Informatiebeveiligingsbeleid van de Gemeenschappelijke Regeling Samenwerking de Bevelanden

Gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Versiebeheer

Het versiebeheer van dit document ligt bij de CISO.

Beheersmaatregel:	5.1.2
Documentversie:	2 februari 2018
Documentnaam:	Strategisch Informatiebeveiligingsbeleid GR de Bevelanden v10.docx

Versiebeheer

Versie	Beschrijving	Datum	Status
0.1	1e concept	02-11-2017	Vervallen
0.2	Aangepast concept	09-01-2018	Vervallen
0.3	Versie tbv hoofd en CISO's gemeenten	18-01-2018	Vastgesteld
0.4	Aanpassingen op basis van opmerkingen CISO's	22-01-2018	Vastgesteld
1.0	Concept tbv de vaststelling door het Dagelijks Bestuur	02-02-2018	Concept
1.0	Vastgesteld door het Dagelijks Bestuur	12-02-2018	Definitief

Inhoud

Inleiding

Aanleiding

Vanuit de (Rijks)overheid is de belangstelling en noodzaak voor informatieveiligheid de afgelopen jaren enorm toegenomen. Dit vanwege de alsmaar toenemende bedreigingen zoals cyber-criminaliteit in de vorm van phishing en DDOS en ransomware aanvallen, maar ook diverse ernstige beveiligingsincidenten, zoals DigiNotar. Daarmee is de kwetsbaarheid van de IT-infrastructuur bij gemeenten op een duidelijke wijze aangetoond. Dit heeft geleid tot een soort wake-up-call. Immers, beveiligingsincidenten kunnen het vertrouwen in de overheid ernstig schaden.

Mede als gevolg hiervan is in 2012 de Informatiebeveiligingsdienst voor gemeenten (IBD) onder de vlag van de Vereniging Nederlandse Gemeenten (VNG) opgericht en is de resolutie informatieveiligheid tijdens de bijzondere algemene ledenvergadering (BALV) in november 2013 door de leden bekrachtigd. In deze resolutie staat onder meer dat informatieveiligheid opgenomen wordt in de portefeuille van één van de leden van het college van B&W en dat de Baseline Informatiebeveiliging Gemeenten (BIG) het gemeentelijke basisnormenkader voor informatie-veiligheid wordt. Ook is in deze resolutie aangegeven dat gemeenten informatieveiligheid bestuurlijk en organisatorisch borgen en informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners. Verder is in deze resolutie afgesproken dat de gemeenteraad jaarlijks wordt geïnformeerd over informatieveiligheid in de gemeente en dat de verantwoordingslast voor gemeenten wordt verminderd.

De Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR) voert de taken op het gebied van Werk, Inkomen en Zorg uit voor de vijf deelnemende gemeenten. Daarnaast voert de GR de ICT-taken uit voor de eigen organisatie en voor de deelnemende gemeenten. Hierdoor is het niet alleen gewenst, maar zelfs noodzakelijk dat voor de GR op het gebied van informatiebeveiliging dezelfde regels gelden als voor de deelnemende gemeenten. Bij enkele onderdelen moet de GR de verantwoordingsdocumenten leveren, die de gemeenten moeten gebruiken bij het informeren van rijksoverheid en de betreffende gemeenteraden.

Met het in deze beleidsnota geformuleerde strategische informatiebeleid geven we verdere uitvoering aan de VNG resolutie en leggen we de basis om aan informatiebeveiliging in de organisatie verder vorm te geven.

Opbouw document

Informatiebeveiliging binnen de GR kan niet worden losgezien van het informatiebeveiligingsbeleid van de deelnemende gemeenten. Vanwege de gezamenlijke uitvoering van het onderdeel Werk, Inkomen en Zorg en omdat de ICT voor de deelnemende gemeenten door de GR wordt verzorgd, moet het informatiebeveiligingsbeleid nadrukkelijk worden afgestemd. Bij het vormen van het informatiebeveiligingsbeleid van de GR en het opstellen van dit document is daarom aansluiting gezocht bij en gebruik gemaakt van het beleid en de documenten van de deelnemende gemeenten.

Net als bij de deelnemende gemeenten is het informatiebeveiligingsbeleid gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Bij het opstellen van het beleid is ook gebruik gemaakt van het model uit het Information Security Management System (ISMS van SEP). Er is aansluiting gezocht bij de beleidsuitgangspunten van de deelnemende gemeenten. De resolutie van de BALV van november 2013 en BIG zijn volledig gericht op de gemeentelijke organisatie. Waar mogelijk is een vertaling gemaakt naar de organisatie van de GR.

In het eerste hoofdstuk geven we de definitie van informatiebeveiliging beschreven en stellen we de visie, het doel en de scope vast.

In hoofdstuk twee geven we aandacht aan de relevantie wet- en regelgeving op gebied van informatiebeveiliging bij gemeenten. In dat hoofdstuk formuleren we de uitgangspunten die we hanteren bij het vorm geven van de informatiebeveiliging in de GR.

De organisatie van de informatiebeveiliging en de taken, rollen en verantwoordelijkheden komen in hoofdstuk drie aan de orde. Tot slot volgt een korte uiteenzetting van de te volgen werkwijze om informatiebeveiliging in de organisatie te borgen.

Op een aantal terreinen wordt op dit moment door onze organisatie nog niet volledig voldaan aan de beleidsuitgangspunten. In het jaarlijks uit te brengen informatiebeveiligingsplan worden de tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt. Hierin staan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Wij hanteren bij de uitvoering van het informatiebeveiligingsbeleid een pragmatische aanpak..Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging binnen de GR de Bevelanden. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Bij het opstellen van dit document is het optimum beleid gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG).

