Strategisch Informatieveiligheidsbeleid 2021-2024

Versie	: 1.0 Definitief
Auteurs	: Chief Information Security Officier (CISO)
Datum	: Augustus 2021

I. Voorwoord

I.I Totstandkoming

In dit document is het strategische informatieveiligheidsbeleid beschreven van de gemeenten Culemborg, West Betuwe, Tiel en de Bedrijfsvoeringsorganisatie West-Betuwe. De basis van dit informatieveiligheidsbeleid wordt gevormd door de Baseline Informatiebeveiliging Overheid (BIO). De BIO is afgeleid van de internationale informatieveiligheidsnormen NEN-ISO/IEC 27001:2017 en 27002:2017. De eerste standaard (ISO27001) is een norm voor de implementatie en planmatige borging van informatieveiligheid binnen de organisatie. De tweede standaard (ISO27002) bevat een verzameling van beveiligingsmaatregelen voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. In de BIO zijn de methodiek en de terminologie specifiek aangepast voor de situatie bij overheden. In ISO27001/2 staan de details voor de toepassing, die niet in de BIO zijn beschreven en die nodig zijn voor een goede implementatie van de BIO.

Het strategisch informatiebeveiligingsbeleid is gebaseerd op de BIO. De impact van de uitwerking van de BIO in de werkorganisaties kan consequenties hebben op de personele capaciteit.

Eerdere strategische informatiebeveiligingsbeleidsstukken zijn beschreven conform de voorganger van de BIO, de Baseline Informatiebeveiliging Gemeenten (BIG).

I.II Leeswijzer en ambitieniveau

Dit document bevat strategische beleidsuitgangspunten op het gebied van informatieveiligheid (geheel van activiteiten, methoden en middelen ter waarborging van de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van informatie) en de organisatie daarvan. Hierin staan de verantwoordingsmechanismen en de rollen en verantwoordelijkheden aangaande informatieveiligheid beschreven. Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen worden gesteld, zoals de Wet basisregistratie personen (Wet BRP), de Algemene Verordening Gegevensbescherming (AVG), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en de Wet openbaarheid bestuur (Wob).

Met dit document worden de uitgangspunten ten aanzien van de veiligheid van informatieprocessen bepaald. Dit beleid brengt niet de huidige situatie in beeld, maar beschrijft het ambitieniveau aangaande gemeente brede informatieveiligheid waarnaar gestreefd wordt gedurende de looptijd van dit beleid. Waar relevant is in dit document met rechte haken [] een verwijzing naar de BIO opgenomen. Dit betekent echter niet dat in alle gevallen dat de volledige maatregel door de implementatie van dit beleid wordt afgedekt.

I.III Algemene oriëntatie en positionering

Informatieveiligheid maakt deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Het doel van informatieveiligheid is het behoud van:
- Beschikbaarheid / continuïteit (voorkomen van uitval van systemen en de controleerbaarheid);
- Integriteit / betrouwbaarheid (gegevens zijn juist, actueel volledig en controleerbaar);

- Vertrouwelijkheid / exclusiviteit (onbevoegden kunnen (controleerbaar) geen kennis nemen van gegevens die niet voor hen bestemd zijn).

I.IV Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en nationale wet- en regelgeving, zoals (niet-uitputtend):

- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet 2017;
- Wet computercriminaliteit;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet / Archiefregeling;
- Databankenwet;
- Wet elektronisch bestuurlijk verkeer (WMEBV;
- Wet elektronische handtekeningen (WEHT);
- Wet algemene bepalingen Burgerservicenummer (WABB);
- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet openbaarheid bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Basisregistratie grootschalige topografie (BGT);
- Wet Basisregistratie Ondergrond (BRO);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet Politiegegevens (WPG);
- Wet ruimtelijke ordening (WRO).

Op grond van bovenstaande wet- en regelgeving worden er eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de (interne) controle daarop.

I.V Forum Standaardisatie

De overheid is verplicht om te voldoen aan de normen NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:20131 waarop de Baseline Informatiebeveiliging Overheid is gebaseerd. Deze normen zijn opgenomen in de lijst met verplichte standaarden voor de publieke sector van het Forum Standaardisatie. De gemeenten Culemborg, West Betuwe, Tiel en de Bedrijfsvoeringsorganisatie West-Betuwe volgen ook de standaarden uit de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie. De BIO geeft diverse verplichte maatregelen aan die zowel voor de eigen organisaties als ketenpartners en leveranciers gelden. 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.

[1] Het Forum Standaardisatie spreekt van de norm uit 2013 waar in de BIO 2017 wordt genoemd. Het Forum Standaardisatie licht dit als volgt toe: “Na plaatsing op de 'pas toe of leg uit'-lijst zijn zowel ISO 27001 als ISO 27002 Europese normen geworden. Inhoudelijk zijn de normen niet gewijzigd. Hierdoor is het meest actuele specificatiedocument NEN-EN-ISO/IEC27002:2017. Inhoudelijk is het gelijk aan de specificatie NEN-ISO/IEC27002:2013 die getoetst is voor opname op de 'pas toe of leg uit'-lijst.” (Bron: https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27001)

Context

Sinds april 2016 werken de gemeenten Culemborg, Geldermalsen en Tiel samen in de Bedrijfsvoeringsorganisatie West-Betuwe (BWB). Vanaf 1 januari 2019 is de gemeente Geldermalsen samen met de gemeenten Neerijnen en Lingewaal gefuseerd tot de nieuwe gemeente West Betuwe. Vanaf dat moment is ook de gemeente West Betuwe aangesloten bij BWB.

