Strategisch Informatiebeveiligingsbeleid gemeente Heumen 2020 - 2023

Datum: mei 2020
Auteur: Jos Baan
Status: Definitief

Inhoudsopgave

Managementsamenvatting

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 – 2023. Met dit ‘strategisch Informatiebeveiligingsbeleid 2020-2023’ zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en door te gaan met de stappen die in de voorgaande jaren zijn gezet. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen met als doel om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere gevoelige informatie te waarborgen binnen de organisatie. Het is de primaire verantwoordelijkheid van de afdelingshoofden om de eigen processen, systemen en gegevens te beveiligen en hier voldoende middelen voor beschikbaar te stellen. En de benodigde maatregelen uit het jaarplan uit te voeren. De CISO adviseert, coördineert en ondersteunt hierbij. Op dit moment is er sprake van twee vastgestelde functies een CISO en een ISO; er wordt onderzocht of taken en verantwoordelijkheden samengevoegd en of anders belegd gaan worden.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de gehele levenscyclus van informatiesystemen. Het beperkt zich echter niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, inwoners, gasten/bezoekers en externe relaties.

Informatie is een belangrijk bedrijfsmiddel. Beveiliging van deze informatie is nodig om een goede en veilige dienstverlening naar burgers, bedrijven en ketenpartners te garanderen. Daarom is het volgende algemene doel gesteld voor de informatiebeveiliging:

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

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico’s van menselijk gedrag.
- Het voorkomen van ongeautoriseerde (fysieke) toegang.
- Het beheersen van de toegang tot informatiesystemen.
- Het garanderen van betrouwbare en veilige informatievoorzieningen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.
- Het waarborgen van de naleving van dit beleid.

De gemeente zet de komende jaren in op het optimaliseren van de informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie.

[Waar relevant is in dit document met rechte haken [] een verwijzing naar de BIO opgenomen. Dit betekent echter niet dat in alle gevallen de volledige maatregel door de implementatie van dit beleid wordt afgedekt.]

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 - 2023. Deze vervangt het in 2017 vastgestelde ‘Gemeentelijk Informatiebeveiligingsbeleid 2017-2021’. Dit laatste beleid was nog gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De BIG wordt per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIO vormt de basis voor dit strategische beleid.

Doelstelling:
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid.

Resultaat:
Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

Met dit ‘Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023’ zet de gemeente Heumen een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te borduren op stappen die in de voorgaande jaren gezet zijn. Deze nota is richtinggevend en kader stellend en wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

1.1 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het zorgen voor een bewust en veilig omgaan met informatie door het toepassen van een combinatie van organisatorische en technische maatregelen. Deze maatregelen zijn er op gericht de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens aantoonbaar te beschermen tegen al dan niet opzettelijk onheil.

De maatregelen borgen de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid en in het geval van incidenten de eventuele gevolgschade (impact) van deze incidenten te beperken. Hoe vertrouwelijker informatie is, hoe meer maatregelen er getroffen moeten worden.

Bij het organiseren van informatiebeveiliging moeten de gemeenten voldoen aan de relevante wet- en regelgeving. Daarbij zal zoveel als mogelijk een goede balans gevonden moeten worden met het faciliteren van een optimale bedrijfsvoering en het bereiken van de dienstverleningsambities van de gemeenten.

Kernpunten van informatiebeveiliging zijn:

- Beschikbaarheid (of continuïteit): het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid (juistheid), volledigheid, tijdigheid van informatie en informatieverwerking oftewel het in overeenstemming zijn van informatie met de werkelijkheid;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe bevoegd en geautoriseerd zijn.
- Controleerbaarheid: waarborgen dat de beoogde toegang tot gegevens en de juiste werking van systemen continu alsook achteraf te controleren is.

1.2 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn en hoe verantwoording op informatiebeveiliging plaatsvindt. In hoofdstuk 4 wordt specifiek aandacht besteed aan het belang van kennis en bewustwording m.b.t. informatiebeveiliging.

2. Strategisch beleid

2.1 Ambitie en visie van de gemeente

De hoofddoelstelling van dit informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente. Er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en middelen aangegeven waarmee dit beleid moet worden vormgegeven.