In dit document is een aantal beleidsuitgangspunten benoemd en zijn beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden. Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de (kwaliteitshandhaving van de) bedrijfsvoering.

Plaats document

Dit Strategisch informatiebeveiligingsbeleid van de GR de Bevelanden is de kapstok waaraan het Tactische en Operationele informatiebeveiligingsbeleid worden opgehangen. Het onderhavige document vormt daarmee ook de basis voor het nog op stellen informatiebeveiligingsplan. In dat plan worden de uit te voeren beheersmaatregelen toegelicht en van een prioritering en planning voorzien. Het informatiebeveiligingsplan wordt in nauw overleg met de deelnemende gemeenten opgesteld.

Strategisch Informatiebeveiligingsbeleid GR de Bevelanden

Het bestuur en management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligings-beleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeenschappelijke regeling hebben, de risico's die de gemeenschappelijke regeling hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeenschappelijke regeling (GR). Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving.

De gemeenschappelijke regeling is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

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

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

1. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de GR. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het Dagelijks Bestuur als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.

2. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

3. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.

4. De organisatiebrede informatiebeveiligingsfunctionaris - binnen de GR de Bevelanden aangeduid als CISO - ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
   Daarnaast kennen we deelfuncties in de informatiebeveiliging zoals voor SUWInet: security officer SUWInet

5. De gemeenschappelijke regeling stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

6. Regels en verantwoordelijkheden voor het beveiligingsbeleid moeten worden vastgelegd en vastgesteld. Alle medewerkers van de gemeenschappelijke regeling worden getraind in het gebruik van beveiligingsprocedures.

7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Dit Informatiebeveiligingsbeleid treedt in werking na vaststelling door het Dagelijks Bestuur.

Aldus vastgesteld door het Dagelijks Bestuur van de Gemeenschappelijke Regeling Samenwerking de Bevelanden op 12 februari 2018.

1 Informatiebeveiliging

1.1 Wat is informatiebeveiliging?

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

- *beschikbaarheid / continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, SD kaart, beeldscherm et cetera) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk policy implementeren of hoe om te gaan met mobiele devices, zoals smartphones en laptops, en aanwijzingen voor telewerken.

1.2 Waarom informatiebeveiliging?

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

1.3 Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van GR de Bevelanden. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

Visie

De komende jaren zet de Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR) in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Dezelfde inzet geldt ook de dienstverlening aan de deelnemende gemeenten bij het realiseren van hun informatieveiligheid. Een betrouwbare informatievoorziening (zie onder 1.1) is noodzakelijk voor het goed functioneren van de GR en de deelnemende gemeenten, en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een ‘enabler’; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.).
Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. Hierbij is een medewerker niet alleen degene die in dienst is bij de GR en ambtenaar is in de zin van het Ambtenarenreglement, maar iedereen die via een arbeids-overeenkomst, via inhuur of anderszins betaalde of niet-betaalde werkzaamheden voor de organisatie verricht.

1.4 Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen, waarmee de GR voldoet aan relevante wet en regelgeving. De GR de Bevelanden streeft er naar om “in control” te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen, onder andere via een Verklaring Van Toepasselijkheid. In control betekent in dit verband dat de GR 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 middels de PDCA-cyclus (Plan-Do-Check-Act) verankerd is in de normale budgetcyclus van begroting, rapportage en jaarverslag.

2 Uitgangspunten informatiebeveiliging

2.1 Wet- en regelgeving

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de Wet Bescherming Persoonsgegevens (WBP). Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De WBP regelt in artikel 13 welke maatregelen organisaties moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft de gemeente is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 16 van de WBP. Deze maatregelen maken deel uit van het informatiebeveiligingsbeleid van een gemeente. Er zijn veel wetten en regelgeving van toepassing op de gemeente. De gemeente dient zich aan al deze wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging. Wetten en regelingen die van toepassing zijn (niet limitatief):

- Wet Bescherming Persoonsgegevens (Wbp)
- Wet Openbaarheid van Bestuur (WOB)
- Wet Computercriminaliteit II
- Comptabiliteitswet
- Archiefwet
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Politiegegevens (WPG)
- Ambtenarenwet
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI2012)
- Beveiligingsvoorschrift 2005 (BVR)
- CAR-UWO
- PUN
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2010)
- Kader Rijkstoegangsbeleid
- Uitgangspunten online communicatie rijksambtenaren
- Programma van Eisen PKI Overheid
- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- wet Structuur Uitvoering Werk en Inkomen (SUWI)
- Wet op de identificatieplicht
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet GBA en wet BRP
- Participatiewet
- Registratiewet
- Algemene wet bestuursrecht
- Richtlijnen van het NCSC

Informatiebeveiliging vereist een integrale aanpak. Dit strategische informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen zoals bij de wet SUWI en wet BRP. Dit strategische informatiebeveiligingsbeleid is als het ware de ‘paraplu’ boven andere documenten over informatiebeveiliging.

2.1.1 Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Het informatiebeveiligingsbeleid van de GR is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en bestaat uit 3 delen, te weten een strategisch, tactisch en operationeel deel. De BIG gaat direct in op de gemeentelijke organisatie. Omdat de GR deels taken uitvoert namens de deelnemende gemeenten (WIZ) en deels werkzaamheden uitvoert ten behoeve van de deelnemende gemeenten (ICT en P&O) hanteert de GR de BIG ook als basis. Waar hieronder de term ‘gemeente’ wordt gebruikt, moet ook ‘GR’ worden gelezen.

Strategische Baseline

Gericht op de organisatie en verantwoording over informatiebeveiliging binnen de gemeente.

