgesteld. Daar waar bepaalde toepassingen, werkomgevingen of specifieke dreigingen een hogere beveiligingsgraad of specialistische maatregelen vereisen, kunnen extra maatregelen getroffen worden. Deze uitzonderingen worden altijd door het DT bekrachtigd.
- Dit beleid is een integraal onderdeel van de bedrijfsvoering en sluit aan bij de planning- en control-cyclus

## **1.4 Randvoorwaarden**

In dit beleid zijn, voor zover mogelijk gegeven de stand van de techniek, de volgende randvoorwaarden op de beveiliging van de gemeente verwerkt.

- Informatiebeveiliging is en blijft een verantwoordelijkheid van het directieteam en de teammanagers.
- Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement.
- De klassieke informatiebeveiligingsaanpak, waarbij inperking van mogelijkheden de boventoon voert, maakt plaats voor veilig faciliteren.
- De focus verschuift van netwerkbeveiliging naar gegevensbeveiliging.
- Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging.
- Informatiebeveiliging vereist een integrale aanpak.

## **1.5 Beveiligingscaterorieën**

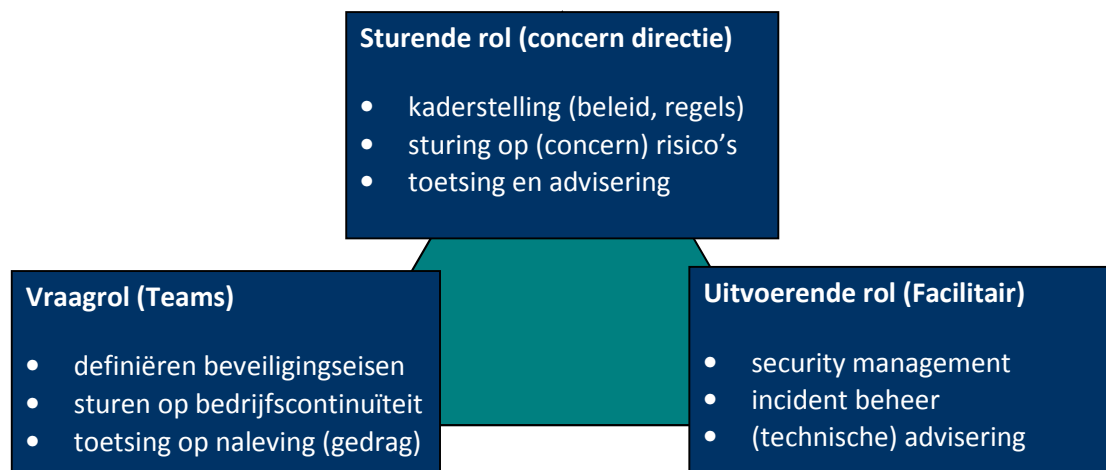
Het informatiebeveiligingsbeleid is opgebouwd conform de BIG en heeft te maken met o.a. de beleidsmakers, personeelszaken, de fysieke beveiliging en de ICT-infrastructuur. In het volgende hoofdstuk worden bovengenoemde onderdelen verder uitgewerkt.

## 2 Hoofdbeveiligingscategorieën

### 2.1 Organisatie

Informatiebeveiliging geldt voor iedereen. Het College van B&W waarborgen dat de doelstellingen worden vastgesteld en het DT en de teammanagers zorgen ervoor dat deze doelstellingen worden uitgevoerd op basis van een expliciete risicoafweging.

De coördinatie van de informatiebeveiliging is belegd bij de Informatiebeveiligingsfunctionaris/Chief Information Security Officer (IBF of CISO) en de privacy aspecten bij de Functionaris Gegevensbescherming (FG). Alle personen (b.v. ambtenaren, inhuurkrachten en leveranciers) die gebruik maken van informatie behoren bewust te zijn dat zij met vertrouwelijke gegevens omgaan. Bewustwordingscampagnes, geheimhoudingsverklaringen, bewerkersovereenkomsten en andere contracten zijn onderdeel van het Informatiebeveiligingsbeleid.



**Figuur 1: relaties**

### 2.2 Beheer van bedrijfsmiddelen

Bedrijfsmiddelen en informatie worden blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik. Voor het bereiken en handhaven van een adequate bescherming van de informatie, worden alle bedrijfsmiddelen (gegevensverzamelingen, hard- en software enz) geïdentificeerd en bijgehouden. Van elk middel is de waarde voor de organisatie, het beschermingsniveau (classificatie) en de verantwoordelijkheid bekend. De gebruikers hebben kennis van de regels en de toegang tot vertrouwelijke informatie kan niet beschikbaar komen voor onbevoegde personen.