Informatie is een belangrijk bedrijfsmiddel dat de gemeente Heumen op gepaste wijze willen beschermen. Daarom is het volgende doel gesteld voor informatiebeveiliging:

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

De gemeente zet daarom de komende jaren in op het optimaliseren van de informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie.

2.2 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is de norm NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en de norm NEN-ISO/IEC 27002:2017 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[1] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze normen zijn opgenomen in de lijst met verplichte standaarden voor de publieke sector van het Forum Standaardisatie. De gemeente volgt de standaarden uit de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie. Bij de aanbesteding van nieuwe producten of diensten of het verlengen van bestaande producten of diensten worden de relevante open standaarden uit de lijst van het Forum Standaardisatie uitgevraagd.
De BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Afhankelijk van uit te voeren risicoanalyses moeten de directie en het management per onderdeel uit de BIO kiezen voor bepaalde niveaus van beveiligen met bijbehorende maatregelen.

2.3 Scope van het strategisch informatiebeveiligingsbeleid

Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen:

- Autorisatiebeleid;
- ICT ontwerp(en);
- Beleid leveranciers/externe partijen;
- Bedrijfsprocessen;
- Beheerrichtlijnen ICT;
- Configuratiebeheer;
- Continuïteitsbeheer;
- Interne controle;
- Fysieke beveiliging (beveiliging die met behulp van fysieke middelen gerealiseerd wordt);
- Gedragsregels;
- HR proces;
- Incidentenbeheer;
- Loggingbeleid;
- Wijzigingsproces.

De uitwerking van het beleid in concrete te nemen maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP)[2]. [18.2.1.1] Dit strategische beleid moet volgens de BIO-eisen minimaal om de 3 jaar opnieuw worden beoordeeld en zo nodig worden bijgesteld. [5.1.2.1]

---

[1] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

[2] Het informatiebeveiligingsplan is een nadere (jaarlijkse) uitwerking van te nemen maatregelen. Het informatiebeveiligingsplan is tevens de basis voor het inrichten van een procesgerichte benadering van informatiebeveiliging, ook wel het Information Security Management System (ISMS) genaamd. Dit proces hanteert een Plan Do Check Act Cyclus (PDCA) en moet aansluiten bij de Planning en Control (P&C) Cyclus van de gemeente. Centraal binnen deze PDCA cyclus staat het opstellen, uitvoeren, evalueren en bijstellen van het jaarlijkse informatiebeveiligingsplan.

2.3.1 Overige normenkaders

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis. Vanuit domeinwetgeving kunnen aanvullende eisen worden gesteld. Deze worden in aanvullende beleidsdocumenten geformuleerd. Dit geldt o.a. voor de Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Basisregistratie Personen (BRP) en Waardedocumenten (WD), de beveiligingsnorm DigiD of de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO).

Bewust wordt in dit beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar dit strategisch beleid gelegd.

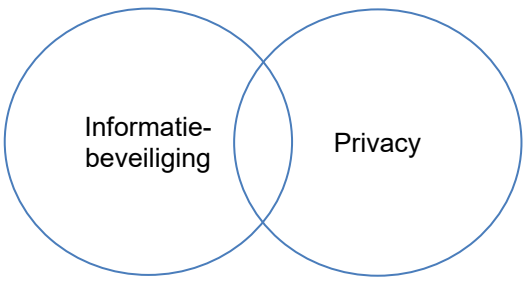
2.3.2 Ketenpartners/externen

De gemeente neemt deel aan verschillende samenwerkingsverbanden zoals het Werkbedrijf Rijk van Nijmegen (WBRN) voor de uitvoering van de Participatiewet en het samenwerkingsverband Instituut Bijzonder Onderzoek (IBO) voor de fraude handhaving bij uitkeringen en de Omgeving Dienst Rijk van Nijmegen (ODRN) als uitvoeringsorganisatie voor vergunningen, toezicht en handhaving voor bouw en milieu. Bij deze samenwerkingen is sprake van uitwisseling van informatie, waarvan de gemeente eigenaar of beheerder is. Informatiebeveiliging dient onderdeel te zijn van een samenwerkingsovereenkomst en deze mag niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente. Externe partijen moeten een zelfde beveiligingsniveau hanteren zoals opgenomen in dit beleid, zij moeten tevens aan kunnen tonen dat zij voldoen aan dit niveau van beveiliging. Bijzondere aandacht is er voor de Gemeenschappelijke Regeling ICT Rijk van Nijmegen (iRvN) waarbij de iRvN de ICT (automatisering) voor de gemeente uitvoert. Vanuit die hoedanigheid is iRvN verantwoordelijk voor een groot gedeelte van de tactische en operationele informatiebeveiligingsrichtlijnen en -maatregelen. Onderstaande richtlijnen en maatregelen zijn door iRvN begin 2020 vastgesteld en gelden ook voor gemeente Heumen:

