Strategisch Informatiebeveiligingsbeleid van de Gemeenschappelijke Regeling Samenwerking de Bevelanden

2020 tot 2023

Gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO)

Versiebeheer

Het versiebeheer van dit document ligt bij de CISO.

Beheersmaatregel:	5.1.1.1
Documentversie:	6 april 2020
Documentnaam:	Informatiebeveiligingbeleid GR BIO van 2020 tot 2023 v04.docx

Versiebeheer

Versie	Beschrijving	Datum	Status
0.1	1e concept	30-09-2019	Concept
0.2	Aanpassingen op basis van opmerkingen CISO's	28-11-2019	Concept
0.3	Aanpassingen na opmerkingen teamleider	09-12-2019	Concept
0.4	Extra aanvulling na concept-advies	20-03-2020	Concept
1.0	Concept tbv de vaststelling door het Dagelijks Bestuur	20-03-2020	Concept
1.0	Vastgesteld door het Dagelijks Bestuur	06-04-2020	Definitief
1.0			

Inhoud

1 Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot 2023 en vervangt het in 2018 vastgestelde ‘Strategisch Informatiebeveiligingsbeleid GR de Bevelanden’. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit ‘Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023’ 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) zie bijlage A. De principes zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage B.

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 op basis van mandaat ICT- en P&O-taken uit voor de eigen organisatie en voor de deelnemende gemeenten. Daarnaast, op basis van delegatie, de taken op het gebied van Werk, Inkomen en Zorg voor de vijf deelnemende gemeenten. 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.

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 Informatiebeveiligingsplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers en CISO’s van zowel de GR als de deelnemende gemeenten, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA bij de deelnemende gemeenten. In het Informatiebeveiligingsplan 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.

1.2 Wat is 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 persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de GR. Met het informatie-beveiligingsbeleid wordt de informatievoorziening gedurende de hele levenscyclus van informatie-systemen geborgd, 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, inwoners, gasten, bezoekers en externe relaties.

Omdat de GR ook P&O 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.

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

De GR zorgt ervoor dat zijzelf en de deelnemende gemeenten tenminste kunnen voldoen aan de wettelijke verplichtingen op het gebied van informatieveiligheid. De GR zet 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.

Eind 2020 is in ieder geval op alle terreinen tactisch beleid opgesteld. Ook zijn dan maatregelen getroffen zodat bij alle BIO-controls beoordeeld kan worden of we aan de eisen voldoen. Binnen de afdelingen moet duidelijk zijn welke eisen er gelden op het gebied van Beschikbaarheid, Integriteit (juistheid) en Vertrouwelijkheid van de gegevens en processen. Vanaf 2021 wordt jaarlijks een audit uitgevoerd, zodat aan de deelnemende gemeenten een verklaring kan worden verstrekt, waaruit blijkt de informatieveiligheid op orde is. Vanaf 2022 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.

Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de GR en de deelnemende gemeenten, en de basis voor het beschermen van rechten van personen en organisaties. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

2 Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2020 tot 2023'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG (Baseline Informatiebeveiliging Gemeenten). Dat wil zeggen dat de afdelingsmanagers 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 10 bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes voor informatiebeveiliging[1] (zie bijlage B) zijn een bestuurlijke aanvulling op het normenkader 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 de deelnemende gemeenten, inwoners, ondernemers en partners van de organisatie. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.3 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.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De GR kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. In dit systeem worden ook incidenten bij de deelnemende gemeenten vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en biedt de mogelijkheid om incidenten uit het verleden ook nadrukkelijk te benutten als input bij het actualiseren van het beleid.

[1] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

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 organisaties bij het formuleren en realiseren van hun informatie-beveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatie-beveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.
De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

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 op tactisch en operationeel niveau.
Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid wordt vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven ‘Informatiebeveiligingsplan’.

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, 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 BRP, PNIK 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). Deze worden in aanvullende documenten geformuleerd.