Tactische Baseline

De Tactische BIG is het afgewogen minimale niveau van beveiliging waar een gemeente aan zou moeten voldoen en beschrijft 303 normen en maatregelen ten behoeve van controle en risicomanagement. Deze zijn gebaseerd op onder andere de internationale beveiligingsnorm ISO/IEC 27002:2007 en de WPB,GBA/BRP, BAG, SUWI en andere relevante wetgeving.

De Tactische BIG kan gefaseerd ingevoerd worden. 'Pas toe of leg uit' is het basisprincipe bij de implementatie van de BIG maatregelen. De maatregelen zijn generiek of specifiek. In het laatste geval dienen ze toegepast de worden op de verschillende systemen en processen binnen de gemeente. De normen en maatregelen uit de Tactische BIG hebben betrekking op de volgende onderdelen:

- Beveiligingsbeleid
- Organisatie van de informatiebeveiliging
- Beheer van bedrijfsmiddelen
- Personele beveiliging
- Fysieke beveiliging en beveiliging van de omgeving
- Beheer van communicatie- en bedieningsprocessen
- Toegangsbeveiliging
- Verwerving, ontwikkeling en onderhoud van informatiesystemen
- Beheer van Informatiebeveiligingsincidenten
- Bedrijfscontinuïteitsbeheer
- Naleving

Een hulpmiddel om te bepalen in hoeverre de gemeente voldoet aan de tactische BIG is de GAP analyse. Hierin kan per maatregel worden aangegeven of de maatregel al genomen is en wie verantwoordelijk is binnen de organisatie.

Operationele Baseline

Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD producten (aanvullend beleid, procedures, handreikingen etc.) ontwikkeld op operationeel niveau.

De rol van Chief Information Security Officer (CISO) is een belangrijke bij de BIG. Het is gebruikelijk dat deze de implementatie van de BIG coördineert en het informatiebeveiligingsplan opstelt.

Het implementeren, verdiepen en onderhouden van de baseline binnen de GR is een groeiproces wat zeker enkele jaren in beslag zal nemen om op het gewenste beveiligingsniveau volgens de BIG te komen. Dat heeft onder meer te maken met beschikbare capaciteit, leermomenten en met een cultuuromslag in het denken en handelen rond dit thema wat doorgaans een geleidelijk proces is.

2.1.2 Algemene Verordening Gegevensbescherming (AVG)

Het Europese Parlement en de Europese Raad hebben op 27 april 2016 officieel ingestemd met de Algemene Verordening Gegevensbescherming. De definitieve tekst is daarna op 4 mei 2016 gepubliceerd in het publicatieblad van de Europese Unie (Pb EU L119), waarna de verordening op 25 mei 2016 in werking is getreden. De Verordening heeft een directe werking en hoeft niet meer in nationale wetgeving geïmplementeerd te worden. Alle organisaties in de publieke en private sector hebben nu tot 25 mei 2018 om volledig aan de nieuwe wetgeving te voldoen. De AVG brengt met zich mee dat gemeenten verplicht zijn om een functionaris gegevensbescherming aan te stellen.

Met de invoering van de AVG verscherpen de eisen waaraan verwerkingen van persoonsgegevens moeten voldoen. De AVG vraagt echter om meer dan enkel ordentelijk met persoonsgegevens omgaan: de AVG vraagt om nieuw denken én handelen. Zo hebben inwoners het recht op inzage in waar welke gegevens van ze worden verwerkt. Inwoners hebben straks ook het recht om ‘vergeten’ te worden. Dat wil zeggen dat ze het recht hebben om zich te laten verwijderen uit databases, tenzij legitieme wettelijke vereisten dit voorkomen. Het in kaart hebben van de wettelijke grondslag van verwerking van persoonsgegevens is in dit kader van groot belang.

2.2 De uitgangspunten

Het bestuur en management spelen een cruciale rol bij het uitvoeren van het informatiebeveiligingsbeleid. Het bestuur en management geven een duidelijke richting aan informatiebeveiliging en laten zien dat zij informatiebeveiliging ondersteunen en zich betrokken voelen door het uitdragen en handhaven van een informatiebeveiligingsbeleid voor de hele GR.

Het Informatiebeveiligingsbeleid wordt vastgesteld door het Dagelijks Bestuur van de gemeenschappelijke regeling GR de Bevelanden. Het Dagelijks Bestuur herijkt periodiek het Informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, alle objecten, alle processen, alle informatiesystemen en gegevensverzamelingen. Bij het opstellen, uitvoeren en handhaven van het beleid geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals o.m. de Wet bescherming persoonsgegevens (WBP), het normenkader SUWInet (SUWI), de basisregistratie adressen en gebouwen (BAG), de paspoort uitvoeringsregeling (PUN) en de archiefwet.
- De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is het gemeenschappelijk normenkader.
- Vanwege de omvang van onze organisatie zijn niet alle genoemde beheersmaatregelen uit de BIG van toepassing of uitvoerbaar. Wij hanteren bij de uitvoering van het informatiebeveiligingsbeleid een pragmatische aanpak. Wij maken bij elke maatregel uit de BIG een afweging tussen het af te dekken risico, de werkbaarheid na invoering van een maatregel en de haalbaarheid van de invoering van een maatregel op budgettair vlak. Na het invullen van deze ‘driehoek’ beoordelen wij of we een gestelde maatregel uit de BIG invoeren. Bij alle maatregelen uit de BIG hanteren wij het pas toe of leg uit principe.