- Beschermingen tegen bedreigingen van buitenaf 2020;
- Procedure wijzigingsbeheer 2020;
- Scheiding van faciliteiten voor OTP 2020;
- Capaciteitsbeheer;
- Systeemacceptatie 2020;
- Maatregelen tegen virussen;
- Procedure back-up iRvN;
- Procedure restore iRvN;
- Maatregelen voor netwerken;
- Aanmaken audit-logbestanden;
- Scheiding van netwerken;
- Security incident management;
- Exit protocol uitdiensttreding.

2.3.3 Relatie met privacy

Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacy zijn echter twee verschillende begrippen. Ze hebben wel een gemeenschappelijk raakvlak.



Informatiebeveiliging heeft een bredere scope dan de bescherming van enkel persoonsgegevens (gegevens privacy[3]). Informatiebeveiliging draait om de bescherming van alle gevoelige informatie tegen

[3] Gegevens privacy is één van de verschillende soorten privacy. Andere soorten zijn: lichamelijke privacy, huiselijke privacy en

aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn.

Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywet. Artikel 32 van de AVG schrijft voor dat:

> *"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen".*

Informatiebeveiliging maakt daarmee een onderdeel uit van de AVG. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Wel geeft de AVG voorbeelden van mogelijke risico's en maatregelen. Normenkaders als de BIO helpen de gemeente om de risico's goed in te schatten en de benodigde maatregelen te treffen. Hoe de gemeente omgaat met privacy en de AVG is beschreven in het privacybeleid van de gemeente Heumen.

2.4. Ontwikkelingen

2.4.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is per 2020 het nieuwe normenkader voor de gehele overheid. Het jaar 2019 gold als overgangsjaar om over te stappen van BIG naar BIO. De werkwijze van de BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de afdelingshoofden nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid. De BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Afhankelijk van de inschatting van het risico (risicoanalyse), zal het management op generiek of proces niveau een beveiligingsniveau moeten bepalen.

2.4.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO[4] en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

---

communicatie privacy.

[4] Deze principes worden tegelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG): https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

2.4.3 Maatschappelijke- en technologische ontwikkelingen

De ontwikkelingen in de samenleving en technologie maken dat informatiebeveiliging steeds belangrijker wordt. Onze inwoners en bedrijven willen snel en digitaal geholpen worden. De markt laat een verschuiving zien van in huis geïnstalleerde applicaties naar extern gehoste Software as a Service (SaaS) oplossingen. Dataverwerking is meer en meer “in de cloud”, dat wil zeggen bij andere organisaties op de servers die op onbekende plaatsen staan. Er is een ontwikkeling naar tijd en plaats onafhankelijk werken, en het gebruik van meer mobiele apparaten (smartphone, laptop, tablet). Er worden veel meer gegevens gedeeld in ketens. Bijvoorbeeld in het sociaal domein en het ruimtelijke domein (Omgevingswet en Digitaal Stelsel Omgevingswet). En tegelijkertijd is er een roep om het beter beschermen van persoonsgegevens. De externe dreigingen zoals hacks, ransomware en phishing nemen sterk toe.

2.4.4 Belangrijkste risico’s informatiebeveiliging

Het Dreigingsbeeld 2019/2020 Informatiebeveiliging Nederlandse Gemeenten van de Informatiebeveiligingsdienst (IBD)[5] geeft de belangrijkste risico’s weer waar het vakgebied informatiebeveiliging last van heeft. Het dreigingsbeeld richt zich op de interne organisatie van gemeenten. De belangrijkste risico’s voor de gemeentelijke informatieveiligheid, die van invloed zijn op het succes van informatiebeveiliging, zijn op dit moment:

- Informatiebeveiliging kampt met imagoprobleem;
- Inzicht in risico’s is niet integraal;
- Aanvallen op infrastructuur zijn succesvol door ontbreken basismaatregelen;
- Te veel werk voor te weinig mensen;
- De complexiteit neemt toe.

