gemeente Tubbergen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tubbergen

Nr. 369974

29 augustus 2023

Strategisch informatiebeveiligingsbeleid Noaberkracht Dinkelland Tubbergen 2023-2026

1 Inleiding

1.1 Voorwoord

Voor u ligt het strategisch informatiebeveiligingsbeleid van de gemeenten Dinkelland en Tubbergen en de bedrijfsvoeringsorganisatie Noaberkracht Dinkelland Tubbergen voor de jaren 2023 tot 2026. Het vervangt de in 2020 vastgestelde nota Strategisch Informatieveiligheidsbeleid 2020 Noaberkracht Dinkelland Tubbergen.
Omwille van de leesbaarheid worden de gemeentenamen en de naam van de bedrijfsvoeringorganisatie in dit document verder samengevoegd tot Noaberkracht.
Het beleid heeft een looptijd van drie jaar, waarna evaluatie en bijstelling zal plaats vinden.
Deze nota is richtinggevend en kaderstellend en wordt uitgewerkt met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

1.2 Leeswijzer en inleiding

Dit document bevat strategische beleidsuitgangspunten op het gebied van informatiebeveiliging (het geheel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en de organisatie daarvan). Hierin staan de uitgangspunten, het sturings- en verantwoordingsmechanisme en de rollen en verantwoordelijkheden aangaande informatiebeveiliging beschreven. Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen worden gesteld, zoals de Wet basisregistratie personen (Wet BRP), Algemene Verordening Gegevensbescherming (AVG), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigID beveiligingsassessment (DigID audit) en Wet open overheid (Woo). Om te voorkomen dat binnen elk van die gebieden separaat (beveiligings-)beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatiebeveiligingsbeleid op te stellen voor alle organisatieonderdelen.
Het gemeentelijke informatiebeveiligingsbeleid geeft een algemene basis gebaseerd op algemene normen, eisen en risico-inschattingen. Het biedt geen afdoende bescherming tegen terrorisme of spionage van (vreemde) mogendheden.
Met dit document worden de uitgangspunten ten aanzien van de beveiliging van informatieprocessen bepaald. Dit beleid brengt niet de huidige situatie in beeld maar beschrijft het ambitieniveau aangaande organisatiebrede informatiebeveiliging. 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.

1.3 Het belang van informatie

Noaberkracht is een informatie-intensieve organisatie met een primaire focus op dienstverlening. Informatie is één van de voornaamste bedrijfsmiddelen voor het realiseren van doelstellingen zoals:

- optimale dienstverlening;
- samenlevingsgericht werken;
- vraaggericht werken;
- zaak- en procesgericht werken;
- datagedreven werken;
- digitalisering van dienstverlening;
- efficiënte interne en ketensamenwerking;
- werken in co-creatie;
- digitaal werken, plaats- en tijdonafhankelijk;
- optimale bereikbaarheid;
- transparant werken, open overheid;
- uitvoering van wettelijke kaders.

Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van Noaberkracht moeten kunnen beschikken over betrouwbare informatie om de klanten (burgers, bedrijven, organisaties) optimaal te kunnen helpen en adviseren. Deze moeten er op hun beurt op kunnen vertrouwen dat hun gegevens bij Noaberkracht in goede handen zijn.
De door Noaberkracht geformuleerde zeven actielijnen voor organisatieontwikkeling vereisen allemaal direct of indirect, een betrouwbare, correcte en veilige informatievoorziening. Zonder dit fundament zullen de ambities niet waargemaakt kunnen worden.

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en gemeenteraad en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen getroffen moeten worden.
Daarnaast zijn er ook eisen die door wet- en regelgeving worden gesteld. In bijvoorbeeld de AVG is de eis opgenomen om “passende” organisatorische- en technische maatregelen te nemen tegen “ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging". Het begrip "passend" geeft niet alleen aan dat er een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens moet zijn, maar ook dat beveiliging niet statisch kan zijn maar mee moet bewegen met dreigingen en de stand der techniek. Daarnaast zijn er specifieke eisen ten aanzien van informatiebeveiliging gesteld in andere wet en regelgevingen, zoals Wet Suwi, Wet BRP, Archiefwet maar ook wet- en regelgeving in het sociale domein.

2 Informatiebeveiliging

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

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
  Gegevens en functionaliteit dienen voor gebruikers zodanig beschikbaar te zijn dat zij hun taken optimaal kunnen uitvoeren.
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
  De juistheid en actualiteit van gegevens en functionaliteit dient te voldoen aan de daarvoor gestelde normen, wet- en regelgeving.
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden.
  Toegang tot (persoons)gegevens en functionaliteit is beperkt tot degenen die daartoe door de eigenaar hiervan zijn vastgesteld.

Naast deze drie meer traditionele elementen horen ook de volgende tot het domein van informatiebeveiliging:

- Controleerbaarheid: de mate waarin de juistheid en volledigheid van informatie en gegevensverwerking kan worden gecontroleerd.
  Zijn verwerkingen, handelingen en besluiten aantoonbaar en daardoor controleerbaar en te auditen. Ook: werken de getroffen maatregelen zoals deze bedoeld zijn.
- Onweerlegbaarheid: de waarborg dat de juistheid niet kan worden betwist.
  De ontvangst en-of verzending van een (al dan niet elektronisch) bericht kan niet worden ontkend door de ontvanger en de verzender.

