gemeenschappelijke regeling DE BEVELANDEN

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 416
19 maart 2024

Officiële uitgave van de gemeenschappelijke regeling Samenwerking De Bevelanden

Strategisch informatiebeveiligings- en privacybeleid GR 2023-2026

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P beleid) voor de jaren 2023 tot en met 2026 en vervangt het in 2020 vastgestelde 'Strategisch Informatiebeveiligingsbeleid Gemeenschappelijke Regeling Samenwerking de Bevelanden 2020-2023' en het Privacybeleid uit hetzelfde jaar.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.
Met dit 'Strategisch Informatiebeveiligingsbeleid 2023-2026' zet de Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR) een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de GR te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens.
De Gemeenschappelijke Regeling samenwerking De Bevelanden (GR) is een openbaar lichaam en rechtspersoon. De GR is een samenwerking tussen de gemeenten Borsele, Goes, Kapelle, Noord-Beveland en Reimerswaal. De GR voert HRM- en ICT-taken uit voor de eigen organisatie en voor de deelnemende gemeenten. Daarnaast de taken op het gebied van Werk, Inkomen en Zorg (WIZ) voor de vijf deelnemende gemeenten. De HRM-taken zijn gemandateerd. De ICT- en WIZ-taken worden uitgevoerd op basis van delegatie. In het geval van delegatie wordt de verantwoordelijkheid voor de betreffende taken overgedragen. In het geval van mandaat worden de taken namens de aangesloten partijen uitgevoerd en blijven deze zelf verantwoordelijk.
Omdat de GR een aantal taken uitvoert voor zes organisaties is het gewenst en in veel gevallen zelfs noodzakelijk, dat voor de GR op het gebied van informatiebeveiliging dezelfde regels gelden als voor de deelnemende gemeenten. Daarom wordt bij het opstellen van beleidsdocumenten en werkinstructies op tactisch en operationeel niveau aansluiting gezocht bij en afstemming gemaakt met het beleid van de deelnemende gemeenten.

Artikel 1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligings- en privacy plan (vastgesteld door de directeur) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teammanagers, de CISO, de privacy functionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de Informatiebeveiligingsdienst voor gemeenten(IBD), en de uitkomsten van risicoanalyses en DPIA's en de uitkomsten van ENSIA bij de deelnemende gemeenten. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.
1.1 Informatiebeveiliging
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de GR en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.
Omdat de GR ook HRM en ICT-taken uitvoert voor de deelnemende gemeenten 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. Tactische en operationele aspecten van informatieveiligheid worden daarom in nauw overleg met de deelnemende gemeenten opgesteld en zoveel mogelijk geüniformeerd.
1.2 Privacy & Gegevensbescherming (AVG)
De GR werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de GR voor het goed kunnen uitvoeren van de (wettelijke) taken. Het gaat hierbij om taken in het sociaal domein, ICT en personeelszaken. Voor de gemeenten zijn dit onder andere het openbare orde en veiligheidsdomein en burgerzaken. Om als GR deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben overheden een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de GR zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.3 Ambitie en visie van de GR op het gebied van informatieveiligheid en privacy

Informatiebeveiliging en privacybescherming moeten eraan bijdragen dat de Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR) haar ambities, doelen en resultaten realiseert. Informatiebeveiliging is om die reden geen doel op zichzelf, en dient in samenhang gebracht te worden met de doelen van de organisatie. De GR zorgt ervoor dat zijzelf en de deelnemende gemeenten tenminste kunnen voldoen aan de wettelijke verplichtingen op het gebied van informatieveiligheid en privacybescherming.

De komende jaren zet de GR in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Dezelfde inzet geldt ook de dienstverlening aan de deelnemende gemeenten bij het realiseren van hun informatieveiligheid. Een goede privacy boekhouding en een betrouwbare informatievoorziening zijn 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 eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de GR.

Op alle terreinen wordt tactisch beleid opgesteld. Ook worden maatregelen getroffen zodat bij alle BIO-controls beoordeeld kan worden of we aan de eisen voldoen. Binnen de teams moet duidelijk zijn welke eisen er gelden op het gebied van Beschikbaarheid, Integriteit (juistheid) en Vertrouwelijkheid van de gegevens en processen. Vanaf 2023 wordt verder gewerkt aan het invoeren van interne periodieke controles en de Plan-Do-Check-Act cyclus, waarmee een continu proces van beoordelingen en verbeteringen wordt gerealiseerd.