2.3 Uitgangspunten informatiebeveiliging GR de Bevelanden

1. Verantwoordelijkheid
   Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de GR en de gemeenten waarvoor de GR taken uitvoert. De verantwoordelijkheid voor informatiebeveiliging ligt bij de directie en de afdelingshoofden, met het Dagelijks Bestuur als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Baseline Informatiebeveiliging Nederlandse Gemeenten
   Het informatiebeveiligingsbeleid van de GR is in lijn met het algemene beveiligingsbeleid en informatie(voorzienings)beleid van de GR en de relevante landelijke en Europese wet- en regelgeving. Het Informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en daarmee op de Code voor Informatiebeveiliging (NEN/ISO 27001/27002). De BIG is het afgewogen minimale niveau van beveiliging waaraan een gemeente zou moeten voldoen. Hierbij is ruimte voor afweging en prioritering op basis van het ‘pas toe of leg uit’ principe.
3. Risico afweging
   De aanpak van informatiebeveiliging in de GR is gebaseerd op risico afweging. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG/KING (GAP-analyse). Als een systeem meer maatregelen nodig heeft of wanneer informatiebeveiliging beperkingen oplegt aan de bedrijfsvoering wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar.
4. Informatiebeveiligingsplan
   Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, beveiligingsincidenten, en bestaande risicoanalyses.

5. Proces
   Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het management systeem van informatiebeveiliging.
6. Chief Information Security Officer (CISO)
   De informatiebeveiligingsfunctionaris of Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover. Tevens onderhoudt de CISO contact met de CISO’s van de deelnemende gemeenten. Hiervoor is het Bevelands Overleg Informatieveiligheid ingesteld.
7. Mensen en middelen
   De GR stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
8. Bewustzijn
   Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging.
9. Medewerkers / Mensenwerk
   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.
10. Informatie Beveiligingsdienst (IBD)
    De GR is aangesloten bij de Informatie Beveiligingsdienst (IBD) en binnen de organisatie is een functionaris (VCIB) aangesteld die de verantwoordelijkheid heeft om beveiligingsincidenten te melden vanuit de gemeente aan de Informatiebeveiligingsdienst en de coördinatie van waarschuwingen vanuit de Informatiebeveiligingsdienst naar de gemeente te stroomlijnen.
11. Samenwerking
    De GR werkt samen met de Bevelandse gemeenten op het gebied van informatiebeveiliging.

2.4 Risicobenadering

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

2.5 Doelgroepen

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

Doelgroep	Relevantie voor Informatiebeveiligingsbeleid
Dagelijks Bestuur	Integrale verantwoordelijkheid
Directie	Kaderstelling en implementatie
Alle leidinggevenden	Sturing op informatieveiligheid en controle op naleving
Alle medewerkers	Gedrag en naleving
Proces en gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
het managementoverleg	Planvorming binnen de informatiebeveiligingskaders
CISO	Algemene en dagelijkse coördinatie van de informatiebeveiliging, adviseren over de implementatie van het informatiebeveiligingsbeleid
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken (via gemeenten)	Fysieke toegangsbeveiliging
de afdeling ICT	Technische beveiliging
Auditors	Onafhankelijke toetsing van het beleid
Leveranciers en ketenpartners	Compliance aan het beleid

2.6 Scope

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de GR, de deelnemers en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit informatiebeveiligingsbeleid is een algemene basis. Dit normenkader geldt dus expliciet ook voor de bedrijfsprocessen waar de audits en/of zelfevaluaties DigiD assessment, BAG inspectie, SUWInet, BRP, reisdocument en rijbewijzen zich op richten.

2.7 Informatiebeveiligingsbeleid en architectuur

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

2.8 ENSIA

Op meerdere taakvelden moeten gemeenten verantwoording afleggen over informatiebeveiliging. Hierdoor ontstond een lappendeken van zelfevaluaties en audits. Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid.

Ook roepen de gemeenten in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. Dit vormde de aanleiding voor de start van het project ENSIA. In nauwe samenwerking tussen het Ministerie van BZK, SZW, I&M en VNG/KING (kwaliteits instituut Nederlandse gemeenten; inmiddels VNG Realisatie) is een nieuw verantwoordingsproces informatieveiligheid opgesteld, te weten de ENSIA (Eenduidige Normatiek Single Information Audit). Dit betekent eenmalige informatieverstrekking en eenmalige IT-audit.

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Inkomen (SUWInet) is samengevoegd en gestroomlijnd.

Vanaf 2017 wordt door gemeenten aan de hand van ENSIA gewerkt. De nieuwe verantwoordings-procedure start met een zelfevaluatie met behulp van de ENSIA-tool. Hierin wordt de situatie van de gemeente getoetst aan de normen uit de BIG. Uitgangspunt is het horizontale verantwoordings-proces aan de gemeenteraad. Het college van B&W legt verantwoording af over informatieveiligheid aan de gemeenteraad in het jaarverslag. Het verantwoordingsproces sluit hierdoor aan op de Planning- en control cyclus. Het gemeentebestuur heeft zo meer overzicht over de informatie-veiligheid van haar gemeente. ENSIA structureert ook de verticale verantwoording richting de rijksoverheid over de Basisregistratie Personen (BRP) Paspoortuitvoeringsregeling (PUN), het gebruik van de digitale identificatie (DigiD), de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT) en de structuur uitvoeringsorganisatie Werk en Inkomen (SUWInet).

De verantwoordelijkheid van het gemeentebestuur voor informatiebeveiliging is niet beperkt tot de eigen organisatie, deze geldt ook voor gemeenschappelijke regelingen of samenwerkingsverbanden.