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

2.6 Uitgangspunten

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening hebben, de risico’s die men loopt en welke van deze risico’s onacceptabel 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 gehele management van de GR geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie.

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 van de GR en de relevante landelijke en Europese wet- en regelgeving.

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

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde 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.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de GR en de deelnemende gemeenten, bepaalde informatie is van vitaal en kritiek belang. Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging binnen de GR.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de GR hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. Ook van de deelnemende gemeenten wordt verwacht dat alle door hen gebruikte informatiesystemen een eigenaar hebben. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- De verantwoordelijkheid voor de beveiliging van de technische omgeving, die door de GR wordt beheerd, inclusief de bestanden die zich daarop bevinden, ligt bij het hoofd van de afdeling ICT.
- 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.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- De GR stelt de benodigde mensen en middelen beschikbaar om 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.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het Dagelijks Bestuur stelt, 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 afdelingsmanagers en ziet erop toe dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen. 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.
- Alle medewerkers van de GR worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Afdelingsmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO en vastgesteld door de directie. Het informatiebeveiligingsplan wordt gebaseerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA) bij de deelnemende gemeenten;
  - het dreigingsbeeld gemeenten van de IBD;
  - de door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn;
  - door het Deelnemersoverleg Informatiebeveiliging (DIB) ingebrachte onderwerpen. Het DIB is een periodiek overleg van de CISO’s van de deelnemende gemeenten en de GR.

3 Organisatie, taken & verantwoordelijkheden

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 verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het Dagelijks Bestuur gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het Dagelijks Bestuur zich ook verantwoorden naar het Algemeen Bestuur en de deelnemende gemeenten.

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

3.2 Uitvoering: afdelingsmanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingsmanagers. 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, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Afdelingsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen en/of teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in een bedrijfsvoeringsoverleg. Voorbereiding en coördinatie van het bedrijfsvoeringsoverleg ligt bij de CISO.

Taken van de afdelingsmanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreken van beveiligingsincidenten en de consequenties die deze moeten hebben voor beleid en maatregelen.

3.3 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het Dagelijks Bestuur van de GR. De bestuurders en directeur van de GR zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.3.1 ENSIA

Gemeenten verantwoorden zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat gemeenten een ENSIA-coördinator aanwijzen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingsmanagers. De afdelingsmanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

Omdat de GR ICT taken uitvoert voor de gemeenten, moet de GR jaarlijks tijdig de relevante informatie verstrekken aan de gemeenten, zodat de gemeenten de vragen in de ENSIA-vragenlijsten kunnen beantwoorden.

De verantwoording over de informatiebeveiliging komt bij gemeenten in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad. De GR zal zich op vergelijkbare wijze in het jaarverslag verantwoorden over Informatiebeveiliging.

Middels deze verantwoording worden het Algemeen Bestuur van de GR en de raden van de deelnemende gemeenten geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de GR informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie, van zowel de deelnemende gemeenten als zichzelf, adequaat te beschermen.

Op 6 april 2020 vastgesteld door het dagelijks bestuur van de Gemeenschappelijke Regeling samenwerking De Bevelanden

P.M.C. van den Beemt,

directeur

Veel gebruikte afkortingen

ACIB	Algemeen Contactpersoon Informatiebeveiliging (tbv IBD)
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie adressen en gebouwen
BGT	Basisregistratie grootschalige topografie
BIG	Baseline Informatiebeveiliging Gemeenten
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 Gemeenten
ICT	(afdeling) Informatie- en communicatietechnologie
NCSC	Nationaal Cyber Security Centrum
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 Contactpersoon Informatiebeveiliging (tbv IBD
WIZ	Afdeling Werk, Inkomen en Zorg

Bijlage A: Baseline Informatiebeveiliging Overheid (versie 1.03)

Bijlage B: De 10 bestuurlijke principes voor informatiebeveiliging