INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie

Handreiking

Informatiebeveiligingsbeleid

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Handreiking beleid BIO

Versienummer

1.1

Versiedatum

Juli 2019

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

VNG Realisatie

Rechten en vrijwaring

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
0.8	02-02-2019	Initiële versie voor interne review
0.9	05-02-2019	Versie voor externe review
1.0	April 2019	Defintieve 1.0 versie
1.1	Juli 2019	Verwijzingen aangepast, kleine aanpassingen in lay-out

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is inzicht verschaffen in de opzet van informatiebeveiligingsbeleid voor de gemeente met voorbeelden hoe dat in de BIG en BIO te vinden is.

Doelgroep

Dit document is van belang voor informatiebeveiligers van de gemeente, de CISO, het management van de gemeente, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligingsbeleid van de gemeente

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

- Alle hoofdstukken met verwijzingen naar beleid en/of procedures.

Inhoudsopgave

1. Informatiebeveiligingsbeleid?

Deze handreiking is geschreven op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Overheid (BIO) die vanaf 1-1-2019 door gemeenten kunnen worden gebruikt. Binnen gemeenten worden - net als bij talrijke andere organisaties - vele soorten beleid gebruikt om aan te geven welke doelen bestuurders en managers willen bereiken rond bepaalde onderwerpen. Zo ook het informatiebeveiligingsbeleid. Gemeenten stellen hun informatiebeleid op conform de BIO. Sommige gemeenten maken geheel nieuw beleid, andere gebruiken daar bestaande templates voor. De geformuleerde beleidsdocumenten hebben als doel te beschrijven wat bestuur en management van de gemeente belangrijk vinden in het realiseren van de organisatiedoelen en het passend beheersen van informatiebeveiligingsrisico's. Als bestuur en management geen duidelijke richting aangeven in beleid, kan dat de realisatie van de gestelde doelen belemmeren. Alle informatiebeveiligingsbeleidsdocumenten worden periodiek geactualiseerd en het beleid van gemeenten is openbaar en toetsbaar.

Minimale onderwerpen in het informatiebeveiligingsbeleid
Welke onderwerpen moeten ten minste uitgewerkt worden in het informatiebeveiligingsbeleid1:

- De strategische uitgangspunten en randvoorwaarden die de gemeente hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op andere vormen van beleid binnen de organisatie.
- De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.
- De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers.
- De gemeenschappelijke betrouwbaarheidseisen in termen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en beveiligingsnormen die op de organisatie van toepassing zijn.
- De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd.
- De bevordering van het beveiligingsbewustzijn.

Het informatiebeveiligingsbeleid is de kapstok voor aanvullend beleid, procedures en standaarden binnen de gemeente of het samenwerkingsverband. Door het informatiebeveiligingsbeleid te ondertekenen laten bestuur en management van de gemeente zien dat men dit belangrijk vindt.

Doelstellingen van informatiebeveiligingsbeleid
De hoofddoelstelling van informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente; er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en de middelen waarmee dit beleid moet worden vormgegeven. Het informatiebeveiligingsbeleid is tevens de basis voor het inrichten van een procesgerichte benadering van informatiebeveiliging, ook wel het Information Security Management System (ISMS) genaamd. Dit proces hanteert een Plan Do Check Act Cyclus (PDCA) en moet aansluiten bij de Planning en Control (P&C) Cyclus van de gemeente.