BWB verricht verschillende bedrijfsvoeringstaken voor de aangesloten gemeenten. Alle gemeenten hebben hun taken op het gebied van informatiemanagement, ICT, financieel beheer, facilitaire zaken en personeelszaken bij BVOWB belegd. Culemborg en Tiel hebben daarnaast ook de afdelingen financieel advies en juridische zaken ondergebracht bij BWB.

BWB voert voor alle aangesloten gemeenten taken op het gebied van informatiebeveiliging uit. BWB voert taken echter alleen uit in mandaat, er zijn door de gemeenten geen bevoegdheden overgedragen aan BWB. De gemeenten blijven zelf dan ook verantwoordelijk voor hun informatiebeveiliging, op de manier zoals die verder in dit document is beschreven. Waar in dit informatiebeveiligingsbeleid wordt gesproken over “onze organisatie(s)” of “de gemeente”, heeft dit betrekking op zowel BWB als de bij BWB aangesloten gemeenten. Alle vier deze organisaties hebben dit beleidsstuk individueel vastgesteld.

BESTUURLIJKE UITGANGSPUNTEN

Informatiebeveiliging wordt voor onze gemeenten steeds belangrijker. Naarmate wij meer informatie vergaren, benutten en als knooppunt fungeren in lokale informatienetwerken, neemt ook het belang van adequate bescherming van informatie verder toe. Niet alleen verwerken wij vaak met gevoelige persoonsgegevens, ook delen wij deze gecontroleerd met netwerkpartners om uitvoering te kunnen geven aan onze maatschappelijke taken. Het feit dat wij dit als gemeenten binnen de context van Bedrijfsvoeringsorganisatie West-Betuwe (BWB) meer en meer in gezamenlijkheid doen, leidt ook tot verdere schaalvergroting en centralisatie van de aan ons toevertrouwde informatie. Wij beschouwen informatiebeveiliging dan ook als een wezenlijk onderdeel van de gezamenlijke bedrijfsvoering.

Dit hoofdstuk bevat de (inter)bestuurlijke beleidsuitgangspunten voor informatiebeveiliging door de samenwerkende gemeenten en BWB. Middels deze uitgangspunten wordt richting gegeven aan de wijze waarop informatiebeveiliging de komende beleidsperiode in de praktijk invulling zal krijgen. Dit vanuit de noodzaak om focus aan te brengen en om de keuzes te maken die nodig zijn om informatiebeveiliging effectief te laten zijn.

De Baseline Informatieveiligheid Overheid (BIO) dient als kader en toetssteen voor het informatieveiligheidsbeleid van BWB dat gestoeld is op het model van de Informatiebeveilingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG). Dit model maakt duidelijk hoe informatieveiligheid in de gemeentelijke context gestalte kan krijgen. Met de uitgangspunten in dit specifieke hoofdstuk maken wij duidelijk hoe wij welke accenten leggen om de BIO in de praktijk van onze gemeenten te laten werken. Voordat wij hieronder de beleidsuitgangspunten presenteren, schetsen wij een aantal trends en daarmee verbonden risico’s.

Trends waar onze inspanningen op het gebied van informatieveiligheid zich op moeten richten:

Onze gemeenten zijn complexe informatiehuishoudingen die over grote en groeiende hoeveelheden data beschikken.

We kunnen stellen dat informatie de kern vormt van de gemeentelijke processen. Data stelt ons in staat om uitvoering te kunnen geven aan toevertrouwde maatschappelijke taken.
Met deze data kunnen wij er tevens in voorzien dat de dienstverlening aan onze burgers tijdig, vertrouwelijk en juist is. Ook kunnen we er zo voor zorgen dat bestuurlijke- en verantwoordingsprocessen adequaat gestalte krijgen. Het feit dat we dit meer en meer in samenwerking doen, zorgt dat de schaal en complexiteit van onze (gezamenlijke) informatiehuishouding verder toeneemt;

Onze gemeenten zijn knooppunten in het lokale informatieverkeer met burgers en partnerorganisaties.
Wij verzamelen, bewaren en delen informatie met partners in het lokale informatienetwerk. Deze datalast is in de voorbije jaren toegenomen door verdergaande decentralisatie, waardoor ons takenpakket is uitgebreid. Binnen het sociaal domein is gegevensuitwisseling met lokale welzijns-, zorg- en veiligheidspartners met het oog op onze maatschappelijke dienstverlening onontbeerlijk. Het delen van – vaak privacygevoelige – data is absoluut noodzakelijk voor de lokale samenleving, maar juist ketensamenwerking brengt ook informatierisico's met zich mee.