De ENSIA-tool, en daarmee de verantwoording, kan niet door de GR worden gebruikt. De GR moet de deelnemende gemeenten wel informatie leveren waarmee zij de verantwoording via de ENSIA kunnen afleggen. De GR gaat deze informatie leveren via een genormeerde verklaring, die vergezeld zal gaan van een verklaring door een EDP-Auditor.

3 Organisatie van de informatiebeveiliging

3.1 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen:

- Beheren van de informatiebeveiliging binnen de organisatie.
- Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Goedkeuring door het Dagelijks Bestuur en het managementoverleg van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

Voor een goede borging van informatiebeveiliging is het noodzakelijk dat verantwoordelijkheden helder zijn belegd. Binnen de GR hebben wij voor het onderwerp informatiebeveiliging te maken met de hierna beschreven verantwoordelijkheden, rollen en taken.

3.2 Verantwoordelijkheden

Het Dagelijks Bestuur van de Gemeenschappelijke Regeling samenwerking de Bevelanden is integraal verantwoordelijk voor de beveiliging (in de beslissende rol) van informatie binnen de werkprocessen van de GR en stelt het informatiebeveiligingsbeleid en –plan vast. Ook de jaarlijkse evaluatie over de uitvoering van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan wordt door het Dagelijks Bestuur vastgesteld. Binnen het Dagelijks Bestuur moet nog worden bepaald wie de portefeuillehouder voor de informatiebeveiliging is. Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar herijkt.

Het Dagelijks Bestuur stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

De directie (in de sturende rol) is verantwoordelijk voor kaderstelling en sturing.

De directie:

- stuurt op concern risico's;
- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen;
- controleert of deze maatregelen voldoende bescherming bieden;
- evalueert periodiek beleidskaders en stelt deze waar nodig bij.

Met betrekking tot informatievoorziening (de i-functie) geeft het afdelingshoofd ICT op dagelijkse basis namens de directie invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.

De leidinggevenden van de verschillende organisatieonderdelen zijn in de vragende rol verantwoordelijk voor de integrale beveiliging van hun organisatie onderdeel. Zie hiervoor de strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten.

De leidinggevenden:

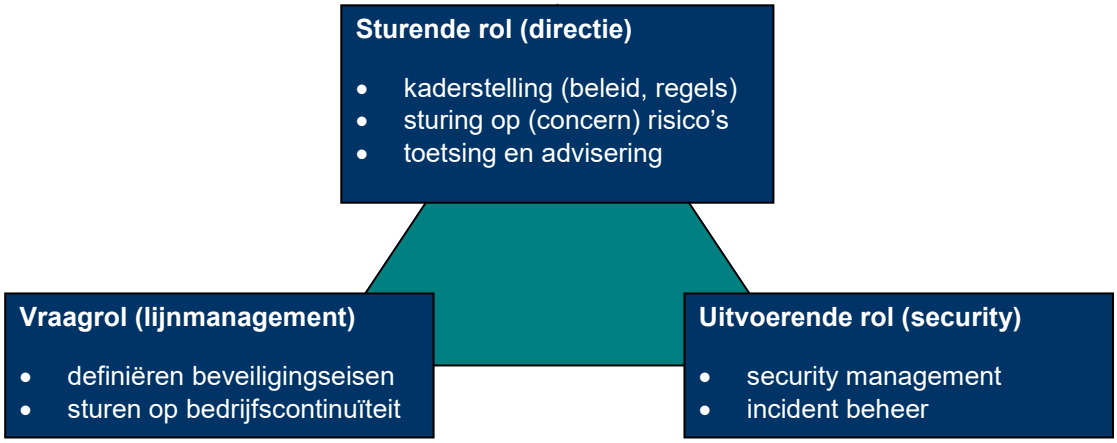
- stellen op basis van een expliciete risicoafweging betrouwbaarheidseisen voor hun informatiesystemen vast (classificatie);
- zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- melden incidenten en rapporteren in de managementrapportages of en in hoeverre hun organisatieonderdeel voldoet aan wet- en regelgeving en algemeen beleid van de GR.

Het managementoverleg moet het bewustzijn van de medewerkers op het gebied van informatiebeveiliging stimuleren. Dit vindt plaats door informatieveiligheid via een i-bewustzijnscampagne actief uit te dragen in de organisatie.

De leidinggevenden zijn in de uitvoerende rol verantwoordelijk voor de uitvoering van de beveiligingsmaatregelen.

Het afdelingshoofd ICT is verantwoordelijk voor:

- beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
- alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
- verzorgt logging, monitoring en rapportage; levert klanten (technisch) beveiligingsadvies.



Figuur 1: relaties

3.3 Taken en rollen

Het Dagelijks Bestuur stelt formeel het Informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het Dagelijks Bestuur als Algemeen Bestuur (controle functie) kunnen hiervoor opdracht geven om dit te (laten) controleren. De directie adviseert het Dagelijks Bestuur formeel over vast te stellen beleid.

Het afdelingshoofd ICT geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.

De taken m.b.t. informatiebeveiliging die hieruit voortvloeien zijn belegd bij de 'Chief Information Security Officer' (CISO). De CISO bevordert en adviseert gevraagd en ongevraagd over Informatiebeveiliging en rapporteert tenminste eens per jaar concernbreed aan de directie over de stand van zaken. Tevens is de coördinatie van informatiebeveiliging belegd bij de CISO. De uitvoerende taken binnen de afdeling WIZ zijn zoveel mogelijk belegd bij de security officer SUWInet. Deze security functionaris rapporteert aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de PDCA cyclus.

De Functionaris gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de algemene verordening gegevensbescherming (AVG) en andere wet-en regelgeving op het werkgebied (privacy en gegevensgebruik. De FG onderhoudt ook contacten met de Autoriteit Persoonsgegevens (AP) en meldt zo nodig incidenten met persoonsgegevens.