1 Zie ook VIR en maatregel 5.1.1.1 uit de BIO

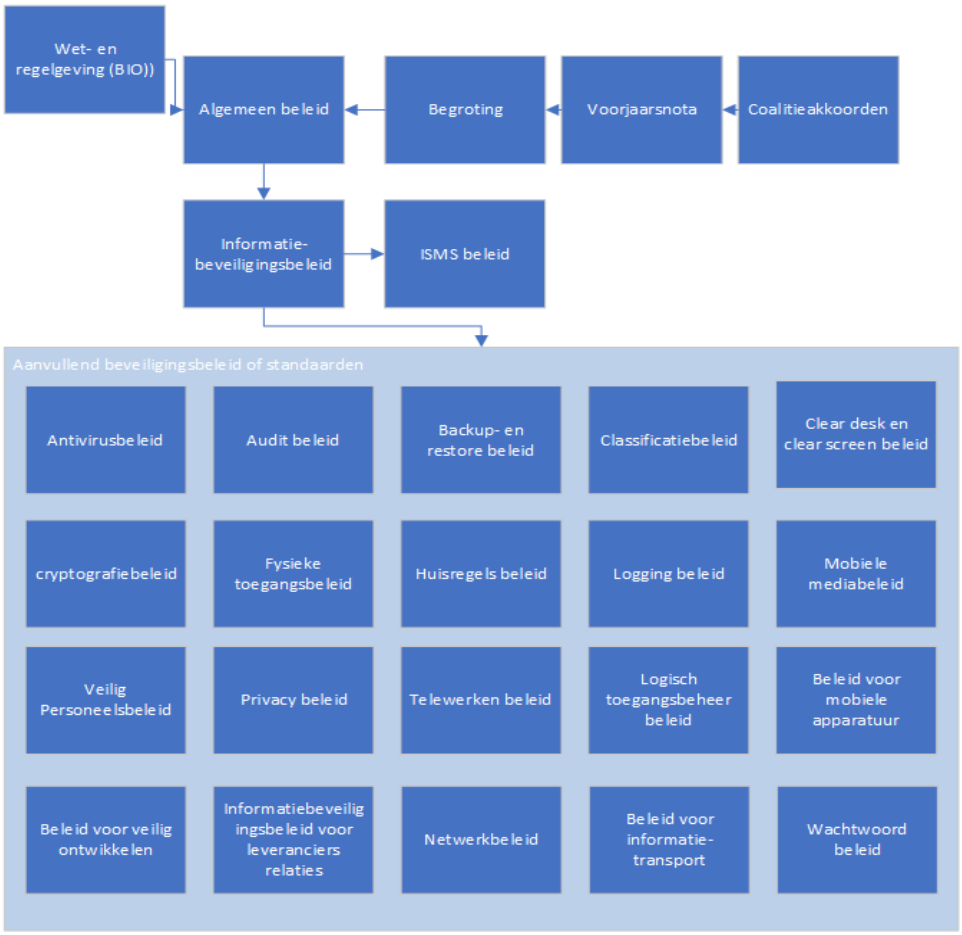
2. Wat is goed beleid?

Wanneer is beleid goed genoeg, hoe weet je dat je niks mist, wanneer is het compleet genoeg? Het zijn veelgestelde vragen. Een manier om 'safe' te zijn is om alle informatiebeveiligingscontroles die van toepassing zijn en alle
gerelateerde onderwerpen uit de BIO in één informatiebeveiligingsbeleiddocument stoppen. Dit heeft wet tot gevolg dat het informatiebeveiligingsbeleid een lijvig document wordt. De nadelen daarvan zijn:

- Het document is te groot om gelezen en begrepen te worden; beleid moet begrijpelijk en te onthouden zijn voor iedereen binnen de gemeente.
- Ook het onderhouden is lastig; beleid en aanvullend beleid zijn nu eenmaal aan wijzigingen onderhevig. Er kunnen altijd zaken zijn waardoor bestaand beleid gewijzigd moet worden, denk aan: wijzigingen in ICT, in wet- en regelgeving, toename van incidenten, nieuwe bedreigingen en nieuwe onderwerpen als IoT-beveiligingsbeleid. Informatiebeveiliging is immers een proces en in de PDCA-cyclus zit ook een stap (Act) aanpassen van beleid en beveiligingsmaatregelen als dat nodig is.

Het is beter om informatiebeveiligingsbeleid zo compact mogelijk te maken en om beleid hiërarchisch op te bouwen in meerdere documenten. Dit heeft als voordeel dat dit beleid sneller gelezen en makkelijker begrepen en onthouden wordt en dat men ruimte creëert om aanvullend specifiek beleid per thema te maken. Men creëert dus flexibiliteit door deze aanpak. Het is ook eenvoudiger omdat mogelijk niet alle (aanvullende) beleidsthema's voor iedereen binnen de gemeente even relevant zijn.

