ARCHIEF

Informatiebeveiligingsbeleid 2017-2020 Gemeente Heumen

Datum: 17 mei 2017
Versie: 1.0
Status: Gecontroleerd
Steller: Klaas Bolte

17.0003246

Inhoudsopgave

1. Inleiding

De gemeente Heumen is een overheidsorganisatie waarin gewerkt wordt met vertrouwelijke informatie. Mede door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties voor gemeenten van groot belang. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening. Goede informatiebeveiliging is een vereiste om hierin te voorzien.

Onder informatiebeveiliging wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie. Deze informatiebeveiliging is nodig om een goede en veilige dienstverlening naar burgers en bedrijven te garanderen.

Bij het opstellen van het informatiebeveiligingsbeleid is met nadruk rekening gehouden met de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG). De BIG is opgesteld door de Informatiebeveiligingsdienst (IBD) in opdracht van de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De BIG dient als norm voor informatiebeveiliging voor alle Nederlandse gemeenten. De VNG heeft op 15 mei 2013 ingestemd met de implementatie van het normenkader uit de BIG. Daarmee conformeren de gemeenten zich aan de 303 normen uit de BIG. Deze vormen de basis voor het vast te stellen informatiebeveiligingsbeleid (zie ook https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/).

Informatiebeveiliging is geen zaak die alleen de ICT-afdeling aangaat. Een groot deel van beveiligingsnormen zoals ISO 27001 en de BIG gaan over beveiligingsmaatregelen die niet onder verantwoording van ICT liggen, maar op het terrein van bestuur, personeelszaken, burgerzaken, sociale zaken, facilitair en de afdelingshoofden.

Een zorgvuldige informatiebeveiliging vormt ook de basis om te kunnen voldoen aan de verschillende audits, zoals: BRP, PUN (Paspoort Uitvoeringsregeling Nederland, reisdocumenten), BAG, SUWI, DigiD.

2. Doelstelling

Het 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.

Informatie is een belangrijk bedrijfsmiddel dat de gemeente op gepaste wijze beschermt. Daarom is het volgende doel gesteld ten opzichte van informatiebeveiliging:

De gemeente Heumen wil ***een betrouwbare partner*** zijn voor burgers, bedrijven en ketenpartners.

Dit doel wordt bereikt door een passende set van maatregelen te treffen om risico's af te dekken en om, in het geval van incidenten, de eventuele gevolgschade (impact) van deze incidenten te beperken. Deze maatregelen staan beschreven in het informatiebeveiligingsplan[1] (zie hoofdstuk 6).

[1] Het informatiebeveiligingsplan is een nadere uitwerking van maatregelen t.b.v. implementatie BIG. Deze dient jaarlijks opnieuw te worden opgesteld om de nieuwe set aan te nemen maatregelen vast te stellen en hierop te kunnen sturen.

3. Uitgangspunten

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

1. Alle 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 in het document 'Informatiebeveiligingsorganisatie gemeente Heumen'.

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 **informatiebeveiligingsfunctionaris**/Chief Information Security Officer (CISO) ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.

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.

3.1. Randvoorwaarden

De gemeenteraad (op voorstel vanuit het college) zal, met afweging van de kosten, risico's en baten, voldoende middelen beschikbaar stellen om informatiebeveiliging binnen de gehele organisatie te implementeren en de diverse initiatieven uit het IB-programma uit te laten voeren.

Adequate informatiebeveiliging vereist de betrokkenheid en ondersteuning van het gehele personeel (inclusief externe en tijdelijke medewerkers). Daarom worden jaarlijks de verantwoordelijkheden op het gebied van informatiebeveiliging met alle medewerkers besproken. En daar waar nodig worden medewerkers geïnformeerd en opgeleid.

Om onze informatiebeveiliging af te stemmen op interne en externe ontwikkelingen wordt tweejaarlijks een risico-analyse uitgevoerd. Of zodra wijzigingen in de omgeving, technische wijzigingen of dreigingsveranderingen hier aanleiding toe geven.