De Vertrouwd contactpersoon informatiebeveiliging (VCIB) onderhoudt contact met de informatiebeveiligingsdienst gemeenten (IBD) over landelijke incidentmeldingen of waarschuwingen waarvan de inhoud een vertrouwelijk karakter heeft en de eventuele interne opvolging daarvan.

De Algemene contactpersoon informatiebeveiliging (ACIB) onderhoudt contact met de informatie-beveiligingsdienst gemeenten (IBD) over waarschuwingen op technisch gebied. Deze rol wordt tevens namens de deelnemende gemeenten uitgevoerd.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
<u>Sturen:</u> **Directie dagelijkse uitvoering:** **Hoofd ICT/ CISO, security officer SUWInet**	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit, pentesten.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie/ Dagelijks Bestuur
<u>Vragen:</u> **Alle organisatie onderdelen**	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy.	Verbeteren bedrijfscontinuïteit. Rapportage aan CIO/CISO.
<u>Uitvoeren</u>: **Afdelingshoofd ICT**	Beleidsvoorbereiding, technische onderzoeken (marktverkenningen).	Leveren van diensten (ICT), incidentbeheer, logging, monitoring en ICT advies.	Kwetsbaarheid scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de directie over aanpassingen aan de informatie-voorziening.

3.4 Functioneel overleg

De CISO zit een werkgroep voor van security gerelateerde functionarissen en organiseert ten minste eenmaal per kwartaal een (security) overleg met deze werkgroep. Deze werkgroep heet Klankbord-groep Informatiebeveiliging. De CISO is voorzitter en verder bestaat deze Klankbordgroep in ieder geval uit de teamleider Cluster ICT beheer, een beleidsmedewerker van de afdeling P&O en de security officer SUWInet. Tevens kunnen relevante andere (externe) deskundigen, zoals inkoop, control en facilitair, worden gevraagd om deel te nemen.

Het overleg heeft binnen de GR een adviesfunctie richting de afdelingshoofden afzonderlijk en rechtstreeks aan het managementoverleg en richt zich met name op beleid en adviseert over tactisch/strategische onderwerpen betreffende informatiebeveiliging.

Het onderwerp Informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van het managementoverleg zodat er sturing kan plaatsvinden op de uitgevoerde activiteiten.

3.5 Externe partijen

Informatiebeveiligingsbeleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de GR samenwerkt (en informatie mee uitwisselt). Beleidsregels voor externe partijen zijn beschreven in de BIG. Ook voor externe partijen geldt hierbij het “pas toe of leg uit” beginsel.

Bij contractuele overeenkomsten gelden in beginsel altijd de eigen inkoopvoorwaarden van de GR. Hierin zijn onder meer geheimhouding, privacybescherming en aansprakelijkheid geregeld. Voor ICT gerelateerde aankopen en inhuur is zijn de Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) van toepassing. Deze voorwaarden zijn in december 2016 vastgesteld door de VNG. Net als de deelnemende gemeenten, heeft de GR deze voorwaarden ook van toepassing verklaard. Afwijkingen dienen te worden getoetst aan Informatiebeveiligingsbeleid zoals vastgesteld door de organisatie. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of verwerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de GR het recht heeft afspraken te (laten) controleren via een auditor “right to audit”.

Voor het tot stand brengen van datakoppelingen met externe partijen, gelden naast dit generiek informatiebeveiligingsbeleid specifieke procedures. Het doel van deze procedures is risicobeheersing. Voor externe hosting van data en/of services gelden naast dit generieke informatiebeveiligingsbeleid de richtlijnen voor cloud computing.

De GR is gehouden aan:

- regels omtrent grensoverschrijdend dataverkeer;
- toezicht op naleving van regels door externe partijen;
- hoogste beveiligingseisen voor bijzondere categorieën gegevens (dit zijn bijvoorbeeld ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen);
- melding bij de Autoriteit Persoonsgegevens bij uitbesteding van het bewerken van persoonsgegevens en toestemming van de Autoriteit Persoonsgegevens bij doorgifte van persoonsgegevens naar landen buiten de EU.

3.5.1 Deelnemende gemeenten

De GR kent enkele bijzondere externe partijen. Dat zijn de deelnemende gemeenten. De GR voert verschillende taken uit namens of ten behoeve van deze gemeenten. Omgekeerd neemt de GR ook een aantal diensten af van deze gemeenten. De afspraken en verantwoordelijkheden van de verschillende taken moeten in aanvullende overeenkomsten worden vastgelegd.

Speciale aandacht moet bijvoorbeeld worden besteed aan de facilitaire dienstverlening (o.a. huisvesting ICT) van gemeenten aan de GR. Daarnaast zijn de gemeenten formeel verantwoordelijk voor het gebruik van SUWInet, terwijl de GR (afdeling WIZ) de grootste gebruiker is. Ook voert de GR voor een aantal applicaties het functioneel beheer uit en beheert ze de Gegevensmakelaar voor de gemeenten. Deze en mogelijk andere bijzondere zaken moeten met voldoende aandacht voor informatieveiligheid en privacy worden vastgelegd in een of meer (verwerkers)overeenkomsten.

De GR rapporteert tenminste eenmaal per jaar aan de deelnemende gemeenten. De afsluitende jaarrapportage gaat vergezeld van een verklaring door een externe auditor (RE).

