GEMEENTE ZEVENAAR

GEMEENTEBLAD

Officiële uitgave van de gemeente Zevenaar

Nr. 164307

15 april

2025

Strategisch Informatiebeveiliging- en privacybeleid

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P beleid). Het in 2021 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2021 - 2023' wordt hiermee ingetrokken. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'strategisch informatiebeveiligings- en privacy beleid' vervolgt de gemeente haar koers, om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit beleid is de ISO-norm 27001/2 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO)[1]. De beschreven principes in de beleidsnota zijn gebaseerd op de 10 principes voor informatiebeveiliging[2] zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens.

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 gemeentelijk Informatiebeveiligings- en privacy plan (vastgesteld door de directie) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdeling/domeinmanagers, de CISO, de privacy functionaris(sen), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's. 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

1.2 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 gemeente 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.

1.3 Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

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

1.4 Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy

Digitalisering zit steeds meer in het hart van onze organisaties. De maatschappelijke relevantie van de lokale overheid richting inwoners en ondernemers is sterk afhankelijk van de inzet van digitale middelen. Daarom zullen wij de komende jaren hierin moeten (blijven) investeren. Doen wij dit niet dan vormt dit

1) https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
2) https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

een rechtstreekse bedreiging voor onze bedrijfsvoering en (publieke) dienstverlening en maatschappelijke waarde van onze organisatie.

Voor de periode vanaf 2023 is daarom ook een visiedocument[3] opgesteld om hier samen met gemeente Duiven, Westervoort, Zevenaar en de Samenwerking De Liemers (RID en RSD) invulling aan te geven. Het visie-deel richt zich op wat er in op het gebied van I&A moet gebeuren en wat daarin voor ons prioriteit heeft en waarom. Het strategie-deel richt zich op hoe we uitvoering willen geven aan deze 'I&A-agenda' en wat we daarin van elkaar en van de samenwerking verwachten. In deze visie zijn ook de speerpunten voor informatiebeveiliging en privacy (IB&P) benoemd en worden hieronder kort samengevat:

1.4.1 Basis op orde krijgen

Voor informatiebeveiliging en privacy is het van groot belang om de fundamenten voor deze onderdelen te borgen in de organisatie. Een passende beheersing van informatiebeveiligings- en privacyrisico's is randvoorwaardelijk voor het bereiken van de strategische organisatiedoelen. Door de komende periode verder te investeren in een stabiele fundering wordt de kans op incidenten (storingen, hacks, onderbrekingen van de dienstverlening, datalekken etc.) verkleind.

1.4.2 Voldoen aan wet- & regelgeving

Voor informatiebeveiliging zijn onder andere de volgende wet- en regelgeving belangrijk:

Baseline Informatiebeveiliging Overheid (BIO), sinds 2019
Er is een volwassenheidsmodel digitale weerbaarheid dat stelt dat we op een schaal van 0-5 een 3 moeten scoren om 'in control' te zijn. Het uitgangspunt voor de BIO is risicomanagement, waarbij het doen van risico-inschattingen en het bepalen van de organisatie-acceptatienorm leidend zijn.

Algemene Verordening Gegevensbescherming (AVG), sinds 2018
De Algemene Verordening Gegevensbescherming (AVG) is de Europese privacywetgeving, die sinds 25 mei 2018 in de hele Europese Unie (EU) geldt. De AVG gaat over de bescherming van persoonsgegevens. Uitgangspunt is dat mensen meer privacy rechten hebben, organisaties meer verantwoordelijkheden hebben en de toezichthouder meer bevoegdheden heeft.
Hiernaast is vanaf 2024 de volgende wetgeving van toepassing:

Network and Information Security (NIS2)
Eind 2022 is deze richtlijn in Europa vastgesteld. De lidstaten hebben tot eind 2024 de tijd om deze richtlijn op te nemen in nationale wetgeving. Hierbij ligt de nadruk op de zorgplicht waarbij elke organisatie verplicht is risicobeoordelingen uit te voeren en passende maatregelen te treffen.

