INFORMATIE

BEVEILIGINGSBELEID

DE GEMEENTE DE MARNE

Gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG)

Kenmerk:	
Versie:	1.1
Versiedatum:	4 januari 2017
Gemaakt door:	Heer R. Schoemaker
Portefeuillehouder	Heer F.H. Wiersma
Goedgekeurd door:	
Classificatie:	Definitief

Gemeente De Marne

Colofon

Versiebeheer

Het versiebeheer van dit document ligt bij de informatiebeveiligingsfunctionaris.

Inleiding

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Dit document is het optimum beleid gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG).
In dit document is een aanzienlijk aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden. Onderdeel van dit document 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.

De toegepaste hoofdstukken uit de Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten zijn (het klopt dat hoofdstuk 1 t/m 4 geen onderdeel uitmaken van het beleid):

- 5 Beveiligingsbeleid;
- 6 Organisatie van informatiebeveiliging;
- 7 Beheer van bedrijfsmiddelen;
- 8 Beveiliging van personeel;
- 9 Fysieke beveiliging en beveiliging van de omgeving;
- 10 Beheer van communicatie- en bedieningsprocessen;
- 11 Toegangsbeveiliging;
- 12 Verwerving, ontwikkeling en onderhoud van informatiesystemen;
- 13 Beheer van informatiebeveiligingsincidenten;
- 14 Bedrijfscontinuïteitsbeheer;
- 15 Naleving.

Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijke schade, openbaarmaking of verlies. Het begrip ‘informatiebeveiliging’ heeft betrekking op:

- *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.

Waarom informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor de gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

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 beheren van toegangsrechten van medewerkers hoe om te gaan met beveiligingsincidenten (datalekken) of mobiele apparaten, en aanwijzingen voor telewerken.

Information Security Management System (ISMS)

De Baseline Informatiebeveiliging Gemeenten is opgebouwd uit 11 categorieën (domeinen) met daarin 133 beheersmaatregelen. Er zijn 303 potentiële beveiligingsmaatregelen uitgewerkt. Voor het houden van overzicht over deze maatregelen is door de gemeente Bedum een Information Security Management Systeem (ISMS) ingevoerd, waarmee de maatregelen (fasegewijs) zullen worden ingevoerd. Dit ISMS vormt de basis van de volledige administratieve organisatie rond informatiebeveiliging. Het ISMS wordt afgenomen bij, en actueel gehouden door het bedrijf Segment.

Relatie met privacy

Het onderdeel privacywetging krijgt momenteel extra aandacht vanuit de drie decentralisaties binnen het Sociaal Domein. De aanpak voor wat betreft informatiebeveiliging en privacy hebben overeenkomsten, maar zijn inhoudelijk toch anders. Privacy heeft te maken met welke informatie/gegevens medewerkers of medewerkers van derden mogen gebruiken/combineren bij de uitoefening van hun taak. Voor een groot gedeelte is dit geregeld in materiewetten (zoals de Jeugdwet, de WMO, de Participatiewet, wet BRP). Met de komst van de nieuwe taken op het gebied van het Sociaal Domein komt er informatie naar de gemeenten toe, waarbij het niet zomaar is toegestaan om alle informatiebronnen aan elkaar te koppelen. Veelal is bij wet geregeld welke informatie mag worden gebruikt en in sommige gevallen is er (nog) niets geregeld en moet vooral worden getoetst aan (artikel 8) van de WBP. Omdat nog niet alles is gevangen in wetgeving, moeten gemeenten beleid vaststellen hoe men met het gebruik en de combinatie van privacygevoelige gegevens wil omgaan. Dit privacybeleid is richtinggevend voor het informatiebeveiligingsbeleid.

Privacy gaat over wat.
(inwinnen, gebruiken, uitwisselen, combineren, en bewaren van informatie voor de taakuitoefening)

Informatiebeveiliging gaat over hoe.
(veilig en geautoriseerd inwinnen, gebruiken, uitwisselen, combineren en bewaren van informatie)

Informatiebeveiligingsbeleid van de gemeente De Marne

Het bestuur en management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management 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 management geeft een duidelijke richting aan informatiebeveiliging en laat zien in woord en daad dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele de gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met dit algemene beleid en de relevante landelijke en Europese wet- en regelgeving.
De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend) bijvoorbeeld BRP, SUWI, BSN, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIG:

1. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het **College van B&W als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
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 informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.
4. De organisatiebrede **informatiebeveiligingsfunctionaris** binnen de gemeente De Marne aangeduid als de informatiebeveiligingsfunctionaris - ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
   Daarnaast kennen we deelfuncties in de informatiebeveiliging zoals
   Voor Suwinet: beveiligingsfunctionaris Suwinet
   Voor de BRP: beveiligingsbeheerder BRP
   Voor de reisdocumenten: beveiligingsfunctionaris Waardedocumenten
   Voor de rijbewijzen: beveiligingsfunctionaris Waardedocumenten
5. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
6. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.