Onze gemeenten zijn de hoeders van de persoonlijke informatie die wij voor en namens onze burgers beheren.
Als samenwerkende gemeenten moeten wij bij uitstek in kunnen staan voor de bescherming van de gegevens van onze burgers. Zij mogen van ons verwachten dat hun informatie beschikbaar, veilig en integer is. Tegelijkertijd bestaat vanuit de uitvoering van gemeentelijke taken een noodzaak tot dataverwerking en bewerking met allerlei diensten binnen en partners buiten de gemeente. Beveiliging en adequate omgang van (privacy)gevoelige gegevens, is daarmee een kerntaak voor onze gemeenten – en biedt een belangrijke voorwaarde om het vertrouwen van burgers te behouden.

Informatierisico's zijn voortdurend in ontwikkeling en laten zich niet altijd makkelijk voorspellen. Vanwege de introductie van nieuwe technologieën en toepassingen, zijn deze risico's bovendien progressief en niet vaststaand. Omdat het verwerken van informatie tot op zekere hoogte mensenwerk blijft, bestaat er een verhoogde kans op onveilige omgang met informatie. Incidenten kunnen daardoor nooit helemaal worden uitgesloten. Hieronder presenteren wij enkele (soorten) risico's die wij de komende beleidsperiode voor onze gemeenten realistisch achten (in willekeurige volgorde):

- **Cybercriminaliteit** komt steeds vaker voor, ook bij gemeenten. Enkele collega-gemeenten zijn de afgelopen jaren al slachtoffer geworden van hackers. *Phishing activiteiten*, al dan niet gericht op specifieke individuen (*spear phishing)*, komen veelvuldig voor. Er zijn ook risico's met betrekking tot *ransomware* waarbij crimelen het netwerk gijzelen in de hoop losgeld te bemachtigen.

  Datalekken, bij een datalek gaat het om toegang tot of het vernietiging van, verlies, wijziging of vrijkomen van (persoons)gegevens zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook de onrechtmatige verwerking van gegevens en het verlies van (of toegang tot) (persoons)gegevens. Datalekken vormen reële risico's die nooit helemaal kunnen worden uitgesloten. Datalekken zijn feitelijk alle beveiligingsincidenten waarbij persoonsgegevens betrokken zijn. Veelal zijn datalekken het gevolg van onbedoeld menselijk handelen, maar uiteraard kunnen deze ook het resultaat zijn van gerichte acties zoals inbraak in systemen. Omdat datalekken veelal het resultaat zijn van onbedoeld menselijk handelen, is de kans op het optreden van datalekken reëel;

- Uiteraard moeten wij altijd attent zijn op **frauderisico's**. Echter, in deze tijd is de kans dat fraude zich digitaal voltrekt groot. Vanwege de hoeveelheid en verscheidenheid van onze administratieve processen bestaat er altijd een kans dat deze oneigenlijk worden gebruikt. Zelfverrijking is daarbij veelal het motief. Vanuit de samenleving zijn diverse voorbeelden bekend waaronder subsidiefraude en fraude via valse facturen;

De bestuurlijke uitgangspunten voor BWB en aangesloten gemeenten ten behoeve van informatieveiligheid zijn als volgt:

Wij zien informatieveiligheid als een gezamenlijke verantwoordelijkheid van BWB en de aangesloten gemeenten.
Dit houdt in dat wij elk vanuit onze eigen verantwoordelijkheid bijdragen aan een betere informatieveiligheid. BWB ondersteunt de gemeenten in technische zin optimaal door bijvoorbeeld de IT-infrastructuur en voorziet in een veilige dienstverlening. Gemeenten dienen als eindgebruiker van de diensten van BWB op hun beurt organisatorisch te voorzien in adequate gegevensbescherming. Bestuur en management dienen het belang hiervan uit te dragen en zich te conformeren aan informatieveiligheid. Medewerkers weten wat er van hen wordt verwacht en nemen hun verantwoordelijkheid. Zo wordt er gezamenlijk toegewerkt naar een cultuur en organisatie waarin informatieveiligheid een vaststaand gegeven is.

Wij beschouwen informatieveiligheid als een proces dat nooit af is en dat continue verbeterd wordt.
Het is onze ambitie om informatie zo goed mogelijk te beschermen. Wij kunnen en zullen echter nooit volledig in control zijn en alle risico's kunnen wegnemen. Het verder institutionaliseren en versterken van onze informatiebeveiliging kost bovendien tijd. Hoewel wij gegevensbescherming uiterst serieus nemen en bijbehorende inspanningen plegen, gaan wij ervan uit dat we altijd te maken zullen krijgen met incidenten. Dit houdt in dat we niet alleen moeten investeren in het zoveel mogelijk wegnemen van de oorzaken van onveiligheid, maar ook dat wij ons moeten voorbereiden op het tijdig signaleren en adequaat afhandelen van incidenten.

Wij geven informatieveiligheid richting en invulling op basis van actieve risicosturing.
Wij hanteren realistische risico's als uitgangspunt voor onze inspanningen. Alleen zo kunnen we recht doen aan de investeringen in verdere risicobeheersing. Het is niet de ambitie om op alle denkbare aspecten 100% veilig te zijn. Het is wèl de ambitie om ervoor te zorgen dat waarschijnlijke en impactvolle informatierisico's bekend zijn èn tot op een acceptabel niveau worden gemitigeerd. Risico-analyse en risicobeheersing vormen de essentie van de beleidscyclus. Op basis van uitkomsten van deze analyses, formuleren wij een risico-agenda met daaraan gekoppelde verbeterplannen die moeten leiden tot een doelgerichte risicoreductie.