2. Strategisch beleid2.1 Doel

Het doel van deze beleidsnota is het presenteren van het ‘Strategisch Informatiebeveiligings- en privacy beleid voor de jaren 2023 tot en met 2026’. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligings- en privacyplan (IB&P-Plan). Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het IB&P beleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teammanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR) is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

2.2.3 De Wpg

De GR heeft BOA’s in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (Wpg). Hiervoor moet de GR beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

2.2.4 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging (zie bijlage A) zijn een bestuurlijke aanvulling op het normenkader[1] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.

8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

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

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het 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 het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.6 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

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

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.
Voor de ondersteuning van overheden bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen.
Binnen de in de GR deelnemende gemeenten wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Voor zover de GR op deze onderdelen taken uitvoert voor de gemeenten geldt het beveiligingsbeleid van de GR ook voor de bescherming van PA. Voor de bescherming van PA gebruikt de GR de Cybersecurity Implementatie Richtlijn (CSIR).

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau.
Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Dit beleid wordt vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligings- en privacyplan'.

2.5 Scope informatiebeveiliging en privacy

De scope van deze beleidsnota omvat alle processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de GR, de deelnemende gemeenten en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten geformuleerd.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

1. Alle informatie en informatiesystemen zijn van belang voor de GR, bepaalde informatie is van vitaal en kritiek belang. Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle informatiesystemen ongeacht waar deze worden gehost.
2. Alle Proces Automatiseringssystemen (PA) die binnen gemeentelijke gebouwen en in de publieke ruimte van de Bevelandse gemeenten worden gebruikt, die van de gemeenten zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen en waarvoor de GR (een deel van) het beheer uitvoert.

2.6 Uitgangspunten

Het bestuur, de directeur en het teammanagement spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de GR heeft, de (privacy) risico's die de GR hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor

informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
Het gehele management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB&P beleid van en voor de hele GR. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het IB&P beleid is in lijn met het algemene beleid van de GR en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het IB&P beleid zijn:

1. Het managen van de informatiebeveiliging.
2. Adequate bescherming van bedrijfsmiddelen en (persoons)gegevens.
3. Het toepassen van dataminimalisatie.
4. Het minimaliseren van risico's van menselijk gedrag.
5. Het voorkomen van ongeautoriseerde toegang.
6. Het garanderen van correcte en veilige informatievoorzieningen.
7. Het beheersen van de toegang tot informatiesystemen.
8. Het waarborgen van veilige informatiesystemen.
9. Het adequaat reageren op incidenten.
10. Het beschermen van (kritieke) bedrijfsprocessen.
11 Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
12 Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
13 Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

1. De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR) hebben een interne eigenaar die de vertrouwelijkheid, privacyeisen 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.
2. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met het IB&P plan het fundament onder een betrouwbare informatievoorziening en privacy bescherming. In het IB&P plan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.
3. Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
4. De GR stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid.
5. Regels en verantwoordelijkheden voor het IB&P beleid moeten worden vastgelegd en vastgesteld.
6. Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
7. Het borgen van privacy in de uitvoering van processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.3 IB&P governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

1. Het Dagelijks Bestuur stelt als eindverantwoordelijke het strategisch IB&P beleid vast.
2. De directeur stelt jaarlijks het IB&P plan vast.
3. De directeur is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
4. Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
5. De directeur 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

(persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid vallen.

6. De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directeur, voorafgaand aan de P&C-gesprekken.
7. De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het Dagelijks Bestuur over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
8. De directeur en de teammanagers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de Functionaris voor Gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
9. Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
10. De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
11 De teammanagers zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
12 De teammanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
13 Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de GR. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de GR en het behalen van de doelen die zijn gesteld.
14 Alle medewerkers van de GR worden getraind in het gebruik van beveiligingsprocedures.
15 Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
16 Medewerkers moeten verantwoord om gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
17 Teammanagers moeten dienen erop toezien 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.
18 De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers voeren quickscans informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG uit om deze risico-afwegingen te kunnen maken.
19 Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.6.4 Randvoorwaarden
Belangrijke randvoorwaarden zijn:

1. De informatiebeveiliging en privacy eisen maken deel uit van afspraken met de deelnemende gemeenten, ketenpartners en leveranciers en worden periodiek geëvalueerd/gecontroleerd.
2. Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie moeten actief worden bevorderd en geborgd.
3. Jaarlijks wordt een IB&P plan opgesteld onder leiding van de directeur, gebaseerd op:
    1. Dit IB&P beleid;
    2. Interne rapporten van CISO en FG;
    3. Andere audit resultaten;
    4. Het dreigingsbeeld gemeenten van de IBD;
    5. Uitkomsten risicoanalyses en DPIA's
    6. De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

1. Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken & verantwoordelijkheden
In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense'). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO, Security Officer, Privacy Officer) ondersteunt,

adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directeur

De directeur zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. De directeur zorgt dat de teammanagers zich verantwoorden over de beveiliging en bescherming van de privacy van (persoons)gegevens of andere informatie die onder hen berust. De directeur zorgt dat de eindverantwoordelijke portefeuillehouders binnen het bestuur gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het bestuur zich ook verantwoorden naar de deelnemende gemeenten.
De directeur stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directeur draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO van de GR. De directeur autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de Gemeenschappelijke Regeling Samenwerking de Bevelanden gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: teammanagers

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, (persoons)gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan de directeur over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het teamoverleg.
Taken van de teammanagers in het kader van informatiebeveiliging en privacybescherming zijn:

1. Het leveren van input voor wijzigingen op maatregelen en procedures.
2. Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is.
3. Het binnen het eigen team uitdragen van het IB&P beleid, de daaraan gerelateerde procedures.
4. Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
5. Het vroegtijdig betrekken van CISO en PO bij nieuwe of gewijzigde processen.
6. Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
7. Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen.

3.3 Controle en verantwoording

Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het bestuur van de Gemeenschappelijke Regeling Samenwerking de Bevelanden (GR). De bestuurders en directeur van de GR gaan werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het tonen van voorbeeldgedrag en het vragen om informatie.
De directeur is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan het Dagelijks Bestuur. De directeur rapporteert daarnaast over de mate waarin invulling is gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

ENSIA

Gemeenten verantwoorden zich over informatiebeveiliging middels de ENSIA-systematiek. Die verantwoording gaat naar de gemeenteraad en naar enkele ministeries. Omdat de GR taken uitvoert voor de Bevelandse gemeenten, moet de GR ieder jaar een aantal antwoorden verstrekken aan de gemeentelijke ENSIA-coördinatoren. De teammanagers ICT en HRM en de proceseigenaar Suwinet leveren de gemeenten alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.
De verantwoording over de informatiebeveiliging en privacybescherming komt in het jaarverslag tot uitdrukking in de paragraaf Informatiebeveiliging en privacy. In die paragraaf geeft het bestuur aan in hoeverre de GR voldoet aan de afspraken die gemaakt zijn voor Informatiebeveiliging en wettelijke eisen zoals uit de AVG. Ook worden de eventuele verbetermaatregelen vermeld die de GR gaat treffen.
Middels deze verantwoording worden het bestuur van de GR en de deelnemende gemeenten geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de GR informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van de inwoners van de Bevelanden adequaat te beschermen.
Vastgesteld op : [datum] door het Dagelijks bestuur van de Gemeenschappelijke Regeling Samenwerking de Bevelanden
[Ondertekening]

gemeenschappelijke regeling
DE BEVELANDEN

Veel gebruikte afkortingen

ACIB	Algemeen Contactpersoon Informatiebeveiliging (t.b.v. IBD)
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie adressen en gebouwen
BGT	Basisregistratie grootschalige topografie
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basisregistratie persoonsgegevens
BSN	Burgerservicenummer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
GR	Gemeenschappelijke Regeling Samenwerking de Bevelanden
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	(team) Informatie- en communicatietechnologie
NCSC	Nationaal Cyber Security Centrum
PDCA	Plan, Do, Check, Act
PO	Privacy Officer
PUN	paspoort uitvoeringsregeling
SMART	Specifiek, meetbaar, aanvaardbaar, realistisch en tijdgebonden
SO	Security Officer
SUWI	wet Structuur Uitvoering Werk en Inkomen
VCIB	Vertrouwd Contactpersoon Informatiebeveiliging (t.b.v. IBD)
WIZ	Werk, Inkomen en Zorg
Wpg	Wet politiegegevens

Bijlage A: De 10 bestuurlijke principes voor informatiebeveiliging
[1] Deze principes zijn gelijk met de BIO van kracht geworden, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG).
[2] *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

Namens deze,
Drs. M.C. Noordhoek, de directeur
Drs. M. Fränzel MSc , de voorzitter