Een handige aanpak is het 'kapstokmodel'. Vanuit de kapstok, het overkoepelend gemeentelijk informatiebeveiligingsbeleid, volgt aanvullend beleid per BIO-thema, proces of zelfs informatiesysteem. Dit heeft ook voordelen voor de onderhoudbaarheid van het beleid; de kans dat alle beleidsdocumenten gewijzigd moeten worden is immers niet zo groot. In het vorige hoofdstuk is weergegeven hoe in de BIO de verschillende beveiligingsdoelstellingen en beveiligingsonderwerpen zijn te groeperen tot aanvullend beleid. Als dit grafisch wordt weergegeven ziet het er op basis van de baseline BIO als volgt uit:



Figuur 1: structuur van beveiligingsbeleid

Er is dus een duidelijke hiërarchische structuur tussen de verschillende soorten beleid. Wat nog niet in het plaatje staat, is dat al dat beleid ook leidt tot één of meer procedures en/of werkinstructies. Beleid gaat immers over een doelstelling, iets **wat** de gemeente wil bereiken en **waarom** en niet **hoe en waarmee**.

Systeem-, proces- of afdelingsbeveiligingsbeleid

Het kan voorkomen dat het organisatiebrede beveiligingsbeleid en organisatiebrede aanvullende beveiligingsbeleid geen recht doen aan specifieke beveiligingseisen uit wetgeving, of die van een bedrijfskolom, proces of informatiesysteem. Dan is het raadzaam om daar apart beveiligingsbeleid voor te maken omdat de beveiligingseisen zo (systeem) specifiek zijn dat dit noodzakelijk is. De verantwoordelijkheid voor dit specifieke beleid per bedrijfskolom, proces of informatiesysteem ligt dan bij de betreffende manager. Een voorbeeld hiervan zijn de aanvullende beveiligingseisen die gelden voor het thuiswerken met de BRP: zie hiervoor de aanbevelingen plaatsonafhankelijk werken van de RvIG.[2]

Zie ook de paragraaf over wetgeving met beleidseisen.

2 https://www.rvig.nl/documenten/richtlijnen/2018/11/23/aanbevelingen-plaatsonafhankelijk-werken-brp

Beveiligingsbeleid voor samenwerkingsverbanden en gemeenschappelijke regelingen

Gemeenten maken gebruik van gemeenschappelijke regelingen (GR) om gezamenlijk met andere gemeenten of partijen bepaalde taken en/of processen bij een derde partij te beleggen. In veel gevallen blijft de gemeente verantwoordelijk voor de beveligingseisen en privacyafspraken. Dat betekent dat er speciaal gemeentelijk beveiligingsbeleid gemaakt moet worden met de eisen en wensen waar de GR rekening mee moet houden. Soms voeren GR'en meerdere taken uit en dan kunnen er ook per taak/proces andere beveligingseisen zijn en dus ook andere beleidsdocumenten.

Beveiligingsbeleid bij leveranciers

Gemeenten maken gebruik van leveranciers voor het leveren van producten en diensten waarbij informatiebeveiliging een rol speelt. Hiervoor bestaat het GibiT als gemeenschappelijk inkoopkader. Leveranciers die gegevens verwerken van de gemeente hebben normaal gesproken eigen beveiligingsbeleid en zijn bij voorkeur gecertificeerd voor hun informatiebeveiliging. Het is verstandig om te onderzoeken of het beveiligingsbeleid van de leverancier dezelfde garanties geeft als het beveiligingsbeleid van de gemeente en of dat past bij het product en/of dienst. Leveranciers moeten hier transparant over kunnen zijn.

Governance voor privacy en ISMS

Sommige gemeenten kiezen ervoor om de governance van beveiliging (ISMS-beleid) en de governance voor het privacybeleid in een aanvullend beleidsstuk ‘Governancebeveiliging en privacy’ op te nemen, omdat er veel raakvlakken zijn tussen het strategisch beleid, ISMS-beleid en privacybeleid en dat dus integraal kan worden beschreven. Gemeenten zijn hier vrij in; deze handreiking is geen wet, maar een hulpmiddel om de structuur van de verschillende beleidsstukken te duiden en hier een aanpak voor neer te leggen.