2.4.5 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen registratie waarin incidenten worden vastgelegd. Deze registratie geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.5 Uitgangspunten

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de gehele levenscyclus van informatiesystemen. Het beperkt zich echter niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, burgers, gasten en externe relaties. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

Het gehele gemeentelijk management speelt een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de gemeente heeft bij de verschillende onderdelen van de informatievoorziening, de risico’s die de gemeente hiermee loopt, welke van deze risico’s onacceptabel hoog zijn en welke maatregelen genomen worden om deze risico’s te beperken.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

2.5.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico’s van menselijk gedrag.
- Het voorkomen van ongeautoriseerde (fysieke) toegang.
- Het beheersen van de toegang tot informatiesystemen.
- Het garanderen van betrouwbare en veilige informatievoorzieningen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.

[5] https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2019-2020/

- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.5.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is vertrouwelijk. Het college van B en W is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Heumen hebben een interne eigenaar die de vertrouwelijkheid bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de gemeente. 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 (zie 3.3 Borging van het informatiebeveiligingsbeleid).
- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging (zie 3.3 Borging van het informatiebeveiligingsbeleid).
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- 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.
- 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 (verantwoordelijkheid iRvN, zie 2.3.2).

2.5.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten[6]:

- Het college van B en W en de gemeenteraad stellen het strategisch informatiebeveiligingsbeleid vast. [5.1.1.1]
- Het managementteam (MT) stelt jaarlijks het informatiebeveiligingsplan vast
- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De 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 rechtstreeks aan het MT, voorafgaand aan de P&C-gesprekken (begroting, jaarrekening etc.).
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.

[6] Een verder uitgewerkte beschrijving van de organisatie (governance) van informatiebeveiliging is opgenomen in hoofdstuk 3. En in meer detail en *per gemeente* in de bijlage ‘informatiebeveiliging en privacy organisatie’.

- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT,BRO) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- De medewerkers die werken met de informatiesystemen van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Afdelingshoofden dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden voeren risicoanalyses informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.5.4 Randvoorwaarden

Randvoorwaarden voor een goede uitvoering van het informatiebeveiligingsbeleid zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt a.d.h.v. informatieveiligheidsanalyse een informatiebeveiligingsplan opgesteld onder leiding van de CISO (zie 3.3 Borging van het informatiebeveiligingsbeleid), gebaseerd op:
    - Information Security Management System (ISMS);
    - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - het dreigingsbeeld gemeenten van de Informatie Beveiligings Dienst (IBD);
    - de door de afdelingshoofden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3. Aansturing, uitvoering en verantwoording

In dit hoofdstuk wordt op hoofdlijnen uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de gemeenten. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

In het separate document ‘informatiebeveiliging en privacy organisatie gemeente Heumen’ zijn de rollen van de informatiebeveiliging en privacy in nader detail beschreven.

3.1 Aansturing: de directie

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De directie zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad. [18.2.2]

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Heumen, gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: afdelingshoofden

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingshoofden. Om deze

verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn, dus door de CISO. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Deze werkzaamheden zullen over het algemeen uitgevoerd worden door beveiligingsbeheerders binnen de eigen afdeling van het afdelingshoofd. De CISO adviseert en ondersteunt in de uitvoering waar nodig. De bedoeling is dat alle processen, applicaties en data altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Afdelingshoofden rapporteren aan de directie over de onder hun verantwoordelijkheid tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het managementteam-overleg. Voorbereiding en coördinatie van dit managementteam-overleg ligt bij de CISO.

Taken van de afdelingshoofden in het kader van informatiebeveiliging zijn:

- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld;
- Het leveren van input voor (wijzigingen op) maatregelen en procedures (input voor het jaarlijkse informatiebeveiligingsplan);
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures;
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

De verdere uitwerking van dit beleid gebeurt in maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard. Die uitwerking biedt handvatten aan medewerkers om het werk op een professionele manier uit te voeren.