Het verwerken van persoonsgegevens vereist in alle gevallen passende organisatorische en technische beveiligingsmaatregelen. Het beschermen van privacy – het eerbiedigen van de persoonlijke levenssfeer – wordt daardoor als een onlosmakelijk onderdeel van informatiebeveiliging beschouwd. Daar waar in dit document over beveiliging wordt gesproken mag ook het beschermen van privacy worden verondersteld.

2.1 Ontwikkelingen / veranderende omgeving

- De BIO (Baseline Informatiebeveiliging Overheid) is vanaf 2020 het normenkader voor de gehele overheid. De werkwijze van deze BIO is sterker gericht op risicomanagement dan het eerder door de gemeenten gehanteerde normenkader, de BIG. Van het (lijn)management wordt veel meer gevraagd om afwegingen en keuzes te maken over een adequaat niveau van beveiliging van hun processen en gegevens.
- Bij de dagelijkse taakuitoefening wordt steeds meer gebruik gemaakt van mobiele computerapparatuur waarbij informatiesystemen steeds meer in open verbinding staan met de buitenwereld. Ook door schaalvergroting en samenwerking in ketenautomatisering neemt de kans op, en de impact van, incidenten toe. Een zelfde risico ligt in het integreren of koppelen van systemen, die niet van oorsprong zijn ontworpen met veiligheid in gedachte.
- Doordat (de uitvoering van) veel taken – zowel wat betreft primaire processen als ondersteunende processen zoals ICT – door samenwerkings- of ketenpartners of toeleveranciers worden uitgevoerd worden hoge eisen gesteld aan opdrachtgeverschap en regievoering.
- De invoering van de Algemene Verordening Gegevensbescherming (AVG) heeft voor een boost gezorgd in de aandacht voor de bescherming van persoonsgegevens. Het belang van privacy

neemt steeds meer toe evenals de impact van privacyschendingen, zowel voor de betrokkene als voor de gemeente.
- De (nog relatief nieuwe) gemeentelijke publieke processen in het sociaal domein kennen een extra gevoeligheid en afbreukrisico.
- De door de VNG opgestelde en door alle gemeenten onderschreven principes voor de digitale samenleving geven richtlijnen en opgaven voor gemeenten in de omgang met digitalisering, dataverzameling en de inzet van technologie. Transparantie, democratische controle maar ook informatieveiligheid zijn hierbij kernbegrippen.
- Met Common Ground wordt een grote stap gezet in de richting van een open, transparante overheid waarbinnen gegevens sneller en veiliger kunnen worden uitgewisseld, zowel intern als extern. Common Ground is een beweging waarin gemeenten werken aan een stapsgewijze modernisering van de ICT-infrastructuur. Dit vraagt naast aandacht voor privacy ook veel aandacht voor informatieveiligheid.
- Internet of things en smart society-projecten dragen bij aan het vergroten van de leefbaarheid en veiligheid binnen de gemeente. Voorheen 'domme' objecten, worden slim (IoT) en maken het besturen van de gemeente makkelijker. Bijvoorbeeld prullenbakken die zelf aangeven dat ze vol zitten, of parkeerplaatsen die zelf aangeven dat ze vrij zijn. Maar ook minder mondaine toepassingen als sluizen, gemalen en riolen. Dit zet echter de informatieveiligheid verder onder druk. De IoT-apparatuur en -software die gemeenten hiervoor inzetten zorgen voor meer risico's en kwetsbaarheden.
- Kunstmatige intelligentie of artificial intelligence (AI) biedt kansen voor gemeenten. AI kan gemeenten helpen om beter inzicht te krijgen in hun processen en gegevens, en daarmee zorgen voor een betere dienstverlening voor inwoners en bedrijven. Het is ook een beveiligingstool van de toekomst. Met AI kunnen betere veiligheidsanalyses worden gedaan van allerlei systeem- en netwerkinformatie. Hiermee hebben gemeenten sneller inzicht in mogelijke incidenten of inbraakpogingen. De technologie is echter nog erg onvolwassen en vormt daarmee een risico voor de bedrijfsvoering. Hackers kunnen dit in de toekomst gebruiken om in te breken op gemeentelijke systemen.
- Het door de IBD/VNG periodiek opgestelde Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee zeer geschikt om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging. De volgende thema's werden en worden geprioriteerd voor 2023/2024:
    - *Financiën, structurele aanpak*: reserveer een vast percentage in het budget voor informatiebeveiliging en privacy.
    - *Techniek*: de basismaatregelen tegen ransomware zijn op orde.
    - *Eigenaarschap management*: informatiebeveiliging en gegevensbescherming staan op de managementagenda .
    - *Organisatie*: positie CISO en een veilige cultuur (CISO en FG als strategisch adviseur & een open en veilige cultuur.)
    - *Samenwerkingsverbanden*: maak afspraken en zie erop toe (laat ook verantwoording afleggen over beveiliging en privacy.)
    - *De factor mens*: investeren in bewustwording (veiligheid en privacy, ook binnen het eigen werkproces.)