Om ervoor te zorgen dat onze informatiebeveiliging 'in control' is en blijft, zal informatiebeveiliging worden opgenomen in de Planning en Control (PDCA) cyclus. Concerncontrol toetst in dat kader of de vastgestelde beveiligingsmaatregelen worden nageleefd.

4. Scope van het informatiebeveiligingsbeleid

4.1. Subjecten van het informatiebeveiligingsbeleid

Informatiebeveiliging en daarmee ook dit informatiebeveiligingsbeleid geldt voor alle personeelsleden in dienst van de gemeente Heumen en alle externe krachten die tijdelijk of voor onbepaalde duur bij de gemeente werkzaam zijn of voor de gemeente werkzaamheden verrichten (bijv. onderaannemers, consultants, leveranciers, e.d.).

Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan de gemeente Heumen eigenaar of beheerder is, dient informatiebeveiliging onderdeel te zijn van de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente Heumen. Bijzondere aandacht is er voor de GR ICT Rijk van Nijmegen (iRvN) waarbij de iRvN taken voor de gemeente uitvoert.

4.2. Objecten van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is van toepassing op:

- de ICT-infrastructuur (netwerk- en server hardware)
- voorzieningen voor (data)communicatie
- software
- gegevens (data), evenals processen waarin gegevens worden verwerkt / bewerkt
- gegevensdragers (zoals laptops, USB-sticks maar bv. ook fysieke mappen met documenten)
- systeem- en applicatiedocumentatie
- werkplekken (zowel werkplekken op gemeentelijke locaties als thuiswerkplekken of andere externe werkplekken)
- gebouwen van de gemeente Heumen
- het personeel.

Het informatiebeveiligingsbeleid richt dus zich niet alleen op de geautomatiseerde gegevensverwerking door middel van ICT-voorzieningen, maar uitdrukkelijk ook op de bescherming van niet geautomatiseerde gegevens (zoals fysieke documenten) en bedrijfseigendommen.

Het informatiebeveiligingsbeleid geldt voor alle informatie, hetzij mondeling, hetzij geschreven, geprint of elektronisch opgeslagen, die eigendom is van, in bewaring is bij of gebruikt wordt door welk gedeelte van de gemeente Heumen dan ook. Het informatiebeveiligingsbeleid geldt ook voor alle (tijdelijke) dragers gebruikt in het creëren, verwerken, versturen, sorteren, gebruiken of controleren van gegevens en informatie.

Het informatiebeveiligingsbeleid is locatieonafhankelijk. Indien een medewerker, zakelijke relatie of leverancier of derde zich op een locatie bevindt buiten het gemeentehuis, maar wel met informatie of informatievoorziening (denk aan onderhoud in het veld, thuiswerken en/of webmail) van de gemeente werkt, is het beleid ook van toepassing.

4.3. Risico's

Zonder beveiligde informatie kan de gemeente Heumen bloot staan aan imagoschade en financiële schade. De risicobronnen waar de informatie en informatievoorziening aan zijn blootgesteld komen voort uit:

- de door de organisatie gewenste en gebruikte functionaliteit;
- de gebruikers van de informatiesystemen;
- de kwetsbaarheden van de ICT-infrastructuur;
- moedwillige kwaadwillende acties door eigen personeel of derden (bijvoorbeeld inbraak, ongeoorloofd gebruik, vernieling)
- externe oorzaken (natuurgeweld, maar ook technische calamiteiten zoals brand en lekkage).

De risico's worden in kaart gebracht in een risico- en impactanalyse en maken deel uit van het informatiebeveiligingsplan (zie hoofdstuk 6).