Er zullen aanspreekpunten informatiebeveiliging en privacy worden aangesteld. Deze aanspreekpunten (veelal de beveiligingsbeheerders) komen onder de verantwoordelijkheid van de CISO en FG/privacy officer minimaal 4 keer per jaar bij elkaar. De CISO en FG/privacy officer zal dit overleg organiseren en voorzitten. Daarnaast komen de beveiligingsbeheerders DigiD, Suwinet, BAG, BGT, BRO, BRP en PUN periodiek bij elkaar om de maatregelen uit het jaarplan voor informatiebeveiliging uit te voeren en daarover verantwoording af te leggen via ENSIA.

3.3 Borging van het informatiebeveiligingsbeleid

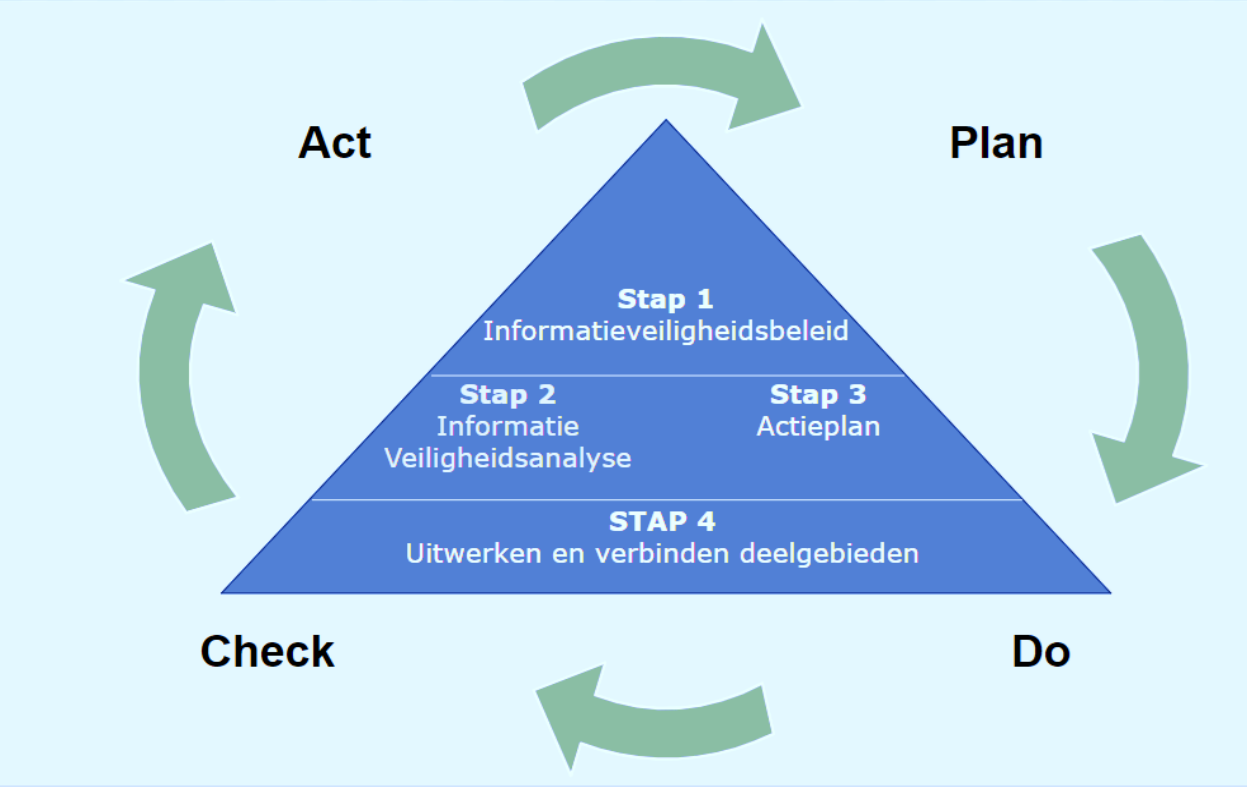
Om de borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie informatiebeveiliging en privacy organisatie), onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA-cyclus resulterend in een Information Security Management System (ISMS) [18.2.1.1] (zie figuur 1):