- De eigen registratie en analyse van incidenten bij Noaberkracht geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.2 Scope

De scope van dit beleid omvat alle gemeentelijke informatieprocessen, zowel ambtelijke als bestuurlijke, inclusief de onderliggende informatiesystemen, informatie en gegevens van de gemeenten en betrokken externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord; ongeacht locatie, tijdstip en gebruikte apparatuur; inclusief Web based-, cloud-, SaaS-, PaaS-, IaaS-, etc. oplossingen.
Organisatorisch zijn de uitgangspunten van dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) de colleges en alle hieronder ressorterende bestuursorganen. Het zelfde geldt ook voor de gemeenteraden en de griffies en de daaraan gelieerde organisatieonderdelen (zoals de rekenkamer).
Het Informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers en ketenpartners van Noaberkracht:

Doelgroep	Rol bij informatiebeveiliging
Gemeenteraad	Controle en toetsing
College van B&W	Integrale verantwoordelijkheid

Directie, MT	Kaderstelling en implementatie
Beleidsmakers	Plan- en beleidsvorming binnen kaders
Gegevenseigenaren	Via classificatie bepalen van beschermingseisen
Teammanagers, proceseigenaren	Sturing op risico's en controle op naleving
ICT	Technische, systeem- en applicatiebeveiliging
Facilitaire zaken	Fysieke beveiliging en fysieke toegangsbeveiliging
HR	Arbeidsvoorwaardelijke zaken
Communicatie	Bevorderen bewustwording
Medewerkers	Gedrag en naleving
CISO	Dagelijkse coördinatie informatiebeveiliging/privacy
FG	Toezicht op naleving AVG
Control	Toetsing
Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance met eisen en richtlijnen
Burgers , klanten	*Informatief*

De specifieke taken en verantwoordelijkheden van beveiligingsrollen zijn nader uitgewerkt in hoofdstuk 5.

2.3 Wettelijke basis en controle beveiligingsnormen
De wettelijke basis van informatiebeveiliging valt af te leiden uit Europese verordeningen en richtlijnen en uit landelijke wet- en regelgeving, zoals (niet uitputtend):

- Auteurswet
- Telecommunicatiewet
- Ambtenarenwet
- Wet computercriminaliteit
- Algemene verordening gegevensbescherming (AVG)
- Archiefwet / Archiefregeling
- Beveiligingsnorm DigID
- Databankenwet
- Wet elektronisch bestuurlijk verkeer
- Wet elektronische handtekeningen
- Wet algemene bepalingen Burgerservicenummer
- Participatiewet
- Jeugdwet
- Wet maatschappelijke ondersteuning (Wmo)
- Paspoortwet
- Paspoortuitvoeringsregeling Nederland (PUN)
- Reglement Rijbewijzen
- Wet algemene bepalingen omgevingsrecht (Wabo)
- Wet basisregistratie personen (Wet BRP)
- Wet open overheid (Woo)
- 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 informatiebeveiliging, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

2.4 Forum Standaardisatie
Noaberkracht is als overheidsorganisatie verplicht te voldoen aan de standaarden uit de 'pas toe of leg uit[1] '-lijst met verplichte standaarden voor de publieke sector van het Forum Standaardisatie. Hiertoe

1) Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

horen onder meer de normen NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017 waarop de Baseline Informatiebeveiliging Overheid (BIO) is gebaseerd. 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.

3 Informatiebeveiligingsbeleid

Doelstelling: Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatiebeveiliging. Resultaat: Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatiebeveiliging alsmede het vereiste beveiligingsniveau zijn vastgelegd.

3.1 Het doel van informatiebeveiliging

Het Informatiebeveiligingsbeleid heeft als doel het waarborgen van de continuïteit van de informatievoorziening - en daarmee van de bedrijfsvoering – en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het beperken van eventuele gevolgen ervan.
Dit strategische kader is richtinggevend en kaderstellend voor het tactische informatiebeveiligingsbeleid en voor passende organisatorische en technische maatregelen. Deze hebben ten doel gemeentelijke informatie te beschermen en te waarborgen dat de gemeente haar bedrijfsdoelstellingen met digitalisering kan realiseren en voldoet aan relevante wet- en regelgeving.
De gemeente streeft er naar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in een PDCA-cyclus.
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 toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

Informatiebeveiliging is geen doel op zich. Dit informatiebeveiligingsbeleid moet dan ook in samenhang gezien worden met onder meer de organisatievisie, de visie op dienstverlening, de visie op informatievoorziening en passen binnen wet- en regelgeving.
In de informatievisie van Noaberkracht is als een van de leidende principes opgenomen dat de IV-organisatie professioneel gemanaged wordt. Governance is hierbij nodig om het te sturen en gericht door te ontwikkelen. Daarbij is governance er ook op gericht om de basis solide te houden. Ditzelfde geldt onverminderd voor informatiebeveiliging. Governance houdt in ieder geval in:

- helderheid in rollen, taken en verantwoordelijkheden (zie hoofdstuk 5);
- sturing door onder meer integratie in de P&C-cyclus (zie hoofdstuk 4);
- samenhang bewaken en prioriteiten stellen in implementatie en ontwikkeling.