De Bevelandse gemeenten zijn in 2014 aangesloten bij de IBD. Vanuit de gemeenten zijn contactpersonen voor de IBD aangesteld. De rol van Algemene Contactpersoon Informatie-beveiliging (ACIB) voor de gemeenten is binnen de GR belegd. Dit omdat de ACIB met name te maken heeft met technische onderwerpen en uitvoering. De meer inhoudelijke en beleidsmatige contacten lopen via de Vertrouwde Contact Contactpersoon Informatiebeveiliging (VCIB).

Om de samenhang in informatieveiligheid tussen de deelnemende gemeenten en de GR te waarborgen is een deelnemersoverleg informatiebeveiliging ingesteld. De CISO van de GR is secretaris van dit overleg.

3.6 ICT crisisbeheersing en landelijke samenwerking

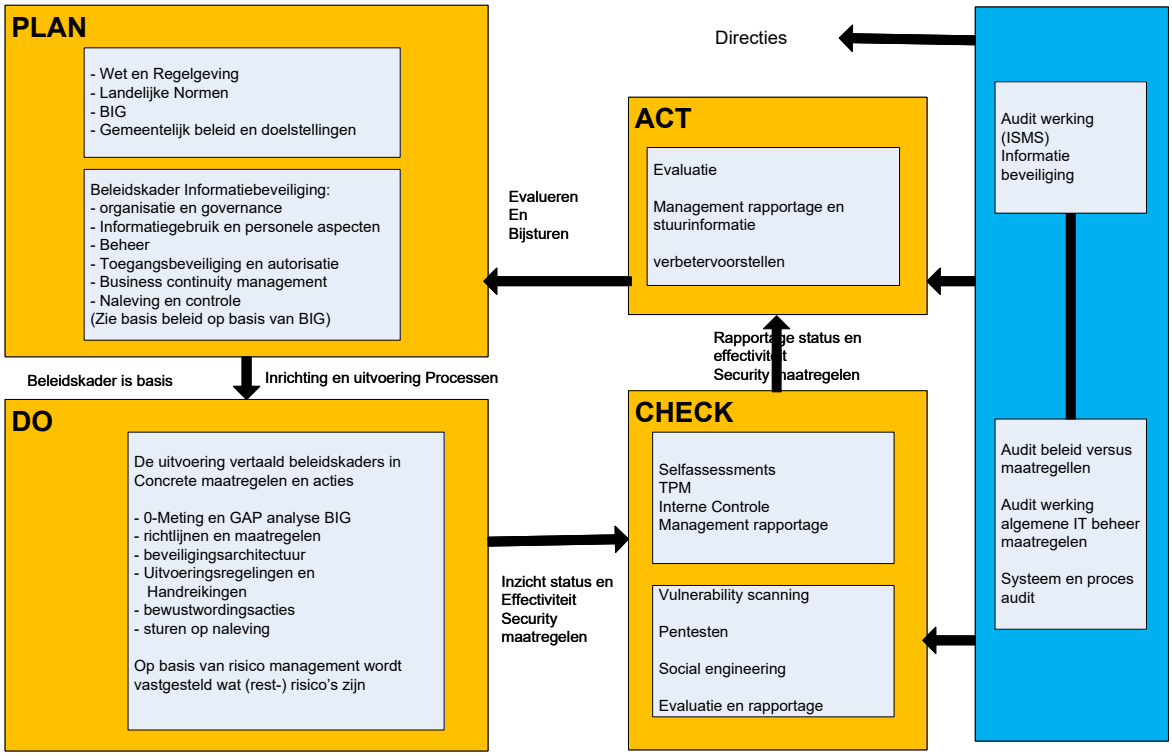
De basislijn voor rapportage en escalaties is Security verantwoordelijke naar CISO naar Directie.

Voor interne crisisbeheersing is er een crisisteam geïnstalleerd. Dit crisisteam bestaat in ieder geval uit de directie, de CISO en de overige leden van de werkgroep informatieveiligheid. Op basis van de situatie wordt het crisisteam uitgebreid met de betrokken afdelingshoofden en/of de CISO's van de eventueel betrokken deelnemende gemeenten. De werkwijze dient te zijn vastgelegd.

De gemeenschappelijke regeling GR de Bevelanden participeert in allerlei landelijke platforms en onderhoudt o.a. contacten met de Informatiebeveiligingsdienst Gemeenten (IBD).

3.7 PDCA cyclus

Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het management systeem van informatiebeveiliging (ISO 27001). Deze kwaliteitscyclus is in onderstaande figuur weergegeven.



Figuur 2: Information Security Management System

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

3.8 Informatiebeveiligingsbeleid en het informatiebeveiligingsplan

Deze beleidsnota wordt door middel van een jaarlijks informatiebeveiligingsplan geoperationaliseerd. Dit betekent dat de concrete uitvoering van deze beleidsnota plaatsvindt door middel van het implementeren van informatiebeveiligingsmaatregelen die worden beschreven in het informatiebeveiligingsplan. Het eerste informatiebeveiligingsplan wordt gebaseerd op de uitkomsten van een GAP-analyse. De deelnemende gemeenten en de GR hebben deze GAP-analyse in 2016 gezamenlijk uitgevoerd. Op basis hiervan kan worden vastgesteld waar onze organisatie staat ten opzichte van de tactische Baseline Informatiebeveiliging Nederlandse Gemeenten. In deze tactische baseline staan 303 beheersmaatregelen op het gebied van informatiebeveiliging die kunnen worden uitgevoerd.
In het eerste informatiebeveiligingsplan wordt, met behulp van de uitkomsten van de GAP-analyse, beschreven welke maatregelen geïmplementeerd moeten worden maar ook welke maatregelen niet geïmplementeerd worden en waarom (pas toe of leg uit principe). Er wordt beschreven op welke manier de maatregelen geïmplementeerd moeten worden en door wie (planning). Daarnaast neemt de CISO de jaarplanning op het gebied van informatieveiligheid op in het jaarlijkse Informatiebeveiligingsplan.
Jaarlijkse toetsen wij waar we staan ten opzichte van de 303 maatregelen uit de BIG.en actualiseren op basis daarvan jaarlijks het Informatiebeveiligingsplan. Het informatiebeveiligingsplan wordt tijdens de jaarlijkse evaluatie over de uitvoering van het informatiebeveiligingsbeleid en –plan door de directie ter vaststelling aangeboden aan het Dagelijks Bestuur en aan de colleges van de deelnemende gemeenten. Bij het opstellen en evalueren wordt intensief samengewerkt met de CISO's van de deelnemers.
Indien van toepassing worden activiteiten uit het informatiebeveiligingsplan verder uitgewerkt in afzonderlijke projectplannen.