1. Informatieveiligheidsbeleid (zowel strategisch als tactisch):
Bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Dit is een organisatiebreed 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 voor de directie, dit wordt ook wel het ‘pas toe of leg uit’ principe genoemd. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 3 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats [5.1.2.1];

2. Informatieveiligheidsanalyse:
Stap twee is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een informatieveiligheidsanalyse. Hiertoe wordt allereerst een overzicht opgesteld van de gegevensverzamelingen/applicaties in de gemeentelijke organisatie door de Ciso. Deze worden toegewezen aan een eigenaar en geclassificeerd op de risicoklassen beschikbaarheid, integriteit en betrouwbaarheid van de informatie (ook wel dataclassificatie genoemd). Tevens wordt het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld. Hierbij geldt dat gemeentebreed het BBN2 wordt gehanteerd. Hiervan kan slechts bij individuele informatiesystemen en mits voldoende beargumenteerd (vastgelegd), worden afgeweken. Hierna wordt de praktijksituatie in de gemeente getoetst aan het gemeentebrede informatieveiligheidsbeleid en aan de beveiligingsmaatregelen uit de BIO, middels het uitvoeren van een GAP-analyse, rondgang door het gebouw, evaluatie ENSIA en een (eventuele) evaluatie van het vorige actieplan. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar;

3. Actieplan Informatieveiligheid (informatiebeveiligingsplan):
Op basis van de informatieveiligheidsanalyse wordt in stap drie een actieplan opgesteld. De in de analyse geconstateerde risico's worden gewogen waar nodig van maatregelen voorzien. Prioritering van de acties wordt gedaan op basis van de risico's die zijn geconstateerd, de beschikbare tijd en de beschikbare middelen. Hierdoor ontstaat een compact actieplan waarmee de gemeente vaststelt welke verbeteracties gedurende een periode van 1 of 2 jaar worden uitgevoerd. Dit actieplan vormt een praktische leidraad voor de verbetering en borging van informatieveiligheid in de organisatie. De informatieveiligheidsorganisatie (beveiligingsbeheerders) komt bij elkaar om de implementatie van het actieplan informatieveiligheid te evalueren te bewaken en waar nodig bij te stellen. Dit vindt conform de bespreking in het informatieveiligheidsoverleg (zie paragraaf 3.2) minimaal viermaal per jaar plaats.

4. Technische en organisatorische maatregelen:
Stap vier bestaat uit het opleveren van een complete set aan technische en organisatorische maatregelen die gericht is op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO, maar ook om applicaties zoals de BRP, SUWI, de BAG, het financiële systeem, of om de primaire processen van de organisatie, ICT-beheerprocessen of de inrichting van de ICT-platformen (iRvN). Dit betreft met name het opstellen van procedures en werkinstructies.



Figuur 1: De informatieveiligheidspiramide met PDCA cirkel

3.4 Controle en verantwoording
Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de individuele gemeente Heumen. De bestuurders, directies en afdelingshoofden van de gemeenten zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De directie beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de beleidsregels, normen en andere eisen met betrekking tot de desbetreffende beveiliging. [18.2.2] Dit mondt uit in het jaarverslag. Daarin wordt in lijn met de P&C-cyclus en ondersteund door een In Control Verklaring (ICV) gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatieveiligheid. In deze rapportage worden ook andere voor informatieveiligheid en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld. [18.1.4.2; 18.2.2.1] De CISO zal de directie ondersteunen in de uitvoering hiervan.

Om te beoordelen of de gemeente haar informatieveiligheidsbeleid- en doelstellingen behaalt, worden periodieke onafhankelijke audits - waarbij een onafhankelijke deskundige partij een toets uitvoert op de opzet, bestaan en werking van beheersmaatregelen - en controles uitgevoerd. Hiertoe kan een externe (erkende) partij worden ingeschakeld of de eigen afdeling concern control/auditafdeling. Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben. [18.2.1.2] In dit plan wordt tevens een beschrijving van de uit te voeren controles opgenomen, evenals de uitvoerders en verantwoordelijken (lijnniveau) voor de controles gekoppeld aan een tijdsplanning. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel van dit plan. [18.2.3.1] Over de resultaten van de uitgevoerde audits wordt door de lijnverantwoordelijken gerapporteerd aan de CISO. De CISO bundelt deze bijdragen en rapporteert hierover periodiek aan het bestuur.