3.2 Strategisch beleidsdocument voor informatiebeveiliging

De colleges van B en W behoren dit gemeentebrede strategische beleidsdocument voor informatiebeveiliging goed te keuren en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen. [5.1.1.1]
Dit beleidsdocument bevat de onderstaande punten:

- De doelstellingen en strategische uitgangspunten van informatiebeveiliging voor de gemeente;
- De beveiligingseisen;
- De organisatie van informatiebeveiliging (zie hoofdstuk 5);
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging voor managers, medewerkers en ondersteunende informatiebeveiligingsrollen (zie hoofdstuk 5);

- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie 2.3) en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie hoofdstuk 4);
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst (zie hoofdstuk 4).

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. Specifieke informatie op het gebied van informatiebeveiliging van relevante expertisegroepen, leveranciers van hardware, software en diensten en de IBD wordt gebruikt om de informatiebeveiliging te verbeteren. [12.6.1] De gemeente heeft uitgewerkt met welke instanties contact wordt onderhouden en door wie. [6.1.3.1] Dit overzicht wordt minimaal jaarlijks bijgewerkt. [6.1.3.2]

3.3 De plaats van het strategisch beleid

In het strategisch beleidsstuk worden de uitgangspunten, leidende principes en de organisatie van de informatiebeveiliging beschreven. Het geeft de hoofdlijnen en de kaders.
Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.
Het fundament van het tactische beleid van Noaberkracht wordt gevormd door de Baseline Informatiebeveiliging Overheid (BIO).
Alle Nederlandse gemeenten hanteren vanaf 1 januari 2020 samen met de rijksoverheid, de waterschappen en de provincies één uniform normenkader voor informatiebeveiliging: de BIO. Deze heeft de voor gemeenten gebruikte Baseline Informatiebeveiliging Gemeenten (BIG) vervangen. De BIO is gebaseerd op de internationale ISO27001/2-standaard en biedt een baseline met verschillende niveaus van beveiliging. Risicomanagement vormt zowel de basis van de BIO als een leidend uitgangspunt bij de implementatie en gebruik er van. De BIO bevat normen op alle te onderscheiden gebieden van informatiebeveiliging en vormt de bulk van het tactische informatiebeveiligingsbeleid van de gemeente. De BIO stelt normen voor de volgende onderwerpen:

- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- IB-aspecten van bedrijfscontinuïteitsbeheer
- Naleving

Daar waar dit vereist is of nodig wordt geacht op basis van risicomanagement worden door de gemeente aanvullende tactische beleidsdocumenten opgesteld.
De vertaling naar operationeel niveau zal bestaan uit talrijke maatregelen, richtlijnen, procedures en andere operationele documentatie. Deze zullen de praktische uitwerking vormen van het tactische beleid. De op te stellen en te implementeren werkzaamheden worden uitgewerkt in een jaarlijks te schrijven informatiebeveiligingsplan.

3.4 Visie op informatiebeveiliging

3.4.1 Uitgangspunten

Noaberkracht draagt er zorg voor dat de informatiebeveiliging (en als onlosmakelijk onderdeel daarvan privacy) goed georganiseerd wordt en blijft. De volgende uitgangspunten en leidende principes worden gehanteerd bij het informatiebeveiligingsbeleid:

- Alle informatie en informatiesystemen zijn van belang voor de gemeenten; bepaalde informatie is van vitaal en kritiek belang. De colleges van B en W zijn eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement (directie en teammanagers). Alle informatiebronnen en -systemen die gebruikt worden door Noaberkracht hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de

informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Informatiebeveiliging vraagt een onafhankelijke regie en soms ingrijpen in bestaande structuren, en dus om centrale en onafhankelijke functionarissen.
- Noaberkracht voldoet aan de wet- en regelgeving op het gebied van informatiebeveiliging en privacy.
- Risicomanagement vormt een basispeiler onder informatiebeveiliging. Dit vereist inzicht in en waardering van mogelijke kwetsbaarheden en dreigingen en de mogelijke impact van verstoringen.
- Het tactisch informatiebeveiligingsbeleid van Noaberkracht wordt gevormd door de BIO, uit te breiden met onderwerpspecifieke beleidsdocumenten waar dat in de BIO vereist wordt. De gemeente conformeert zich tevens aan toekomstige wijzigingen in de BIO.
- Door periodieke controle, organisatiebrede 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 risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging. Er wordt aansluiting gevonden bij de bestaande P&C-systematiek.
- Noaberkracht 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.

3.4.2 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
- De colleges van B en W stellen als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers 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 centrale positie alle onderdelen van de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de voortgangsgesprekken in het kader van de P&C-cyclus.
- Tijdens P&C-gesprekken dient 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 teammanagers zijn verantwoordelijk voor het realiseren van de informatiebeveiliging binnen de processen waar zij verantwoordelijk voor zijn. Dit geldt ook voor onderdelen die uitbesteed zijn of worden uitgevoerd bij samenwerkingsverbanden, ketenpartners of leveranciers. Deze vallen onverminderd binnen de scope van het informatiebeveiligingsbeleid van Noaberkracht.
- Hoewel de basisregistraties (zoals BRP, BAG, BGT) belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de organisatie. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de organisatie en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers gaan verantwoord om met persoonsgegevens en andere informatie.
- Teammanagers zien erop toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers voeren risicoscans informatiebeveiliging uit om deze risico-afwegingen te kunnen maken.