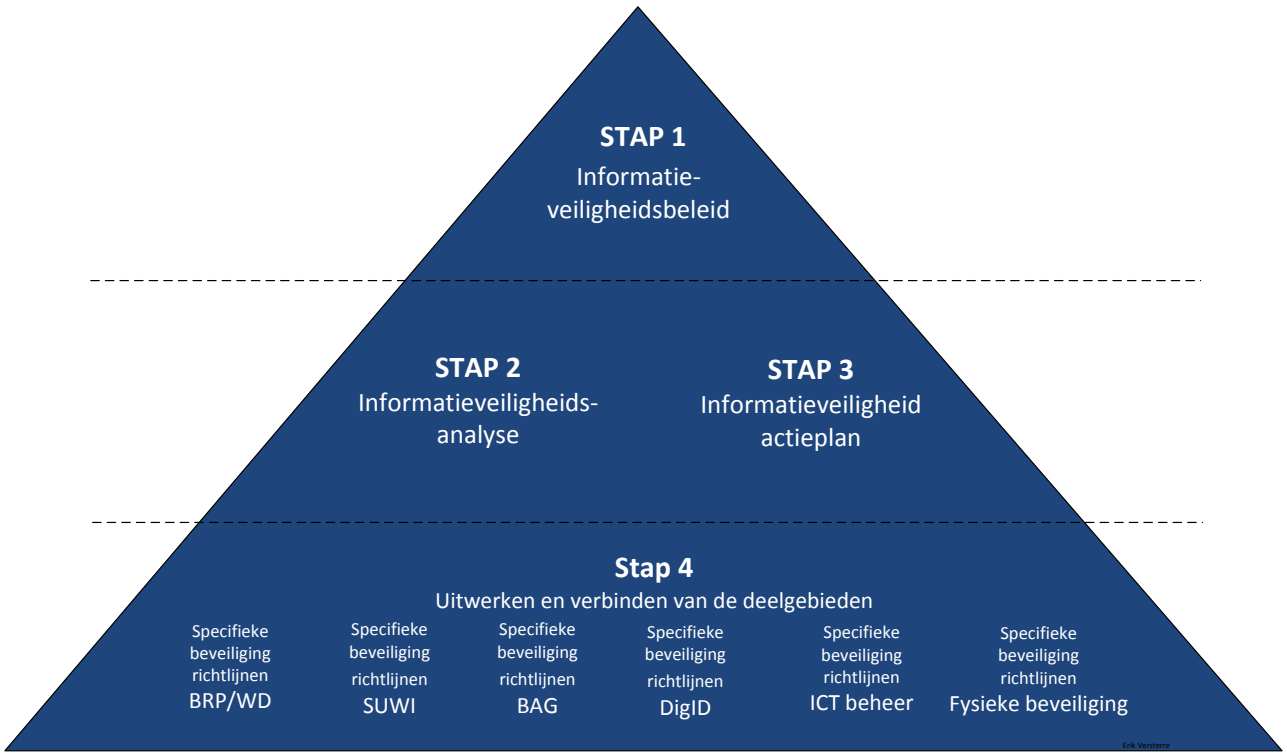
4.4. De informatieveiligheidspiramide

Om de scope van dit document verder te verduidelijken, is in figuur 1 aangegeven welke niveaus van informatieveiligheid zijn te onderkennen.

Bovenaan de piramide treffen we het informatiebeveiligingsbeleid aan. Dit is het organisatiebrede beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar. Het informatieveiligheidsbeleid is zodanig opgezet dat praktijksituaties eenvoudig kunnen worden opgezet of hieraan worden getoetst.

De tweede laag van de piramide is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een risico-inventarisatie en evaluatie (RI&E). Tijdens deze RI&E worden de uitgangspunten in het gemeentebrede informatieveiligheidsbeleid getoetst met de praktijksituatie. Hier worden niet alleen de 'harde aspecten' onderzocht. Dat wil zeggen de techniek, de regels en de procedures. Maar worden ook de 'zachte aspecten' meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie. Na de risico-inventarisatie vindt risicoweging en prioritering plaats. Tijdens deze stap worden de geconstateerde risico's gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van risico's en te treffen maatregelen.

Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals de BRP, de BAG of het financiële systeem, maar kan ook gericht zijn op de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.