3.4.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen (de CISO). Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA per gemeente wordt opgehaald bij de verantwoordelijke afdelingshoofden. De afdelingshoofden zijn er voor verantwoordelijk dat alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten wordt aangeleverd.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van de individuele gemeente aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording word het college en de raad van de gemeente Heumen geïnformeerd. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente informatiebeveiliging serieus neemt.

4. Bevordering beveiligingsbewustzijn

Informatiebeveiligingsbeleid is niet iets dat wordt gemaakt om in de kast te leggen. Een goed informatiebeveiligingsbeleid wordt beoogd de basis te leggen voor goede informatieveiligheid binnen de gemeente. Niet alle delen van het informatiebeveiligingsbeleid van de gemeenten zijn voor alle doelgroepen binnen de gemeenten even belangrijk. En ook niet alle doelgroepen zullen hetzelfde kennisniveau (hoeven) hebben. De gemeenten onderscheiden daarom verschillende doelgroepen. De volgende doelgroepen worden onderscheiden:

1. De medewerkers die werken met de informatie(systemen)
2. Beheerders van informatie(systemen)
3. Bestuurders, directie en afdelingshoofden

1. De medewerkers die werken met de informatiesystemen

Door het houden van bewustwordingscampagnes wordt structureel invulling gegeven aan het informeren van de medewerkers binnen de gemeente over de algemene beginselen van informatiebeveiliging die iedere medewerker zou moeten kennen en toepassen. Hier wordt invulling aan gegeven door het plaatsen van berichten op het intranet, het geven van workshops of het beschikbaar stellen van e-learnings.

2. Beheerders van informatiesystemen

Dit betreft de technisch- en functioneel applicatiebeheerders. Specifieke aandachtspunten voor de beheerders zijn:

- De bijzondere positie van de beheerder en de gevaren
- Omgang met beheerdersaccounts, autorisaties en wachtwoorden
- Dataclassificatie (passende bescherming van gevoelige gegevens zoals persoonsgegevens)
- Back-up en restore
- Beheren op afstand
- Bedrijfscontinuïteit
- Open standaarden (Forum Standaardisatie)
- IT-beveiligingsprocessen en procedures zoals incidentmanagement, CMDB, wijzigingsbeheer etc.

3. Bestuurders, directie en afdelingshoofden

Onderwerpen die van belang zijn voor hoofden, leidinggevenden en bestuurders:

- Beveiligingsverantwoordelijkheden van het hoofd
- Personeelsprocessen (in dienst, uit dienst en functiewisselprocessen)
- Beveiliging en projecten
- Risicomanagement
- Bedrijfscontinuïteit en crisisbeheersing
- Beveiliging en inkoop
- Dataclassificatie
- Privacy
- Verantwoording over beveiliging (ENSIA)

Naast het kunnen beschikken over de juiste middelen, vraagt bovenstaande om een bewuste houding. Bewust van de kansen die digitaal werken biedt voor de medewerkers en voor burgers en bedrijven. En bewust van de risico's ten aanzien van de vertrouwelijke gegevens en de middelen waarmee die kansen worden gerealiseerd.

Die bewuste houding ontstaat niet vanuit het niets. Medewerkers worden geïnformeerd over de aanwezigheid van ondersteunende middelen en hoe deze praktisch en veilig benut kunnen worden. En medewerkers worden geïnformeerd over de mogelijke bedreigingen waaraan onze

informatiehuishouding tegenwoordig bloot staat. Waarbij uiteraard ook wordt geleerd hoe deze bedreigingen het hoofd te bieden.

De informatiebeveiliging kan immers nog zo goed op orde zijn, deze valt of staat op basis van de kennis en bewustwording en de houding en het gedrag van de medewerkers die met de informatie werken. Het is de verantwoordelijkheid van iedere medewerker om de aangeboden kennis tot zich te nemen en toe te passen. En het is aan de leidinggevenden om deze professionele houding te ondersteunen en waar nodig te stimuleren.

Bijlage 1 – Organogram informatiebeveiliging en privacy organisatie