3.4.3 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met samenwerkingsverbanden, ketenpartners en leveranciers.
- Kennis en bewustzijn van informatiebeveiliging en het omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
  - de uitkomsten van de uitgevoerde informatiebeveiligingsanalyse;
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA) en andere uitgevoerde IT-audits;
  - de uitkomsten van de jaarlijkse zelfevaluaties BRP en PNIK;
  - het dreigingsbeeld gemeenten van de IBD;
  - de door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

4 Borging van het informatiebeveiligingsbeleid

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen. Resultaat: Een beheerst proces voor ontwikkeling, uitvoering, controle en bijsturing van informatiebeveiliging binnen de organisatie.

Om de borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 5), 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) (zie figuur 1). [18.2.1.1]

4.1 Informatiebeveiligingsbeleid (zowel strategisch als tactisch)

De start ligt bij de visie op informatiebeveiliging en het informatiebeveiligingsbeleid. Dit is organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de beveiliging van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar; dit wordt ook wel het ‘pas toe of leg uit’-principe genoemd. Bijstelling van het (strategische) informatiebeveiligingsbeleid vindt plaats rond een cyclus van drie jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats; [5.1.2.1]

4.2 Informatiebeveiligingsanalyse

Stap twee is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een informatiebeveiligingsanalyse. Tijdens deze informatiebeveiligingsanalyse wordt de praktijksituatie in de gemeente getoetst aan het gemeentebrede informatiebeveiligingsbeleid en aan de beveiligingsmaatregelen uit de BIO door middel van het uitvoeren van een risico-inventarisatie en -evaluatie (RI&E), een GAP-analyse, een scan van de fysieke beveiliging (rondgang gebouw) en een evaluatie van het vorige informatiebeveiligingsplan.
Bijstelling van de informatiebeveiligingsanalyse vindt jaarlijks plaats.
In de informatiebeveiligingsanalyse 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.

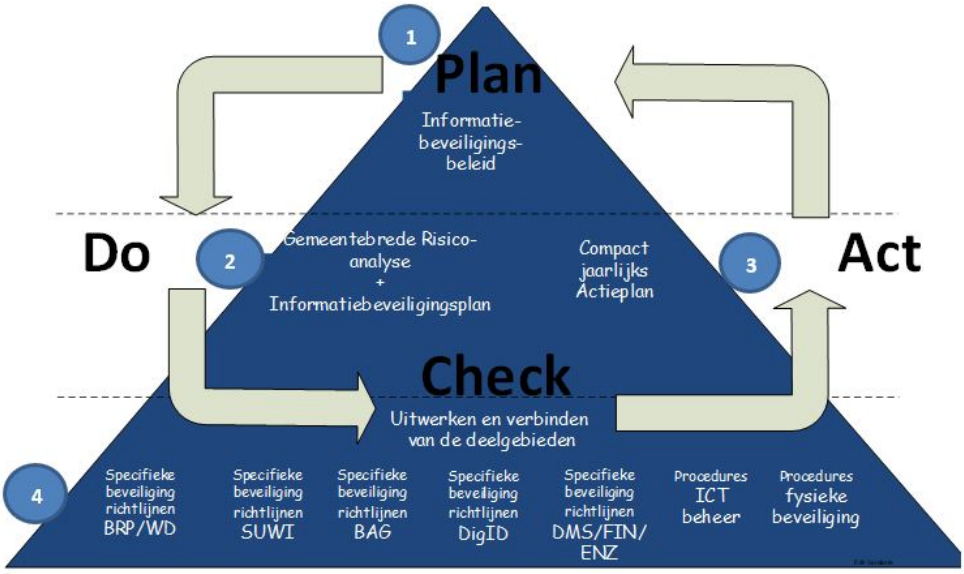
4.3 Informatiebeveiligingsplan

Op basis van de informatiebeveiligingsanalyse wordt in stap drie een actieplan opgesteld; het jaarlijkse informatiebeveiligingsplan. De in de analyse geconstateerde risico’s worden gewogen en waar nodig van maatregelen voorzien. Het invoeren van maatregelen gebeurt vanuit een risicobenadering: de effecten van de maatregelen moeten in verhouding staan tot de noodzakelijke beveiliging. Hierbij wordt ook gebruik gemaakt van beveiligingsclassificaties (dataclassificatie). 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 organisatie vaststelt welke verbeteracties gedurende een periode van een jaar worden uitgevoerd. Dit actieplan vormt een praktische

leidraad voor de verbetering en borging van informatiebeveiliging in de organisatie. De governancegroep informatiebeveiliging komt bij elkaar om de implementatie van het actieplan informatiebeveiliging te evalueren te bewaken en waar nodig bij te stellen. Dit vindt conform de bespreking in het informatiebeveiligingsoverleg minimaal vier maal per jaar plaats (zie paragraaf 5.2).

4.4 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 specifieke maatregelen voor 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.