Figuur 1: De informatieveiligheidspiramide

5. Kwaliteit en belang van informatiebeveiliging

De kwaliteit van de informatievoorziening is uit te drukken in termen van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid:

1. ***Beschikbaarheid*** betekent dat informatie(systemen) beschikbaar zijn op de juiste momenten. Hierdoor hebben burgers, bedrijven en organisaties toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en hun dienstverlening richting de burgers, bedrijven en organisaties ongestoord uit te kunnen voeren.

   De informatiesystemen moeten voldoen aan een beschikbaarheid tijdens kantoortijd van minimaal 95%. Buiten kantoortijd zijn er geen beschikbaarheidseisen met uitzondering van voorzieningen in het kader van rampenbestrijding. In het geval van uitval van bedrijfsprocessen en/of informatiesystemen ten gevolge van een calamiteit dient de dienstverlening binnen 48 uur hersteld te zijn.

2. ***Integriteit*** betekent het waarborgen van de correctheid en de volledigheid van de informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het van belang dat de correcte informatie tijdig aanwezig is in de systemen.

3. ***Vertrouwelijkheid*** betekent dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Voor de gemeente is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens van burgers en gegevens van bedrijven alleen toegankelijk is voor bevoegden. Of een persoon bevoegd is, bepaalt de taak en verantwoordelijkheid of functieomschrijving van de betreffende persoon.

4. ***Controleerbaarheid*** betekent het gemak waarmee de volledigheid en correctheid van informatie is te controleren, zelfs na een bepaalde periode. De verantwoordelijke personen en afdelingen treffen maatregelen, zodat op ieder gewenst moment en periodiek de gegevens in de informatiesystemen zijn te controleren. Deze controle kan bestaan uit een intern of extern onderzoek.

6. Informatiebeveiligingsplan

Voor het uitvoeren van het informatiebeveiligingsbeleid is een informatiebeveiligingsplan vereist.
Als onderdeel van het informatiebeveiligingsplan 2015 is een GAP- en risicoanalyse uitgevoerd. Op basis van de risicoanalyse zijn maatregelen geselecteerd en geïmplementeerd uit de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)[2]. Dit jaar zal er opnieuw een GAP- en risicoanalyse moeten plaatsvinden. De maatregelen die hieruit voortkomen moet de gemeente op basis van het risicoprofiel (de dreigingen, kwetsbaarheden en impact op de organisatie) met prioriteit implementeren[3].

Het normenkader voor de maatregelen staat benoemd in de tactische BIG. In het informatiebeveiligingsplan staat wat de maatregel inhoudt, op welke manier, door wie en wanneer de maatregel wordt ingevoerd. Het informatiebeveiligingsplan wordt één keer per jaar herijkt en vastgesteld door het MT.

De BIG is opgesteld op basis van een algemeen risicoprofiel over alle gemeenten en richt zich niet op alle voor de gemeente Heumen relevante risicobronnen en de gevolgen. Het kan zijn dat een informatiesysteem of bedrijfsproces meer beveiligingsmaatregelen nodig heeft dan in de BIG staan beschreven. Bijvoorbeeld de maatregelen die specifiek voor het sociaal domein en burgerzaken vereist zijn. Om vast te stellen of voor een informatiesysteem of bedrijfsproces meer beveiligingsmaatregelen gewenst zijn, wordt een dataclassificatie uitgevoerd voor informatiesystemen en bedrijfsprocessen. Vanuit het resultaat van een dataclassificatie, worden de maatregelen vastgesteld en opgenomen in de PDCA-cyclus van informatiebeveiliging. De PDCA-cyclus wordt nader toegelicht en uitgewerkt in het informatiebeveiligingsplan.

[2] Tactische BIG: https://www.ibdgemeenten.nl/wp-content/uploads/2015/07/15-0727-Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.01.pdf

[3] Dit komt terug in het informatiebeveiligingsplan 2017 Gemeente Heumen

7. Organisatie van informatiebeveiliging

De informatiebeveiligingsorganisatie beschrijft de verantwoordelijkheden, taken en bevoegdheden die met betrekking tot informatiebeveiliging per functie of rol verankerd zijn.