Wij geloven dat toezicht op de naleving van het beleid een cruciale succesfactor is voor de uiteindelijke effectiviteit van informatieveiligheid.
In onze beleving wordt nog al eens onderschat wat er nodig is om informatiebeveiliging daadwerkelijk in te bedden in een organisatie. Zoals bijvoorbeeld de inbedding van een managementsysteem en een cyclisch (terugkerend) proces dat het continue leren en verbeteren van informatieveiligheid in de praktijk ondersteunt. Het is hierdoor duidelijk welke thema's, op welke momenten en op welke manier onderwerp zijn van toezicht en handhaving. Alleen zo bieden wij waarborgen voor de daadwerkelijke effectiviteit van de noodzakelijke maatregelen. Wij zetten daartoe in op vaste controle-, handhavings- en verantwoordingsmomenten, zoals terugkerende toezicht activiteiten, het inzetten van communicatie-instrumenten en het plannen van vaste terugkerende (hoog) ambtelijke en bestuurlijke handhavingsmomenten.

Wij willen tot op een verantwoord niveau transparant zijn en verantwoording afleggen over het gevoerde informatieveiligheidsbeleid. Vanwege onze belangrijke rol in democratische verantwoordingsprocessen en onze nabijheid tot de burger moeten wij in staat zijn om openbaar verslag te doen van onze inspanningen op het gebied van privacybescherming. Ook als dit niet altijd heeft geleid tot het gewenste resultaat, maar ook tot onveilige situaties of incidenten. Het in staat zijn om afwijkingen zoals datalekken te kunnen melden vergt immers een open cultuur en een transparante houding, waar in de toekomst steeds vaker een beroep op zal worden gedaan. Wij juichen openheid over eventuele tekortkomingen toe omdat we alleen op die manier onze informatieveiligheid verder kunnen verbeteren.

Wij zien informatiebeveiliging als breed geheel van technische en organisatorische maatregelen en procedures, bewustzijn en handelen.
Dit beleidsstuk gaat vooral in op te nemen technische maatregelen en organisatorische procedures. Minstens zo belangrijk is het om in te zetten op bewustzijn en handelen. Het merendeel van de incidenten wordt namelijk veroorzaakt door een menselijke fout. De gemeente zal daarom naast dit beleid ook zorgen voor een uitgebreid bewustwordingsprogramma om zo informatiebeveiliging als breed geheel te behandelen.

1. Informatieveiligheidsbeleid

Visie:
De komende jaren zetten de gemeenten en BWB samen in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Bewustwording is hierbij een belangrijk onderdeel in het verhogen van informatieveiligheid.

Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en vormt de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatie-onderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op een verantwoorde manier mogelijk, zo ook nieuw en innovatieve manieren van werken. De focus ligt op veilig informatie uitwisselen in alle verschijningsvormen, zowel elektronisch, op papier of mondeling. Dit beleid gaat dan ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers, of ze nu in- of extern zijn, is essentieel voor informatieveiligheid.

Doelstelling informatiebeveiligingsbeleid:
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid en door er voor te zorgen dat er zorgvuldig met informatie wordt omgegaan.

Resultaat:
Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid èn het vereiste beveiligingsniveau zijn vastgelegd zodat we de informatieveiligheid kunnen waarborgen en er sprake is van een hoge mate van bewustzijn op gebied van informatieveiligheid.

1.1 Strategisch beleidsdocument voor informatieveiligheid

Het college van B&W/bestuur stelt dit strategische beleidsdocument voor informatieveiligheid vast en maakt dit kenbaar aan alle medewerkers en handelt hiernaar. [5.1.1.1] Dit beleidsdocument bevat onderstaande punten:

- Doelstellingen en strategische uitgangspunten van informatieveiligheid;
- Beveiligingseisen;
- Organisatie van informatieveiligheid (zie hoofdstuk 2);
- omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatieveiligheidsrollen (zie hoofdstuk 2);
- Verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie II.II) en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie II.VI);
- Beschrijving van het periodieke evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid getoetst wordt (zie hoofdstuk 1.5).

1.2 Scope van het informatieveiligheidsbeleid

De scope van dit beleid omvat alle gemeentelijke informatieprocessen inclusief de onderliggende informatiesystemen, hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college, dit geldt ook voor de Gemeenteraad en de Griffie. Alle strategische beleidsuitgangspunten met betrekking tot informatieveiligheid en de organisatie van informatieveiligheid zijn in dit document samengebracht.