### 2.3 Personele beveiliging

Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De verantwoordelijkheden ten aanzien van de informatiebeveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden (b.v. VOG en ambtseed). Alle kandidaten voor een aanstelling, ingehuurd



personeel en externe medewerkers worden gescreend, in het bijzonder voor vertrouwensfuncties. Werknemers, ingehuurd personeel en externe medewerkers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden. Bij wijziging van het dienstverband worden de verantwoordelijkheden opnieuw beoordeeld en zo nodig aangepast. Bij beëindiging van het dienstverband worden de bedrijfsmiddelen geretourneerd en de toegang tot informatie geblokkeerd.

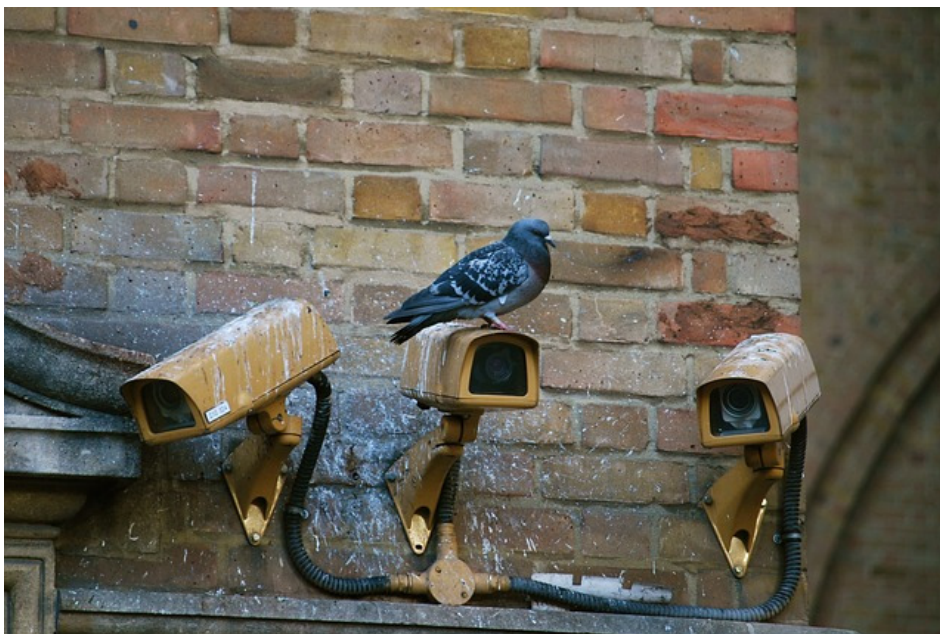
Bij inbreuk op de beveiliging gelden voor medewerkers disciplinaire maatregelen, zoals deze is beschreven in de arbeidsvoorwaardenregeling Rijssen-Holten (ARH). Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

De directie bevordert algehele communicatie en bewustwording rondom informatieveiligheid. De teammanager bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen. In werkoverleggen wordt periodiek aandacht geschonken aan informatieveiligheid.

## **2.4 Fysieke beveiliging**

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, wordt gerealiseerd door de fysieke beveiliging. De gebouwen zijn voorzien van toegangsbeveiliging (met eventuele zonering) en er zijn maatregelen genomen tegen bedreigingen van buitenaf, zoals b.v. brand, storm, blikseminslag en inbraak. De toegangsmiddelen worden geregistreerd en periodiek gecontroleerd op autorisatie. Onderhoud werkzaamheden en bewakingsdiensten worden door gekwalificeerd personeel uitgevoerd.

De apparatuur wordt zo geplaatst dat de risico's van schade en storingen van buitenaf en de gelegenheid voor onbevoegde toegang wordt vermeden. Voor storingen in de nutsvoorziening (b.v. stroomuitval) zijn beschermde maatregelen getroffen. Informatiesystemen voldoen aan de beveiligingseisen die voor kunnen komen bij het verwerken van informatie. Bij beëindiging of hergebruik van het informatiesysteem, wordt door de beheeromgeving de aanwezige data op een veilige methode verwijderd of vernietigd.





## 2.5 Communicatie- en bedieningsprocessen

Voor de correcte en veilige bediening van de ICT-voorzieningen zijn de bedieningsprocedures beschreven. De taken en de verantwoordelijkheden zijn vastgelegd en er wordt functiescheiding toegepast om onbedoelde wijziging of misbruik van de bedrijfsmiddelen te verminderen.