Figuur 1. Informatiebeveiligingspiramide met PDCA-cyclus.

4.5 Audits en naleving

De directie beoordeelt regelmatig 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. 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 informatiebeveiliging. In deze rapportage worden ook andere voor informatiebeveiliging 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 organisatie haar informatiebeveiligingsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke controles en audits uitgevoerd - waarbij een onafhankelijke deskundige partij een toets uitvoert op de opzet, bestaan en werking van beheersmaatregelen. Hiertoe kan een externe (erkende) partij worden ingeschakeld of het eigen team concern control.
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 (lijnmanagement; teammanagers) 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 (teammanagers) gerapporteerd aan de CISO. De CISO bundelt deze bijdragen en rapporteert hierover periodiek aan management en bestuur.

5 Organisatie van de informatiebeveiliging

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 organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatiebeveiliging.

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement (i.c. de teammanagers) als de eerste lijn verantwoordelijk voor de eigen processen, waaronder ook voor informatiebeveiliging. De tweede lijn (CISO, risicomanagement, beveiligingsbeheerders) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn vindt nadere toetsing plaats door verbijzonderde interne controle (VIC) en wordt het geheel door een interne auditor getoetst en van een objectief oordeel voorzien met mogelijkheden tot verbetering. Het toezicht door de FG (functionaris gegevensbescherming) is hier een onderdeel van. Hier is op onderdelen nog een vierde lijn aan toe te voegen in de vorm van een (op onderdelen verplichte) externe audit.

5.1 Verantwoordelijkheidsniveaus binnen Noaberkracht
Binnen Noaberkracht worden – waar relevant in lijn met geldende wet- en regelgeving – de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatiebeveiliging onderscheiden [6.1.1.2]:

5.1.1 Controle en toetsing door de gemeenteraad
De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de eigen gemeente, zo ook voor informatiebeveiliging. Het college van B&W legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de raad, door middel van een collegeverklaring/ICV – waarop door een auditor assurance wordt afgegeven – en in het jaarverslag met een passage over informatiebeveiliging in de paragraaf bedrijfsvoering. [18.2.2.1]

5.1.2 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het college van B en W draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de eindverantwoordelijkheid voor een passend niveau van informatiebeveiliging. Verder stellen ze met het voorliggende beleidsdocument de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving vast. Het college informeert de gemeenteraad over de informatiebeveiliging van de gemeente, door een aparte paragraaf op te nemen in de jaarrekening van de gemeente. Hierin wordt de gemeenteraad op de hoogte gebracht over de stand van zaken, de uitgevoerde plannen van het afgelopen jaar en de planning en plannen voor het volgende jaar. Daarnaast worden de Chief Information Security Officer (CISO) en de controller informatiebeveiliging op basis van een vastgesteld functieprofiel aangesteld door het college van B en W. [6.1.1.2; 6.1.1.3; 6.1.1.4]

5.1.3 Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De directie van Noaberkracht voert onder mandaat van de colleges activiteiten uit voor informatiebeveiliging. Dit wordt in een mandaatbesluit vastgelegd. De directie stelt in overleg met het managementteam en de CISO het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De directie 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 aan. Deze is verantwoordelijk voor het stellen van eisen aan een systeem en de inrichting van de controle hierop, zodat voldaan wordt aan het informatiebeveiligingsbeleid en aan de wettelijke eisen. [8.1.2]
De *directie* heeft in ieder geval de volgende verantwoordelijkheden:
- Het stellen van operationele kaders en het geven van sturing ten aanzien van informatiebeveiliging;
- Het sturen op risico's omtrent informatiebeveiliging;
- Het periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen beveiligingsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze beveiligingsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en -systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging om fraude en/of fouten te voorkomen.

5.1.4 Verantwoordelijkheden en taken op teamniveau
De teammanagers (proceseigenaren) zijn eigenaar van en integraal verantwoordelijk voor de (informatie) beveiliging van de informatieprocessen en -systemen binnen hun organisatieonderdeel.
De *teammanagers* hebben in ieder geval de volgende verantwoordelijkheden:
- Het classificeren van opgeslagen data in applicaties en gegevensverzamelingen;

- Medewerkers attenderen op hun verantwoordelijkheid ten aanzien van informatiebeveiliging in hun dagelijkse werkprocessen;
- Het (laten) uitvoeren van maatregelen uit de informatiebeveiligingsanalyse die op het team van toepassing zijn;
- Het opstellen van betrouwbaarheidseisen voor de informatiesystemen van het team;
- De keuze voor en de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen;
- Het oplossen van beveiligingsincidenten (voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatiebeveiliging kan aantasten) [16.1.2.5];
- Het expliciet vaststellen van relevante wettelijke, statutaire, regelgevende, en/of contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen voor elk informatiesysteem (een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen) en de organisatie [18.1.1];
- Het 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;
- Het rapporteren, via de CISO, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de organisatie in de P&C-rapportages.