Externe partijen moeten hetzelfde beveiligingsniveau hanteren zoals opgenomen in dit beleid, zij moeten kunnen aantonen dat zij voldoen aan dit niveau van beveiliging. Specifieke informatie op het gebied van informatiebeveiliging van relevante expertisegroepen, leveranciers van hardware, software en diensten en de IBD wordt gebruikt om informatiebeveiliging verder te verbeteren[12.6.1]. Er is door de gemeente uitgewerkt wie met welke (overheids-) instanties en toezichthouders contact heeft ten aanzien van Informatiebeveiliging (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn. [6.1.3.1] Dit overzicht wordt minimaal jaarlijks bijgewerkt. [6.1.3.2]

Op basis van dit strategische beleidsdocument wordt door het Gemeenschappelijk Opdrachtgevers- & Opdrachtnemersoverleg (GO&O) informatieveiligheidsbeleid op tactisch niveau vastgesteld. Hierin wordt beschreven op welke manier de gemeente informatieveiligheid borgt, rekening houdend met de risico's. De kernelementen in het Tactisch informatieveiligheidsbeleid zijn de uitwerkingen van de volgende onderwerpen:

- Autorisatiebeleid;
- Dataclassificatiebeleid;
- Beleid leveranciers/externe partijen;
- Beleid gebruik bedrijfsmiddelen;
- Bedrijfsprocessen;
- Beheerrichtlijnen ICT;
- Configuratiebeheer;
- Continuïteitsbeheer;
- Interne controle;
- Fysieke beveiliging (beveiliging die met behulp van fysieke middelen gerealiseerd wordt);
- Gedragsregels;
- HR processen zoals in-, door- en uitstroombeleid;
- Incidentenmanagement;
- Logische toegangsbeveiliging;
- Loggingbeleid;
- Testbeleid;
- Thuiswerkbeleid;
- Wachtwoordbeleid;
- Wijzigingsbeleid.

In deze uitwerkingen wordt tevens rekening gehouden met privacy specifieke beveiligingseisen. Vervolgens zal de gemeente aanvullende procedures en andere operationele documentatie opstellen. Deze zullen de praktische uitwerking vormen van het tactisch beleid.

1.3 Borging van het informatieveiligheidsbeleid

Om de borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van de rollen (zie hoofdstuk 2), 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), geborgd in een ISMS applicatie.

1. Informatieveiligheidsbeleid (zowel strategisch als tactisch)
Bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Dit is een organisatie breed 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 èn verifieerbaar, dit wordt ook wel het 'pas toe of leg uit' principe genoemd.
Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. [5.1.2.1];

2. Informatieveiligheidsanalyse
Deze stap 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. 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 gemeente breed het BBN2 wordt gehanteerd, hiervan kan voor individuele informatiesystemen mits voldoende beargumenteerd en vastgelegd van worden afgeweken. Hierna wordt de praktijksituatie in de gemeente getoetst aan het gemeente brede informatieveiligheidsbeleid en aan de beveiligingsmaatregelen uit de BIO door het uitvoeren van een risico inventarisatie en evaluatie (RI&E), GAP-analyse, rondgang van het gebouw en een (eventuele) evaluatie van het vorige actieplan. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar;

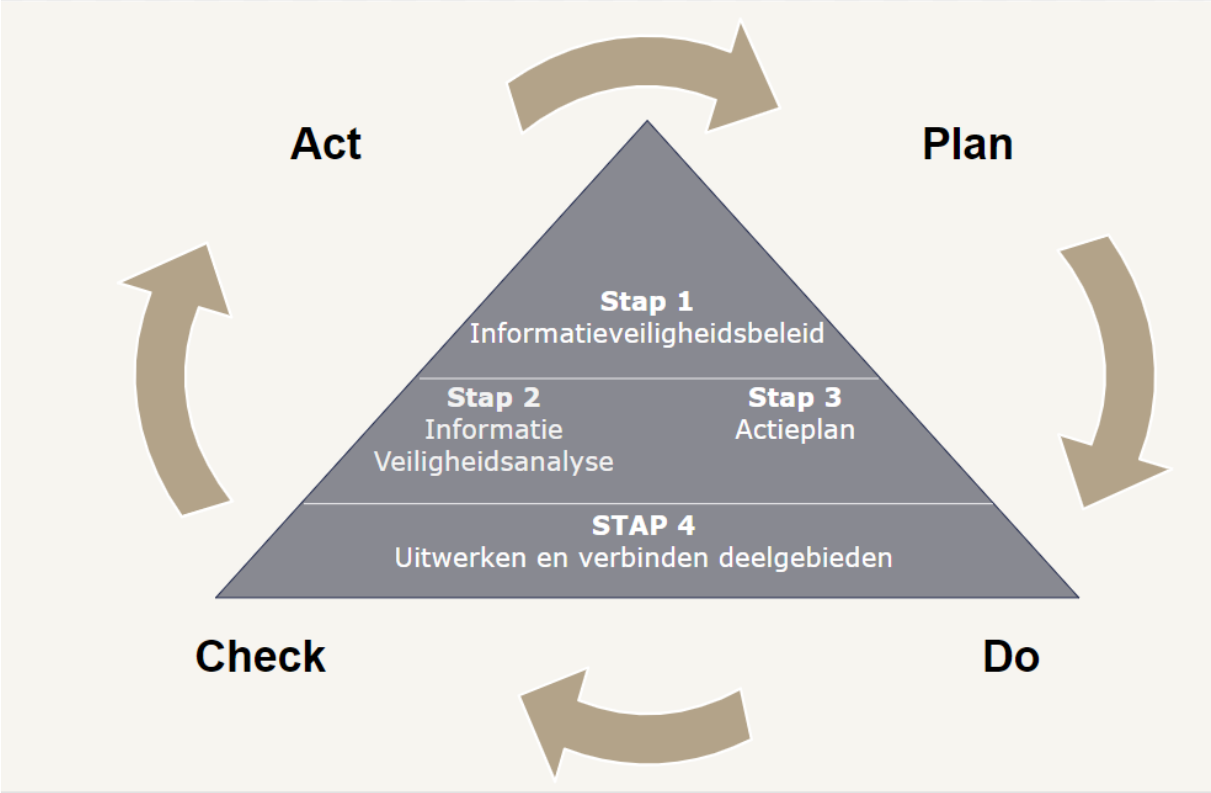
3. Actieplan Informatieveiligheid
Op basis van de informatieveiligheidsanalyse wordt in deze stap een actieplan opgesteld. De in de analyse geconstateerde risico's worden gewogen en waar nodig van beheersmaatregelen voorzien. Prioritering van de acties wordt gedaan op basis van de risico's die vanuit de RI&E 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 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 2.2) minimaal tweemaal per jaar plaats.