7. 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.

Dit Informatiebeveiligingsbeleid treedt in werking na vaststelling door college van College van B&W. Hiermee komt het oude Informatiebeveiligingsbeleid van de gemeente De Marne te vervallen.

Aldus vastgesteld door burgemeester en wethouders van de gemeente De Marne op 1 november 2016,

heer F.H. Wiersma, burgemeester

_____

mevrouw S. Scherstra a.i., secretaris

_____

1 Uitgangspunten informatiebeveiliging

1.1 Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van De Marne. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering en dienstverlening, 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 het proces dat dit belang dient.

Visie

De komende jaren zet de gemeente De Marne 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.[1] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel en iedere medewerker is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en 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.[2]

1.2 Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen, waarmee de gemeente voldoet aan relevante wet en regelgeving. De gemeente De Marne streeft er naar om "in control" te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen via een Verklaring Van Toepasselijkheid. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de Planning & Control cyclus.

1.3 Uitgangspunten

- Het informatiebeveiligingsbeleid van de gemeente De Marne is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.[3]
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) zoals vertaald naar de BIG.
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College van B&W van de gemeente De Marne. Het College van B&W herijkt periodiek het Informatiebeveiligingsbeleid.

[1] *Met betrouwbare informatievoorziening wordt bedoeld dat de volgende zaken geregeld zijn: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.*
[2] *Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor een organisatieverricht.*
[3] *Daarbij geldt het 'comply or explain' principe (pas toe of leg uit)*

- Het College van B&W van de gemeente Bedum is volgens de Wet bescherming persoonsgegevens (Wbp) de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. De informatiebeveiligingsfuctionaris ziet hier op toe.

1.4 Risicobenadering

De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in De Marne is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de baseline. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beveiligingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: **risico = kans x impact**.

1.5 Doelgroepen

Het Informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers van de gemeente:

Doelgroep	Relevantie voor Informatiebeveiligingsbeleid
College van B&W	Integrale verantwoordelijkheid
Directie	Kaderstelling en implementatie
Alle leidinggevenden	Sturing op informatieveiligheid en controle op naleving
Alle medewerkers	Gedrag en naleving
Proces en gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
Directie	Planvorming binnen de informatiebeveiligingskaders
Informatiebeveiligingsfunctionaris	Algemene en dagelijkse coördinatie van de informatiebeveiliging, adviseren over de implementatie van het informatiebeveiligingsbeleid
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
Afdeling I&A BMW	Technische beveiliging
Auditors	Onafhankelijke toetsing van het beleid
Leveranciers en ketenpartners	Compliance aan het beleid

1.6 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 waarin de audtis en/of zelfevaluaties DigiD assessment, BAG inspectie, Suwinet, BRP, reisdocument en rijbewijzen zich op richten.

1.7 Informatiebeveiligingsbeleid en architectuur

Informatiebeveiliging is onderdeel van de informatiearchitectuur en zal worden uitgewerkt als onderdeel van die architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie).[4]

[4] *De processen van informatiebeveiliging worden onderdeel van de volgende GEMMA versie om daarmee de basis voor informatieveiligheid te verankeren als integraal onderdeel van de bedrijfsvoering.*

2 Organisatie van de informatiebeveiliging

2.1 Risico's

Volgens de baseline zijn de te beperken risico's in dit de organisatie van informatiebeveiliging:

- Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, verhindert het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.

2.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Beheren van de informatiebeveiliging binnen de organisatie.
- Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Goedkeuring door het College van B&W en de directie van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