5.1.5 Chief Information Security Officer (CISO)

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's en het opstellen van rapportages.
De *CISO* heeft in ieder geval de volgende verantwoordelijkheden:

- Rapporteert rechtstreeks aan de directie, gemeentesecretaris en het bestuur;
- Coördineert het formuleren van informatiebeveiligingsbeleid en privacybeleid;
- Coördineert de uitvoering van de informatiebeveiligingsanalyse en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatiebeveiligingsmaatregelen uit de informatiebeveiligingsanalyse en de uitvoering van het actieplan informatiebeveiliging;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatiebeveiliging;
- Ondersteunt bestuur, gemeentesecretaris, directie en managementteam met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers van Noaberkracht en de gemeenten over informatiebeveiliging en privacy;
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse;
- Geeft gevraagd én ongevraagd advies over informatiebeveiliging en privacy aan de gehele organisatie;
- Bevordert het bewustzijn ten aanzien van informatieveiligheid en privacy in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van informatiebeveiligingsincidenten;
- Ondersteunt het college bij het maken van de rapportage over de informatiebeveiliging van de gemeente in het jaarverslag;
- Onderhoudt contact met relevante overheidsinstanties;
- Rapporteert over de informatiebeveiliging van de organisatie in de P&C-managementrapportages en levert een In Control Statement. Hierbij bundelt de CISO de deelbijdragen van het teammanagement.

5.1.6 De controller informatiebeveiliging

Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen beveiligingsmaatregelen en de escalatie van beveiligingsincidenten.
De *controller* informatiebeveiliging is in ieder geval verantwoordelijk voor:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatiebeveiliging; dit gebeurt in samenwerking met de beveiligingsbeheerders;
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatiebeveiligingsanalyse en het actieplan informatiebeveiliging;

- De controle op de periodieke actualisatie van het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse;
- De bewaking van het niveau van informatiebeveiliging;
- De toetsing van evaluatieproces van beveiligingsincidenten;
- De rapportage van bevindingen aan gemeentesecretaris en het college van B en W.

De rol van controller informatiebeveiliging heeft op twee specifieke deelgebieden een voorgeschreven benaming. Dit betreft het gebied van reisdocumenten en rijbewijzen. Het betreft de volgende benamingen:
- *Beveiligingsfunctionaris reisdocumenten:* verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- *Beveiligingsfunctionaris rijbewijzen:* verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

5.1.7 De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatiebeveiliging 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 verkrijgen wordt in dit beleidsdocument de beveiligingsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan de zogenoemde beveiligingsbeheerder. Op de volgende deelgebieden is een beveiligingsbeheerder 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, BGT en BRO. Daarnaast worden er (indien mogelijk) beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals facilitaire zaken, ICT, DIV (archivering) en HR/personeelszaken) en de primaire processen (bijvoorbeeld sociaal domein, financiën, beveiliging & 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 SUWI verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het college en vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

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 informatiebeveiligingsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden.

5.1.8 Verantwoordelijkheden bedrijfsvoeringsapplicaties

Bedrijfsvoeringsapplicaties zijn teamoverstijgende (informatie)systemen binnen de organisatie en worden onder de verantwoordelijkheid van het team Informatiemanagement en facilitair (IMF) gefaciliteerd en onderhouden. Deze systemen, die door meer dan één organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor iedere bedrijfsvoeringsapplicatie heeft het management de zorg dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem. De procesverantwoordelijke van een bedrijfsvoeringsapplicatie draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften (waaronder de juiste classificatie) 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 organisatieonderdeel of de externe organisatie dat van het teamoverstijgend (informatie)systeem gebruik maakt:
- Voorwaarden voor het toegestane gebruik van het teamoverstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het teamoverstijgend (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 informatiebeveiliging;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van afspraken en oplossen van eventuele geschillen;
- Het 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 informatiebeveiligingsbeleid voldoet.

5.1.9 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] Het is in die hoedanigheid een functie; geen rol. De FG heeft de volgende wettelijke taken (AVG Art. 39), vertaald naar de situatie bij Noaberkracht:
Het takenpakket van de *FG* bestaat uit de volgende punten (art. 39 lid 1 AVG):

- 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 als andere wetten met betrekking tot gegevensbescherming als ook het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de verwerker. Hierbij hoort tevens toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Adviseren omtrent gegevensbeschermingseffectbeoordelingen, ook wel Data Protection Impact Assessments (DPIA) genoemd, en toezien op de uitvoering daarvan;
- Toezichthouden op de registraties en afhandeling van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en toezichthouden op het melden van een datalek bij de Autoriteit Persoonsgegevens en bij de betrokkenen;
- 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;
- Contactpersoon binnen de organisatie;
- Rapporteren aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, zijnde in veel gevallen het college van B en W of de burgemeester en in sommige gevallen de gemeenteraad.

De FG vervult dezelfde functie voor de Wet politiegegevens (Wpg).
De FG heeft voor privacy een toezichthoudende taak, vergelijkbaar met de taak van controller informatiebeveiliging voor informatiebeveiliging. De uitvoering en implementatie van het beleid is belegd bij een of meerdere privacybeheerders, al dan niet specifiek voor een bepaald team, zoals bijvoorbeeld het sociaal domein.