4. Technische en organisatorische maatregelen
De vierde stap 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. Dit betreft met name het opstellen van procedures en werkinstructies.

1.4 Audits en naleving

De directie beoordeelt de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. [18.2.2] Dit mondt uit in het jaarverslag. In een additionele 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]

Om te beoordelen of de gemeente haar informatieveiligheidsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke audits - waarbij een onafhankelijke deskundige partij een toets uitvoert op de opzet, bestaan en werking van beheersmaatregelen - en controles uitgevoerd. Deze audits staan los van de verplichte ENSIA audits. Hiervoor kan een (erkende) externe 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, 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.



Figuur 1: De informatieveiligheidspiramide met PDCA cirkel

2. Organisatie van de informatieveiligheid

Doelstelling:
Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.[8.1.2]

Resultaat:
Verankering in de gemeentelijke – en BWB organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid.

2.1 Verantwoordelijkheidsniveaus binnen de gemeenten Culemborg, West Betuwe en Tiel en de Bedrijfsvoeringsorganisatie West-Betuwe

Binnen de gemeenten Culemborg, West Betuwe, Tiel en de Bedrijfsvoeringsorganisatie West-Betuwe worden – waar relevant en in lijn met geldende wet- en regelgeving – de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden [6.1.1.2]:

2.1.1 Controle en toetsing door de Raad / bestuur
De gemeenteraad heeft een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatieveiligheid. Het college legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de raad, door middel van een collegeverklaring ENSIA (Eenduidige Normatiek Single Information Audit) – waarover door een auditor assurance wordt afgegeven – en daarnaast in het jaarverslag met een passage over informatieveiligheid in de paragraaf bedrijfsvoering. [18.2.2.1] BWB legt verantwoordelijkheid af aan het bestuur.

2.1.2 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het college van B&W van de gemeenten draagt als eigenaar van fr gemeentelijke informatieprocessen en (informatie)systemen de politieke - en bestuurlijke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Zij stellen met het voorliggende beleidsdocument de kaders ten aanzien van informatieveiligheid op basis van nationale - en Europese wet- en regelgeving vast. Het college informeert de Raad over de informatieveiligheid van de gemeente, door een aparte paragraaf op te nemen in de jaarrekening van de gemeente. Hierin wordt de Raad op de hoogte gebracht over de stand van zaken, de uitgevoerde plannen van het afgelopen jaar en de planning en plannen van het volgende jaar. Ook is een Chief Information Security Officer (CISO) op basis van een vastgesteld functieprofiel aangesteld door het college van B&W en werkt deze waar nodig samen met de controller. [6.1.1.2; 6.1.1.3; 6.1.1.4]

2.1.3 Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De gemeentesecretaris/directeur (bedrijfsvoering) voert onder mandaat van het college activiteiten uit voor informatieveiligheid die in een mandaatbesluit worden vastgelegd. In overleg met het directieteam / managementteam en de CISO stelt hij het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar (deze is verantwoordelijk voor het stellen van eisen aan een systeem en de inrichting van de controle hierop, zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen) aan.[8.1.2]

De *gemeentesecretaris/directeur (bedrijfsvoering)* heeft in ieder geval de volgende verantwoordelijkheden:

- Stellen van operationele kaders en het geven van sturing ten aanzien van informatieveiligheid;
- Sturen op risico's met betrekking tot informatieveiligheid;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- (laten) Controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Beleggen van de verantwoordelijkheid voor informatieveiligheidscomponenten en -systemen;
- Inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid om fraude, onrechtmatigheden en/of fouten te voorkomen.

2.1.4 Verantwoordelijkheden en taken op afdelingsniveau

De afdelings- of teamhoofden2 zijn eigenaar van en integraal verantwoordelijk voor de (informatie)veiligheid van de informatieprocessen en -systemen binnen hun afdeling.