2.3 Beheersmaatregelen

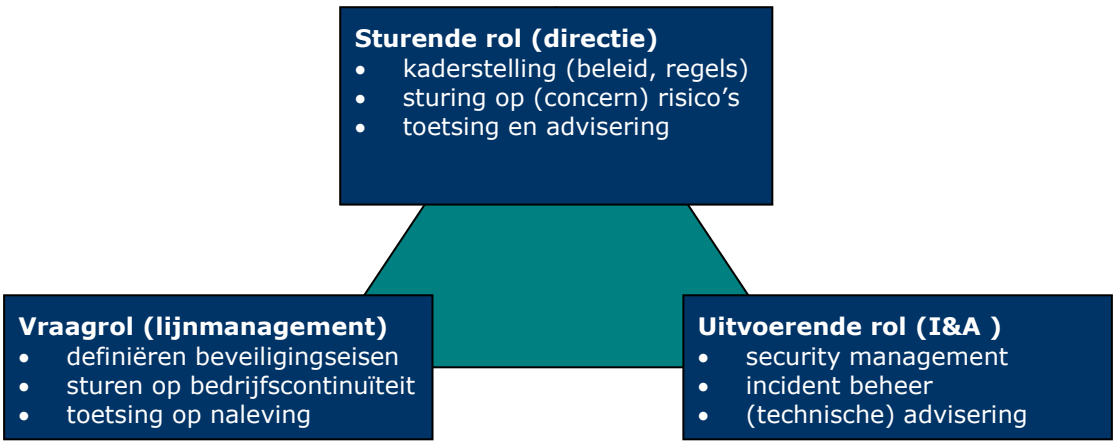
De baseline maakt onderscheid in de volgende beheersmaatregelen voor dit domein:

Beheersmaatregelen voor de interne ambtelijke organisatie

- Het College van B&W van de gemeente De Marne is integraal verantwoordelijk voor de beveiliging (in de beslissende rol) van informatie binnen de werkprocessen van de gemeente.[5]
  Het College van B&W stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;
- De directie (in de sturende rol) is verantwoordelijk voor kaderstelling en sturing.
  De directie:[6]
  - stuurt op concern risico's;
  - controleert de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen;
  - controleert of deze maatregelen voldoende bescherming bieden en;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij.
- De leidinggevenden van de verschillende onderdelen van de organisatieonderdelen zijn in de vragende rol verantwoordelijk voor de integrale beveiliging van hun organisatie onderdeel. [7]
  De leidinggevenden:
  - stellen op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie);
  - zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
  - sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
  - rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.
  - De directie moet het bewustzijn van de medewerkers op het gebied van informatiebeveiliging stimuleren. Dit vindt plaats door het beleid/plan actief uit te dragen in de organisatie.

[5] *Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten*
[6] *Met betrekking tot de i-functie geeft de informatiemanager op dagelijkse basis namens de directie invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.*
[7] *Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten*

- De Facilitaire Dienst is in de uitvoerende rol verantwoordelijk voor de uitvoering van de beveiligingsmaatregelen.[8]
- De gemeentesecretaris De Marne is verantwoordelijk voor:
  - beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
  - is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
  - verzorgt logging, monitoring en rapportage; levert klanten (technisch) beveiligingsadvies.



Figuur 1: relaties

Beheersmaatregelen m.b.t. de taken en rollen

- Het College van B&W stelt formeel het Informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het College als de gemeenteraad (controle functie) kunnen hiervoor opdracht geven om dit te (laten) controleren. De directie adviseert College van B&W formeel over vast te stellen beleid.
- De informatiemanager of een vergelijkbare rol, geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan. De taken m.b.t. informatiebeveiliging die hieruit voortvloeien zijn belegd bij de de informatiebeveiligingsfunctionaris. De informatiebeveiligingsfunctionaris bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert eens per jaar concernbreed aan de directie over de stand van zaken.
- De coördinatie van informatiebeveiliging is belegd bij een strategische adviesfunctie binnen alle organisatie onderdelen. Uitvoerende taken zijn zoveel mogelijk belegd bij (decentrale) beveiligingsfunctionarissen (rollen) zoals beveiligingsfunctionaris Suwinet, beveiligingsbeheerder BRP en beveiligingsfunctionaris Waardedocumenten. Deze beveiligingsfunctionarissen rapporteren aan de informatiebeveiligingsfunctionaris. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de Planning & Control cyclus.
- De Facilitaire Dienst (met name de afdeling I&A BMW) heeft een beveiligingsfunctionaris aangesteld voor dagelijks beheer van technische informatiebeveiligingsaspecten. Deze beveiligingsfunctionaris rapporteert aan de informatiebeveiligingsfunctionaris. Informatiebeveiliging is ingericht naar een PDCA cyclus.
- De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur zijn beschreven en duidelijk en gescheiden zijn belegd. Operationeel beheer, functioneer beheer, technisch beheer, aansturing ICT-leveranciers, autorisatiebeheer en eigenaarschap Suwinet worden belegd.