De inrichting van de informatiebeveiligingsorganisatie wordt beschreven in het document 'informatiebeveiligingsorganisatie gemeente Heumen'.

8. Relevante Wet- en regelgeving

Er zijn wettelijke eisen gesteld aan de beveiliging van gegevens en informatiesystemen. Voorbeelden hiervan zijn te vinden in:

- de ***Wet Bescherming Persoonsgegevens (Wbp)*** gaat in op de bescherming van persoonsgegevens in gestructureerde gegevensverwerkingen. De gemeente dient volgens deze wet ervoor zorg te dragen dat persoonsgegevens van burgers, bedrijven, medewerkers, leveranciers en overige belanghebbenden worden beschermd tegen onrechtmatige verwerking van of onbevoegde toegang tot deze gegevens.
- de ***Wet Computercriminaliteit II***. Deze wet gaat in op computergerelateerde strafbare handelingen. De gemeente dient door middel van adequate informatiebeveiligingsmaatregelen ervoor te zorgen dat deze wet door medewerkers van de gemeente Heumen of door derden waarvoor de gemeente verantwoordelijk is niet wordt overtreden.
- ***Burgerlijk Wetboek***, de ***Telecommunicatiewet***, de ***Auteurswet***, de ***Wet op de Jaarrekening***, de ***Archiefwet*** en het ***Wetboek van Strafvordering***, etc. Deze bevatten in het algemeen een resultaatverplichting tot een passend niveau van informatiebeveiliging.

De BIG is een afgeleide van de Code voor Informatiebeveiliging (NEN/ISO 27002). Deze code bevat elf categorieën waarop informatiebeveiliging betrekking heeft. Deze categorieën zijn:

1. Beveiligingsbeleid
2. Organisatie van informatiebeveiliging
3. Classificatiebeheer van bedrijfsmiddelen
4. Personele beveiligingseisen
5. Fysieke- en omgevingsbeveiliging
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen
9. Incidentmanagement
10. Bedrijfscontinuïteitsmanagement
11. Naleving

De onderwerpen in de BIG zijn gebaseerd op de indeling van de NEN/ISO-normering voor informatiebeveiliging (NEN/ISO-27001 en -27002). Aangevuld met de specifieke wetgeving/regels binnen thema's als:

- BRP (Basisregistratie persoonsgegevens)
- BAG (Basisregistraties Adressen en Gebouwen)
- WOZ (Basisregistratie Waardering Onroerende Zaken)
- BGT (Basisregistratie Grootschalige Topografie)
- SUWI (wet Structuur Uitvoering Werk en Inkomen)
- Participatiewet, Wmo en Jeugdwet
- DigiD (Digitale Identiteit bij de overheid)
- PUN (Paspoort Uitvoeringsregeling Nederland)
- Wbp (Wet bescherming persoonsgegevens) waaronder de Wet meldplicht datalekken
- Archiefwet
- Wet algemene bepalingen omgevingsrecht (Wabo), Wet Ruimtelijke Ordening (WRO) etc.

Deze categorieën en regels per thema komen terug in de toe te wijzen rollen binnen de informatiebeveiligingsorganisatie van Heumen.

9. Werking en geldigheidsduur

Het informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van B&W. Na deze vaststelling komt enig voorgaand informatiebeveiligingsbeleid van de gemeente Heumen te vervallen.

Daarnaast evalueert en beoordeelt de CISO het informatiebeveiligingsbeleid om de 4 jaar op relevantie en actualiteit. Indien noodzakelijk stelt de CISO het document voortijdig bij en laat het vaststellen door het college van B&W.

Het informatiebeveiligingsplan (hoofdstuk 6) wordt één keer per jaar herijkt door de CISO en vastgesteld door het MT. De informatiebeveiligingsorganisatie (hoofdstuk 7) wordt herijkt door de CISO wanneer vereist en vastgesteld door het MT.