1.4.3 Inzetten op digitale weerbaarheid

Digitalisering van de gemeentelijke diensten is niet meer weg te denken in de dienstverlening. Dit zorgt echter voor een afhankelijkheid van externe factoren (stroomvoorziening, leveranciers etc.). Door in te zetten op digitale weerbaarheid wordt er structureel aandacht besteed aan:

- inzicht hebben op cyberincidenten, -dreigingen en risico's en hoe hiermee om te gaan: Het is van belang om structureel te kunnen beschikken over betrouwbare informatie . Verder zijn er zogenaamde cyberdreigingen, -incidenten, -trends en kwetsbaarheden die periodiek worden bijgehouden en gedeeld met de organisatie(s), zodat we tot handelen over kunnen gaan.
- bescherming tegen digitale risico's: Het minimaliseren van negatieve effecten voor onze organisatie(s) en onze afnemers, toeleveranciers of anderen. Doel is het borgen van de bedrijfscontinuïteit en het behoud van de data.
- in staat zijn om adequaat te reageren, te herstellen en snel te leren op en van cyberincidenten en –crises: Periodieke oefeningen zijn voor de digitale weerbaarheid (net als het herhalen van brand- en BHV oefeningen) van cruciaal belang.

1.4.4 Inzetten op bewustwording (awareness)

Investeren in onze collega's is van cruciaal belang om informatiebeveiliging en privacy te kunnen borgen in onze organisatie(s). Hierop zetten we al in en we kunnen kennis en ervaring delen. Door periodiek verschillende onderdelen te trainen wordt de kans op incidenten en interrupties van de dienstverlening steeds kleiner (voorbeelden hiervan zijn naast trainingen , e-learnings, phishing testen, uitnodigen van sprekers, omgaan met nieuwe ontwikkelingen, etc.).

3) I&A-visie en -strategie 2023-2025 "Beter Samen"

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligings- en privacy beleid'. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligings- en privacyplan (IB&P-P). 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 informatiebeveiligingsbeleid 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 domeinmanagers 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 gemeente Zevenaar 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 gemeente heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (WPG). Hiervoor moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risicoinschatting, registratie en logging, meldplicht en documentatieplicht

2.2.4 De 10 principes voor informatiebeveiliging[4]

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op de 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 gemeentelijke 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 gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is informatiebeveiliging ook een onderwerp voor 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.

4) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

2.2.6 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd[5]. 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 27001:2012. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[6] 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 gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsafdelingen die zich met PA bezig houden.[7] Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR).[8]

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om een kader te geven en de basis te leggen voor de onderwerp specifieke beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks op te stellen 'Gemeentelijk Informatiebeveiligingsplan'. Input voor dit plan wordt verkregen van de team- en domeinmanagers, de CISO, het dreigingsbeeld van de IBD en uit uitkomsten van jaarlijkse Audits (ENSIA, themaonderzoeken, controle jaarrekening etc)

2.5 Scope informatiebeveiliging

De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente 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 gemeentelijke 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.

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.
- Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.

2.6 Uitgangspunten

Het bestuur, de directie en het (domein)afdelingsmanagement 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 gemeente heeft, de (privacy) risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management

5) Beveiligingsincidenten worden vastgelegd in Topdesk (RID) en gerapporteerd in de kwartaalrapportage
6) De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.
7) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
8) https://www.cert-wm.nl/csir

dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk 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 gemeente. 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 gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Belangrijkste elementen van informatiebeveiliging

De strategische doelen van het IB&P beleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- 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.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Zevenaar 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.
- Door periodieke controle, organisatiebrede 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 organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De gemeente 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.
- Regels en verantwoordelijkheden voor het IB&P beleid dienen te worden vastgelegd en vastgesteld.
- 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.
- Het borgen van privacy in de uitvoering van gemeentelijke 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:

- Het college van B en W stelt als eindverantwoordelijke het strategisch IB&P beleid vast.
- De directie stelt jaarlijks het IB&P plan vast.
- De directie is verantwoordelijk voor vaststellen en het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.

- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het door de gemeente aangewezen syste(e)m(en)
- De directie is verantwoordelijk voor het vragen om informatie bij de domeinmanagers en ziet erop toe dat de domeinmanagers adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen 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.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W 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.
- De directie en de domeinmanagers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de functionaris gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- 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.
- De domein- en teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De domein- en teammanagers zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De domeinmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- 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 gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Domein- en teammanagers 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. Domein- en teammanagers (laten) quickscans informatiebeveiliging uitvoeren op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's op basis van de AVG om deze risico-afwegingen te kunnen maken.
- 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:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB&P plan opgesteld, gebaseerd op:
    - Dit IB&P beleid;
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Andere audit resultaten;
    - het dreigingsbeeld gemeenten van de IBD;
    - Uitkomsten risico-analyses en DPIA's
    - De door de domeinmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

- 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 officers, PO) 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, hier zit ook de ENSIA coördinator.

Lines of Defence	Algemeen	Gemeente	Rol
	Raad van Commissarissen	Gemeenteraad	Toezicht
	Raad van Bestuur	College van B&W	Eindverantwoordelijk en toezicht
3e Lijn	• Interne auditfunctie	• Verbijzonderde interne controlefunctie • Concern control	Totaaloverzicht, aanvullende zekerheid over in control zijn
2e Lijn	• Controlling • Riskmanagement • Compliance • Kwaliteitsmanagement • Etc.	• Business control • Financial control • Dienst-/Sector-/Domeincontroller • Kwaliteitsmedewerker • Etc.	Ondersteunend en verantwoordelijk voor de infrastructuur, methodiek, richtlijnen etc.
1e Lijn	• Business management • Divisie-/unitmanagement	• Directie • Afdelingsmanager/-hoofd • Teammanager/-leider • Coördinator • Etc.	Primair verantwoordelijk voor goede interne beheersing (control)

3.1 Aansturing: algemeen directeur

De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een domeinmanager. De directie zorgt dat de domeinmanagers zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college 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 college zich ook verantwoorden naar de raad.

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

3.2 Uitvoering: domein- en teammanagers

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle domein- en 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. Domeinmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het bedrijfsvoeringsoverleg.

Taken van de domein- en teammanagers in het kader van informatiebeveiliging en privacybescherming zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- 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.
- Het binnen de eigen domein en afdeling uitdragen van het IB&P beleid, de daaraan gerelateerde procedures.

- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO en PO bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen.

3.2.1 Ondersteuning: Stuurgroep-Informatie, RID de Liemers, RID contactpersonen en Informatiebeveiligingsoverleg

De *Stuurgroep Informatie* adviseert de algemeen directeur over de strategische ontwikkeling van de bedrijfsinformatievoorziening en de inzet van de middelen daarvoor. Ze geeft namens de algemeen directeur invulling aan de sturende rol door besluitvorming voor te bereiden en toe te zien op de uitvoering hiervan. De informatiebeveiligingstaken die hieruit voortvloeien, kunnen door de algemeen directeur worden gedelegeerd naar de verantwoordelijk proceseigenaar, de CISO adviseert hierin.