[8] *Let op, de service organisatie, stafdienst, afdeling bedrijfsvoering is tegelijk ook klant, het gaat hier echter om de uitvoerende rol.*

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
<u>Sturen:</u> Directie dagelijkse uitvoering: Informatiemanager /de informatiebeveiligingsfunctionaris, decentrale functionarissen	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit, pentesten.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie/ College van B&W
<u>Vragen:</u> Alle organisatie onderdelen	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy.	Verbeteren bedrijfscontinuïteit. Rapportage aan informatiemanager/de informatiebeveiligingsfunctionaris.
<u>Uitvoeren</u>: De gemeentesecretaris De Marne en de Facilitaire Dienst	Beleidsvoorbereiding, technische onderzoeken (marktverkenningen).	Leveren van diensten (ICT), incidentbeheer, logging, monitoring en ICT advies.	Vulnerability scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de informatiemanager /de informatiebeveiligingsfunctionaris over aanpassingen aan de informatievoorziening.

<u>Beheersmaatregelen m.b.t. het instellen van De projectgroep Informatiebeveiliging</u>

De informatiebeveiligingsfunctionaris stelt een organisatie voor van informatiebeveiliging gerelateerde functionarissen en organiseert ten minste eenmaal per kwartaal een (informatiebeveiligings) overleg met dit gremium. De informatiebeveiligingsfunctionaris is voorzitter en verder bestaat de projectgroep Informatiebeveiliging in ieder geval uit relevante ICT en personele en fysieke beveiliging experts, en indien nodig zijn inkoop, control en het team Communicatie vertegenwoordigd. Tevens kunnen de diverse decentale beveiligingsfunctionarissen zoals beveiligingsfunctionaris Suwinet, beveiligingsbeheerder BRP en beveiligingsfunctionaris Waardedocumenten worden gevraagd om deel te nemen.
Het overleg heeft binnen de gemeente een adviesfunctie richting de Informatiemanager[9] of gelijkwaardig of rechtstreeks aan de directie en richt zich met name op beleid en adviseert over tactisch/strategische informatiebeveiliging kwesties.
Het onderwerp Informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van de directie zodat er sturing kan plaatsvinden op de uitgevoerde activiteiten). De toegewezen ISMS adviseur van Segment is agendalid en zal op verzoek van de voorzitter een vergadering bijwonen.

<u>Beheersmaatregelen m.b.t. externe partijen</u>

- Informatiebeveiligingsbeleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt).[10] Ook voor externe partijen geldt hierbij het “pas toe of leg uit” beginsel.
- Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV dienen te worden getoetst aan Informatiebeveiligingsbeleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren.[11]
- Voor het tot stand brengen van datakoppelingen met externe partijen, gelden naast dit generiek informatiebeveiligingsbeleid specifieke procedures. Het doel van deze procedures is risicobeheersing. Voor

[9] *Informatiemanager of “gelijkwaardig” kan bijvoorbeeld hoofd ICT, Ondersteuning, Facilitair Bedrijf zijn.*
[10] *Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Nederlandse Gemeenten.*
[11] *Hiervoor kan gebruik worden gemaakt van een ‘third party mededeling’ (TPM), ISO27001 of een ISAE 3402-verklaring.*

externe hosting van data en/of services gelden naast dit generieke informatiebeveiligingsbeleid de richtlijnen voor cloud computing.[12]

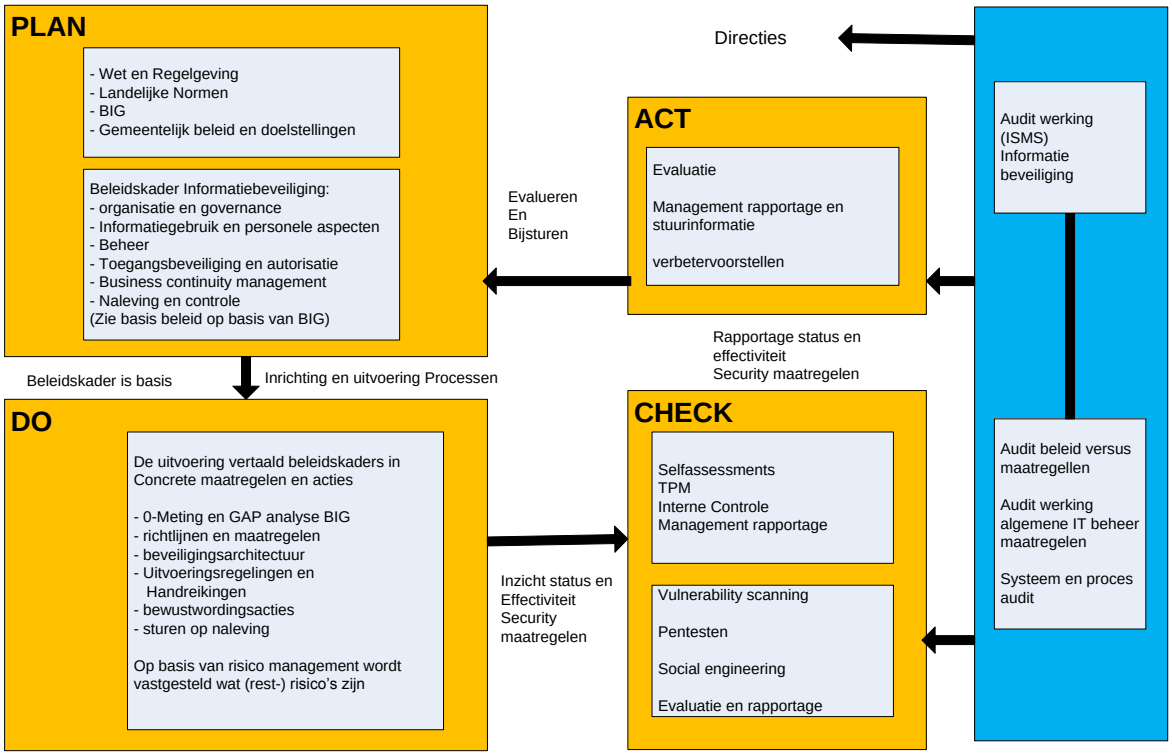
- De gemeente is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door externe partijen;
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens;[13]
  - melding bij de Autoriteit Persoonsgegevens bij uitbesteding van het bewerken van persoonsgegevens en toestemming van de Autoriteit Persoonsgegevens bij doorgifte van persoonsgegevens naar landen buiten de EU.