Voor integriteit (juistheid, volledigheid en beschikbaarheid) van de informatiesystemen zijn adequate maatregelen getroffen (b.v. back-up en virusscanner) om storingen tot het minimum te beperken.

Informatie-uitwisseling en opslag (netwerken of via gegevensdragers) gebeurt op een beveiligde manier om deze te beschermen tegen onbevoegde openbaarmaking of misbruik. Medewerkers zijn geïnstrueerd over veilig communiceren en verstrekken van informatie.

Het ontdekken van onbevoegde informatieverwerkingsactiviteiten worden door middel van audit-trail en logging opgespoord. Van de logbestanden worden rapportages gemaakt en worden periodiek beoordeeld. De logbestanden worden beschermd tegen inbreuk en onbevoegde toegang en worden gedurende een overeengekomen periode bewaard.

## 2.6 Toegangsbeveiliging

De toegang tot de informatiesystemen voor de medewerkers en derden worden vastgesteld, gedocumenteerd en beoordeeld op basis wat voor hun taak nodig is (need-to-know, need-to-use). De toegang wordt gerealiseerd door middel van unieke authenticatiegegevens en op basis van risicoafweging wordt gebruik gemaakt van twee-factor authenticatie. Wachtwoorden worden conform het wachtwoordbeleid ingesteld en de toegekende autorisaties worden eens per jaar geëvalueerd.

Kritische informatiesystemen worden door zonering gescheiden en zijn beschermt met adequate middelen (b.v. virusscanner). Onbeheerde en mobiele apparatuur worden passend beschermd om onbevoegde toegang tot informatie te voorkomen.



## 2.7 Nieuw of onderhoud op informatiesystemen

Bij de aanschaf van nieuwe informatiesystemen (of onderhoud hieraan) wordt rekening gehouden met de veiligheidsconsequenties (security by design) en deze voldoen aan de geldende standaarden en bestaande richtlijnen. Invoering of wijziging op het informatiesysteem worden getest en gedocumenteerd volgens vastgesteld procedures (b.v. patchbeleid).

De informatiesystemen beschikken over controle mogelijkheden, waardoor invoer-, transactie- en verwerkingsfouten zijn te detecteren. De informatie in de systemen worden beschermd voor onbevoegd gebruik (achterdeurtjes) en het transport van informatie is versleuteld.

## 2.8 Informatiebeveiligingsincidenten

Informatie kan bewust of onbewust voor onbevoegden toegankelijk zijn gekomen. Voor het rapporteren en registreren van incidenten zijn procedures gemaakt en worden gemeld aan de IBF. Datalekken (wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is) worden behandeld als beveiligingsincidenten en worden aanvullend gemeld bij de FG en bij de Autoriteit Persoonsgegevens. Medewerkers kunnen beveiligingsincidenten eenvoudig melden en zijn verplicht waargenomen of zwakke plekken in de informatiesystemen te melden.

Informatie over de beveiligingsrelevante handelingen (b.v. foute loginpoging) worden regelmatig gecontroleerd en gerapporteerd aan de IBF.

## 2.9 Continuïteitsbeheer

Bedrijfsactiviteiten steunen veelal op informatiesystemen en zijn daardoor gevoelig voor onderbrekingen hiervan. De continuïteitsplannen worden op basis van de risicoanalyse (b.v. BIA) gemaakt, om bij omvangrijke storingen/calamiteit de prioriteit en tijdig herstel van de bedrijfsactiviteiten te bewerkstelligen. De continuïteitsplannen worden jaarlijks getest en aan de hand van de resultaten worden de plannen bijgesteld en de medewerkers bijgeschoold.



## 2.10 Naleving

Bescherming van bedrijfsdocumenten, persoonsgegevens, auteur- en gebruiksrechten vallen onder de verantwoording van het directieteam en de teammanager. De informatiesystemen worden regelmatig gecontroleerd op de naleving van de beveiligingsnormen (b.v. door in- en externe audits en penetratietesten).



## **3 Slotbepaling**

### **3.1 Verdere uitwerking**

Na het vaststellen van dit beleid, wordt verder uitwerking gegeven aan dit beleid door het opstellen van het informatiebeveiligingsplan. In dit plan worden de hoofdbeveiligingscategorieën omgezet in de te nemen maatregelen (conform BIG) en geprioriteerd aan de hand van de risico-analyse (b.v. GAP-analyse).

### **3.2 Vaststelling**

Aldus vastgesteld door het college van burgemeester en wethouders in de vergadering van ...-2017.

De burgemeester

De secretaris

A.C. Hofland

A.C. van Eck