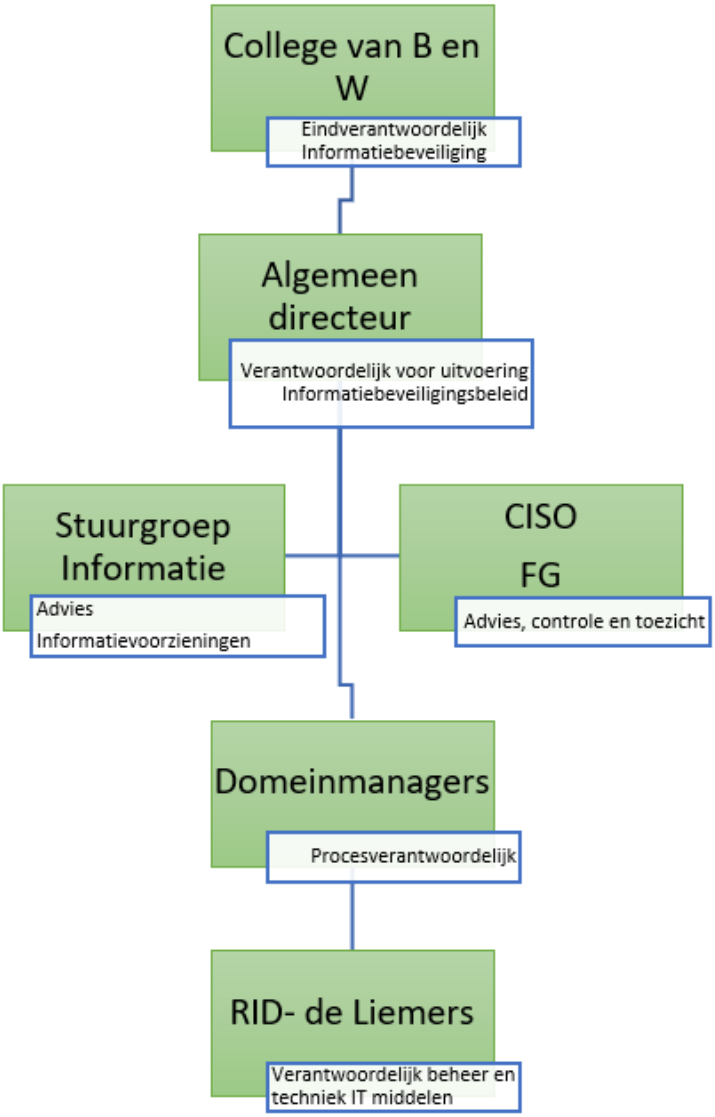
RID de Liemers [9] is verantwoordelijk voor het dagelijks beheer van technische informatiebeveiligingsaspecten zoals beschreven in de SLA en de Productiedienst Catalogus (PDC). De RID is net als de aangesloten gemeenten ook zelf verantwoordelijk om haar eigen informatiebeveiligingsbeleid in lijn met de BIO uit te voeren.

In het '*RID contactenpersonen overleg*' wordt de coördinatie van het projectportfolio van de Liemerse gemeenten, RID en RSD[10] Afgestemd. Activiteiten van Portfoliomanagement zijn het identificeren, prioriteren en accorderen van (beveiligings)projecten en het bijsturen binnen het projectportfolio

In het '*Informatiebeveiligingsoverleg SDL*' zitten de CISO's van de Liemerse gemeenten, RID, RSD en MGR[11]. In dit overleg worden de (gezamenlijk) beveiliging onderwerpen afgestemd zoals bijvoorbeeld lopende projecten, rapportages, incidentmeldingen of beleidsdocumenten.

Schematisch overzicht van rollen en verantwoordelijkheden

9) RID: Regionaal ICT en inkoop Dienstencentrum
10) RSD: Regionale Sociale Dienst de Liemers
11) MGR; Modulair Gemeenschappelijke Regeling



3.3 Controle en verantwoording

Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het bestuur van de gemeente Zevenaar. De bestuurders en directeuren van de gemeente zevenaar zullen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.3.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdeling/domeinmanagers. De domeinmanagers leveren 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 collegeverklaring Informatiebeveiliging en privacy. 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 en wettelijke eisen zoals uit de AVG. 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.

Via ENSIA verantwoordt de gemeente zich ook aan de stelselhouders voor DIGID/BAG/BGT/BRO/BRP/PUN en SUWI.

Middels deze verantwoording worden het bestuur van de gemeente Zevenaar en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Zevenaar informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.