De *afdelingshoofden* hebben in ieder geval de volgende verantwoordelijkheden*:*

- Classificeren van opgeslagen data in applicaties en gegevensverzamelingen;
- Medewerkers attenderen op hun verantwoordelijkheid ten aanzien van informatieveiligheid in hun dagelijkse werkprocessen;
- (laten) Uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn;
- Opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- Keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen;
- Oplossen van beveiligingsincidenten (Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten) [16.1.2.5];
- Expliciet vaststellen van relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem (een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen) en de organisatie;[18.1.1]
- Waarborgen van privacy en bescherming van persoonsgegevens conform relevante wet- en regelgeving [18.1.4];
- Opdrachtgeven tot en toezien op het uitvoeren van periodieke beveiligingsaudits;
- Rapporteren over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C rapportages.

2.1.5 Chief Information Security Officer (CISO)

De CISO is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het adviseren bij het beheersen van risico's en het opstellen van rapportages. De CISO heeft een onafhankelijke positie tegenover zowel het lijnmanagement als het bestuur van de gemeenten en BWB. Tevens heeft hij een directe rapportagelijn naar de (eindverantwoordelijke) gemeentesecretaris en de (bestuurlijk) portefeuillehouder en overlegt hij daarmee periodiek.

De CISO is centraal gepositioneerd binnen de bedrijfsvoeringsorganisatie West-Betuwe. De CISO is voor zover het de uitvoering van zijn taken betreft niet hiërarchisch ondergeschikt aan de algemeen directeur van de bedrijfsvoeringsorganisatie, noch aan de gemeentesecretaris/algemeen directeur (bedrijfsvoering).

De *CISO* heeft in ieder geval de volgende verantwoordelijkheden:

- Rapporteert rechtstreeks aan de gemeentesecretaris/directeur (Bedrijfsvoering) en het college en bestuur;

[2] Per gemeente kan de benaming anders zijn. Voor afdelings-/teamhoofden kan ook worden gelezen: teamleiders, teammanagers, etc.

- Coördineert het formuleren van informatieveiligheidsbeleid;
- Coördineert de uitvoering van de informatieveiligheidsanalyse en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;
- Coördineert de ENSIA verantwoording en rapporteert hierover aan het college;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de gemeentesecretaris/directeur (Bedrijfsvoering) en het directieteam / managementteam met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Geeft gevraagd èn ongevraagd advies over informatieveiligheid aan de gehele organisatie;
- Bevordert het beveiligingsbewustzijn in de organisatie door onder andere het organiseren van bijeenkomsten, trainingen, e-learning en andere awareness activiteiten;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Ondersteunt het college bij het maken van de rapportage over de informatieveiligheid van de gemeente in het jaarverslag.
- Onderhoudt contact met de Informatiebeveiligingsdienst;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages.

2.1.6 Functie specifieke beveiligingsfunctionaris

Op een specifiek deelgebied is er een beveiligingsfunctionaris met een voorgeschreven benaming. Dit betreft het gebied van reisdocumenten. Het betreft hier:

- *Beveiligingsfunctionaris reisdocumenten:* verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten;

Taken voor deze beveiligingsfunctionaris zijn:

- Periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid, dit gebeurt in samenwerking met de beveiligingsbeheerders en de CISO;
- Controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan informatieveiligheid dit gebeurt in samenwerking met de CISO;
- Controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse, dit gebeurt in samenwerking met de CISO;
- Bewaking van het niveau van informatieveiligheid, dit gebeurt in samenwerking met de CISO;
- Toetsing van evaluatieproces van beveiligingsincidenten, dit gebeurt in samenwerking met de CISO;
- Rapportage van bevindingen aan gemeentesecretaris en het college van B&W.

2.1.7 De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid binnen een specifiek deelgebied. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te hanteren wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: DigiD, BRP, Waardedocumenten

(officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations en Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI) en de BAG, BRO en BGT. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals Facilitaire Zaken, ICT, DIV (Archivering) en Personeelszaken) en de primaire processen (bijvoorbeeld Sociaal Domein, Financiën, Veiligheid & Handhaving, publieksdiensten (eventueel gecombineerd met BRP en Waardedocumenten), Ruimte/omgeving).

Specifiek verplichte beveiligingsbeheerdersrollen:

- *Autorisatiebevoegde Reisdocumenten/Aanvraagstations:* Verantwoordelijk voor het beheer van de autorisaties (het toekennen van rechten in informatiesystemen aan personen of groepen) voor de reisdocumentenmodules (RAAS en aanvraagstations);
- *Autorisatiebevoegde Rijbewijzen:* Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW;
- *Security Officer SUWI:* verantwoordelijk voor het beheer van beveiligingsprocedures en maatregelen in het kader van Suwinet. De Security Officer vraagt meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente en rapporteert hierover.

De *beveiligingsbeheerder* is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden. De proceseigenaar blijft verantwoordelijk, maar wordt in het proces ondersteund door de beveiligingsbeheerder.

2.1.8 Verantwoordelijkheden afdeling overstijgende (informatie)systemen

Afdeling overstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van de afdeling ICT gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatie-onderdeel worden gebruikt, bevatten gegevens die door meerdere organisatie-onderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie / het management het primaat om dit te mandateren aan een organisatie-onderdeel, dat kan ook BWB zijn, dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem. De procesverantwoordelijke van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

De gemandateerd eigenaar maakt minimaal de volgende schriftelijk afspraken met het gemeentelijke organisatie-onderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt:

- Voorwaarden voor het toegestane gebruik van het afdeling overstijgend (informatie)systeem;
- Verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatieveiligheid;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van afspraken en oplossen van eventuele geschillen;
- Recht op inzage in de resultaten van de externe audits en zelfevaluaties bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatieveiligheidsbeleid voldoet.