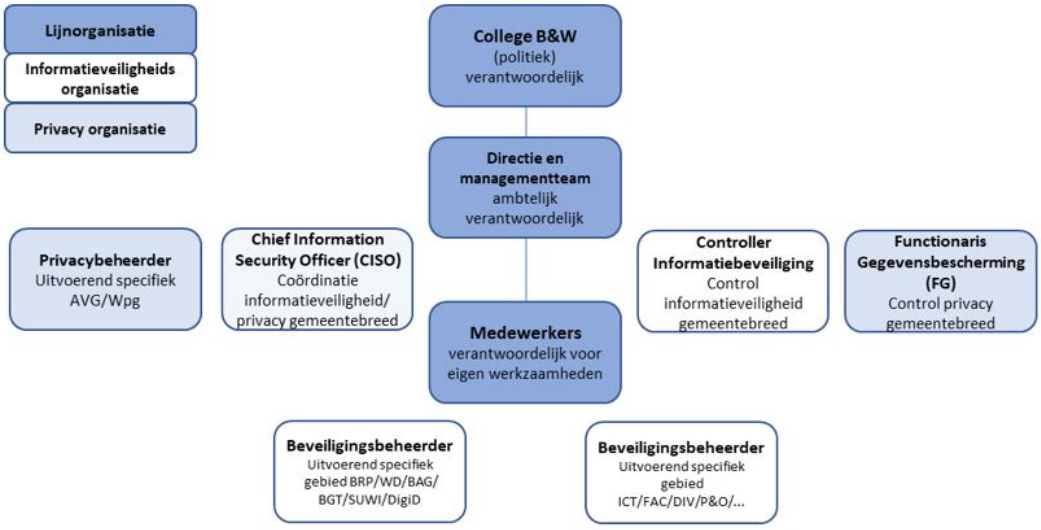
5.1.10 De privacy officer (privacybeheerder)

Deze rol is gericht op de uitvoering en de naleving van de Algemene verordening gegevensbescherming (AVG). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.
De *privacy officer* heeft in ieder geval de volgende verantwoordelijkheden:

- Beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van privacywetgeving en adviseert het management bij wijzigingen in procesuitvoering, bedrijfsvoering en de toepassing van een gegevensbeschermingseffectbeoordeling (DPIA).
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- Uitleggen van de privacyvoorschriften in de AVG en de sectorale en andere wetgeving;
- Coördineren van privacywerkzaamheden, informeren en het verzorgen van meldingen bij de AP;
- Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
- Coördineren van verzoeken om inzage, correctie, verwijdering en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
- Bijdragen aan rapportages aan het directieteam;
- Inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

5.1.11 De medewerkers

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



Figuur 2. Functies en rollen in de informatiebeveiligingsorganisatie

5.2 Overleg en afstemming

Governancegroep IBP

Minimaal vier maal per jaar wordt een overleg van de governancegroep IBP georganiseerd. De CISO is voorzitter van het overleg. Bij dit overleg zijn aanwezig:

- CISO;
- Controller informatiebeveiliging;
- Beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, BGT, BRO, DigiD en SUWI;
- Beveiligingsbeheerders t.a.v.: FZ, ICT, DIV en HR;
- Beveiligingsbeheerders t.a.v. kritieke processen;
- Functionaris gegevensbescherming;
- Privacy officer;
- Agendaleden: directielid of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatiebeveiligingsanalyse c.q. uit het actieplan informatiebeveiliging;
- Evaluatie van beveiligingsincidenten;
- Planning en voorbereiding van audits, controles en zelfevaluaties;
- Evaluatie en actualisatie informatiebeveiligingsbeleid, informatiebeveiligingsanalyse en actieplan.

Overleg informatiebeveiliging en privacy

Tweewekelijks overleggen de CISO, de functionaris gegevensbescherming en de privacy officer over tactische en operationele zaken.

Datalekteam

Het datalekteam heeft tot taak het onderzoeken en afhandelen van mogelijke incidenten, waaronder datalekken. Het komt in actie zodra er een informatiebeveiligingsincident is geconstateerd of aangemeld. Het team bestaat uit de CISO, de FG, de privacy officer en de voor het incident verantwoordelijke proceseigenaar. Indien nodig wordt het team per casus uitgebreid met andere specialisten.

Overleg CISO-IMF

Maandelijks overleggen de CISO en IMF over ontwikkelingen en tactische en operationele zaken binnen de organisatie.
Daarnaast vindt afstemming plaats tussen de CISO en de functioneel-, applicatie- en gegevensbeheerder(s) en de procesverantwoordelijke van (informatie)systemen.

5.3 Informatiebeveiligings-crisisbeheersing
Voor interne crisisbeheersing dient een kernteam informatiebeveiliging geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten (gebeurtenis die een zodanige verstoring van informatiesystemen of processen tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen). Het directieteam stelt vast in welke gevallen en door wie contacten met autoriteiten (brandweer, toezichthouders, IBD [12.6.1, 6.1.3.3] enz.) wordt onderhouden. [6.1.3] De criteria voor de handels- en werkwijze tijdens grote incidenten of calamiteiten worden nader in een procedure[2] uitgewerkt. Het kernteam bestaat in ieder geval uit:

- Directeur (voorzitter);
- CISO;
- De beveiligingsbeheerder ICT;
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit);
- Relevante experts (indien nodig);
- Een lid van het team communicatie.

2) Business continuity plan (BCP)