3.9 Benodigde middelen

De middelen voor jaarlijks terugkerende kosten die voortvloeien door het uitvoeren van het Informatiebeveiligingsplan zijn in de begroting opgenomen. Het betreft hier kosten die wij hebben voor de uitvoering van verplichte audits zoals de SUWInet-audit en de jaarlijkse uitwijktest. De kosten van de DigiD-audits lopen nu nog via de gemeenten. Voor de uitvoering van specifieke maatregelen waarbij software moet worden aangeschaft, wordt via het informatiebeleidsplan geld gevraagd.

3.10 SUWInet

De GR gebruikt SUWInet bij het uitvoeren van taken op het gebied van Werk, Inkomen en Zorg. De GR moet zorgen dat wordt voldaan aan alle wettelijke vereisten die hierbij gelden. Conform het verantwoordingsbeleid van de uitvoeringsorganisatie BKWI (Bureau Keteninformatisering Werk & Inkomen) zijn de gemeenten altijd verantwoordelijk voor het gebruik. Dit betekent dat de GR aan de gemeenten verantwoording moet afleggen over het gebruik en het toegepaste beleid. In het beleid zijn de navolgende onderdelen geregeld.

- De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van SUWInet gegevens, applicaties, processen en infrastructuur zijn beschreven en duidelijk en gescheiden zijn belegd. Operationeel beheer, functioneel beheer, technisch beheer, aansturing ICT-leveranciers, autorisatiebeheer zijn belegd.

- Security officer SUWInet beheert en beheerst de beveiligingsprocedures en -maatregelen in het kader van SUWInet zodanig dat de beveiliging van SUWInet overeenkomstig wettelijke eisen is geïmplementeerd.

- Security officer SUWInet bevordert en adviseert over de beveiliging van SUWInet en verzorgt rapportages over de status en controleert dat de beveiliging van de SUWInet maatregelen wordt nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van SUWInet.

- Security officer SUWInet rapporteert rechtstreeks aan het hoogste management.

- Het beveiligingsbeleid/plan moet aantoonbaar centraal beschikbaar zijn voor alle gebruikers. Bijvoorbeeld beschikbaar op intranet of op de afdelings-/organisatieschijf. Het uitdragen van het beleid/plan moet niet alleen onder de direct bij de beveiliging betrokken medewerkers plaatsvinden, maar bij alle mensen in de organisatie die SUWInet gebruiken.

- Een adequaat ingerichte organisatie is een belangrijke voorwaarde voor het realiseren van een voldoende beveiligingsniveau voor SUWInet. Het gaat dan met name over functiescheiding. Zo zullen in principe de functies gebruik van SUWInet, beheer van autorisaties SUWInet, controle op het gebruik van SUWInet en beslissen over wie welke functies krijgt in SUWInet gescheiden moeten zijn. Door middel van functiescheiding worden risico's beperkt. Wanneer functiescheiding niet of onvoldoende is geïmplementeerd verhoogt dit de kans op oneigenlijk gebruik en/of misbruik zonder dat dit wordt ontdekt.

- De diverse functies noodzakelijk voor SUWInet moeten schriftelijk zijn vastgelegd, of er een heldere overweging ten grondslag ligt aan de toedeling van taken en of er functiescheiding is toegepast. Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken. Er wordt met name gekeken naar vier gescheiden functies. Beoordeeld wordt of minimaal de volgende functies bij verschillende personen zijn belegd:
    - uitvoering van taken (het gebruik van SUWInet zoals door de klantmanager);
    - beheer van autorisaties (toegang verlenen tot SUWInet, de applicatiebeheerder van SUWInet);
    - kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van SUWInet, bijvoorbeeld de security officer SUWInet);
    - management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik SUWInet).

Veel gebruikte afkortingen

ACIB	Algemeen
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie adressen en gebouwen
BGT	Basisregistratie grootschalige topografie
BIG	Baseline Informatiebeveiliging Gemeenten
BRP	Basisregistratie persoonsgegevens
BSN	Burgerservicenummer
CIO	Chief Information Officer
CISO	Chief of Corporate Information Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
GR	Gemeenschappelijke Regeling Samenwerking de Bevelanden
IBD	Informatiebeveiligingsdienst Gemeenten
ICT	(afdeling) Informatie- en communicatietechnologie
P&O	Afdeling Personeel en Organisatie
PDCA	Plan, Do, Check, Act
PUN	paspoort uitvoeringsregeling
SMART	Specifiek, meetbaar, aanvaardbaar, realistisch en tijdgebonden
SUWI	wet Structuur Uitvoering Werk en Inkomen
VCIB	Vertrouwd
Wbp	Wet bescherming persoonsgegevens
WIZ	Afdeling Werk Inkomen en Zorg