2.1.9 Functionaris gegevensbescherming (FG)
De FG is conform de Algemene Verordening Gegevensbescherming (AVG) de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente. [18.1.4.1] De FG heeft een onafhankelijke positie. De FG heeft de volgende wettelijke taken (AVG Art 39), vertaald naar de situatie bij de gemeente:

- Informeren en adviseren van het college, het management, de raad en de medewerkers over hun verplichtingen met betrekking tot gegevensbescherming;
- Toezien op naleving van zowel de AVG en andere wetten met betrekking tot gegevensbescherming als het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of BWB als verwerker. Hierbij hoort tevens toezien op de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de bij de verwerking betrokken personeel en de betreffende audits;
- Adviseren omtrent gegevensbeschermingseffectbeoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, en toezien op de uitvoering daarvan;
- Samenwerken met en als contactpunt optreden voor de Autoriteit Persoonsgegevens (AP);
- Rekening houden met risico's naar de aard, omvang en context van verwerkingen van persoonsgegevens.

De FG heeft voor privacy een toezichthoudende taak. Vanuit deze rol houdt hij ook toezicht op de registratie en de afhandeling van beveiliginsincidenten waar persoonsgegevens bij betrokken zijn. De FG rapporteert, op basis van art. 38 AVG, aan de hoogste leidinggevende van de verwerkingsverantwoordelijke. In de meeste gevallen is dit het college of de burgemeester, maar in sommige gevallen is dat de gemeenteraad.

De uitvoering en implementatie van het privacy beleid is belegd bij de proceseigenaar, die hierbij ondersteund wordt door de privacy officer en/of privacy beheerder(s) (per gemeente kan de benaming hiervan verschillen), al dan niet specifiek voor een bepaalde afdeling, zoals bijvoorbeeld het sociaal domein.

2.1.10 De privacy officer
Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast adviseert de privacy officer over privacybescherming en over activiteiten ter bescherming van persoonsgegevens. De taken en verantwoordelijkheden van de privacy officer zijn beschreven in het privacy beleid.

2.1.11 Medewerkers
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline in het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien van de betrouwbaarheid, de integriteit en de beschikbaarheid en controleerbaarheid van de informatieprocessen waarbij zij zijn betrokken. In het tactisch informatieveiligheidsbeleid zijn gedragsregels in het kader van informatieveiligheid uitgewerkt. Iedere medewerker wordt geacht deze gedragsregels te kennen en uit te dragen bij het uitoefenen van zijn of haar functie.

2.1.12 Overzicht organisatie en rollen
Het strategische informatiebeveiligingsbeleid beschrijft in hoofdstuk 2 een aantal verantwoordelijkheden met hierbij de rollen, taken en bevoegdheden. Hierin is een rolverdeling tussen de gemeenten en de bedrijfsvoeringsorganisatie West-Betuwe bepaald. Deze is in onderstaande tabel uitgewerkt.

Benaming	*Type*	*Waar*	*Inzet*	*Borging*
CISO	Functie	Centraal vanuit BWB	1 FTE	in formatie BWB
FG	Functie	Centraal vanuit BWB	1 FTE	in formatie BWB
Privacy Officer	Rol	Decentraal bij de gemeenten	NNB	in formatie gemeenten
Security Officer Suwinet	Rol (onder mandaat)	Decentraal bij de gemeenten	+- 0,1 FTE	In formatie gemeenten

2.2 Overleg en afstemmingsorganen

De CISO voert twee tot vier keer per jaar overleg met de directeur (bedrijfsvoering) en/of gemeentesecretaris en de FG.

Onderwerpen (niet-uitputtend):
- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid;
- Evaluatie van beveiligingsincidenten;
- Planning en voorbereiding van audits, controles en zelfevaluaties;
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse.

Daarnaast vindt afstemming plaats tussen de CISO en manager ICT en Facilitaire zaken, functie specifieke beveiligingsbeheerders, privacy officers en waar nodig de functioneel-, applicatie- en gegevensbeheerder(s) en de procesverantwoordelijken van (informatie)systemen.

2.3 Informatiebeveiligings crisisbeheersing

Voor interne crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit wordt vastgelegd in een separaat bedrijfscontinuïteitsplan (BCP). Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit zijn gebeurtenissen die een zodanige verstoring van informatiesystemen of processen tot gevolg hebben dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen. Directieteam/managementteam stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, IBD [12.6.1] enz.) wordt onderhouden. [6.1.3] De criteria voor de handels- en werkwijze tijdens grote incidenten of calamiteiten worden in een procedure nader uitgewerkt.

Dit team bestaat in ieder geval uit:
- Gemeentesecretaris (voorzitter)/Directeur BWB;
- CISO;
- De beveiligingsbeheerder ICT;
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit);
- Relevante experts (indien nodig);
- Een lid van de afdeling communicatie.