Beheersmaatregelen m.b.t. ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing is er een crisisteam geïnstalleerd, in ieder geval bestaande uit de burgemeester, en de directie. De werkwijze dient te zijn vastgelegd.
- De gemeente De Marne participeert in allerlei landelijke platforms en is aangesloten bij de Informatie Beveiliging Dienst (= IBD) van KING.

Beheersmaatregelen m.b.t. de PDCA cyclus

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[14] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.



Figuur 2: Information Security Management System

[12] *Zie NCSC: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html*
[13] *Ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen*
[14] *ISO 27001*

Toelichting figuur 2:

- Plan: De cyclus start met Informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de BIG en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het jaarplan en uitgewerkt in het informatiebeveiligingsplan (Informatiebeveiligingsbeleid) van de gemeente. Afdelingsspecifieke activiteiten worden gepland in het afdelingsplan.
- Do: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.
  Externe controle: betreft controle buiten het primaire proces door een auditor.[15] Dit heeft het karakter van een steekproef. Jaarlijks worden diverse onderzoeken uitgevoerd, waarbij de informatiemanager in principe opdrachtgever is. Bevindingen worden gerapporteerd aan de directie.
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan de directie. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

Beheersmaatregelen m.b.t. Suwinet

- Beveiligingsfunctionaris Suwinet beheert en beheerst de beveiligingsprocedures en -maatregelen in het kader van Suwinet zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.
- Beveiligingsfunctionaris Suwinet bevordert en adviseert over de beveiliging van Suwinet en verzorgt rapportages over de status en controleert dat de beveiliging van de Suwinet maatregelen wordt nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.
- Beveiligingsfunctionaris Suwinet rapporteert rechtstreeks aan het hoogste management.
- Het beveiligingsbeleid/plan moet aantoonbaar centraal beschikbaar zijn voor alle gebruikers. Bijvoorbeeld beschikbaar op intranet of op de afdelings-/organisatieschijf. Het uitdragen van het beleid/plan moet niet alleen onder de direct bij de beveiliging betrokken medewerkers plaatsvinden, maar bij alle mensen in de organisatie die Suwinet gebruiken.
- Een adequaat ingerichte organisatie is een belangrijke voorwaarde voor het realiseren van een voldoende beveiligingsniveau voor Suwinet. Het gaat dan met name over functiescheiding. De diverse functies noodzakelijk voor Suwinet moeten schriftelijk zijn vastgelegd, of er een heldere overweging ten grondslag ligt aan de toedeling van taken en of er functiescheiding is toegepast. Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken. Er wordt met name gekeken naar vier gescheiden functies. Beoordeeld wordt of minimaal de volgende functies bij verschillende personen zijn belegd:
  - uitvoering van taken (het gebruik van Suwinet zoals door de klantmanager);
  - beheer van autorisaties (toegang verlenen tot Suwinet, de applicatiebeheerder van Suwinet);
  - kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, bijvoorbeeld de beveiligingsfunctionaris Suwinet);
  - management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet) .

[15] *Van onder meer de IT auditor, de accountant (jaarrekening), rijksoverheid (voor bijv. basisregistraties) en interne auditors*.