3. Wat staat er in de BIO over beleid?

In de BIO wordt de basis gelegd voor een goed informatiebeveiligingsbeleid van de gemeente. Met name in hoofdstuk 5 en 6 van de baseline gaat men in op beleid. Dit informatiebeveiligingsbeleid vormt de kapstok waar al het deelbeleid en daaraan gerelateerde informatiebeveiligingsactiviteiten van zijn afgeleid.

3.1. Hoofdstuk 5 BIO

In hoofdstuk 5 van de BIO staat het informatiebeveiligingsbeleid beschreven. De beschreven doelstellingen zijn niet veel gewijzigd ten opzichte van die in de BIG. Wat opvalt in de BIO is dat het beleid in tabelvorm beschreven is met achtereenvolgens per onderwerp/regel: een nummer, corresponderend met de ISO27002 indeling, het Basis Beveiligings Niveau (BBN) nummer, de omschrijving en de verantwoordelijke. Lees hiervoor ook de handreiking BIO die door de IBD is uitgegeven. Onderstaand ter illustratie hoofdstuk 5 van de BIO (met eigen nummering):

5. Informatiebeveiligingsbeleid

5.1 Aansturing door de directie van de informatiebeveiliging

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

Nummer	BBN	Omschrijving	Verantwoordelijke
5.1.1	1	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Secretaris/algemeen directeur
5.1.1.1	1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a. de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b. de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c. de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d. de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e. de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f. de bevordering van het beveiligingsbewustzijn.	
		Handreikingen: BIO-001-Informatiebeveiligingsbeleid	
5.1.2	1	**Beoordeling van het informatiebeveiligingsbeleid** Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Secretaris/ algemeen directeur

5.1.2.1	1	Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	

3.2. Hoofdstuk 6 BIO

In hoofdstuk 6 van de BIO staat het volgende over het organiseren van informatiebeveiliging dat in beleid zou moeten worden opgenomen.

6. Organiseren van informatiebeveiliging

6.1 Interne organisatie

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.

6.1.1	**1**	**Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Secretaris/algemeen directeur
6.1.1.1	1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	
6.1.1.2	1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	
6.1.1.3	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	
6.1.1.4	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	
		Handreiking: BIO-CISO-functieprofiel	

3.3. Aanvullend beleid in de BIO

In de gehele BIO staan op diverse plaatsen beleid en aanvullend beleid genoemd. Nieuw is dat daar nu ook bij staat wie daar verantwoordelijk voor is. In de bijlage is een tabel opgenomen met een opsomming van informatiebeveiligingsbeleid en aanvullend beleid, zoveel als mogelijk logisch gegroepeerd. In deze tabel wordt ook het BBN-niveau weergegeven. Zie bijlage A.

4. Verdere input om te komen tot beleid

Zoals eerder is aangegeven vertellen de baselines BIG en BIO welk beveiligingsbeleid er minimaal moet zijn. Het groeperen van onderwerpen wordt dusdanig gedaan dat er een logische samenhang is in de verschillende beveiligingsbeleidsdocumenten.
Er zijn echter meerdere bronnen om te komen tot beveiligingsbeleid dan alleen de BIG of de BIO. De baseline is als norm niet zo veranderlijk en er kunnen dwingende redenen zijn om beleid aan te passen.

Wetgeving

Wetgeving is aan verandering onderhevig en dat kan inhouden dat er wetswijzigingen zijn die tot gevolg hebben dat het gemeentelijk informatiebeveiligingsbeleid moet veranderen. Een voorbeeld hiervan is de invoering van de Algemene Verordening Gegevensbescherming (AVG).

Gemeentelijk beleid

Er zijn vele veranderingen binnen gemeenten die kunnen leiden tot het wijzigen van gemeentelijk algemeen beleid. Denk hier aan ontwikkelingen als Gemeentelijke Gemeenschappelijke Infrastructuur (GGI)[3]. Een ander voorbeeld is een gemeentelijke verkiezing en als resultaat daarvan de nieuwe coalitieakkoorden en plannen die invloed kunnen hebben op de bedrijfsvoering. Vergeet ook niet zaken als herindelingen of het samenwerken in gemeenschappelijke regelingen rondom bepaalde thema's.

Resultaten van een Business Impact Analyse gevolgd door een risicoanalyse

Met de komst van de BIO moeten proceseigenaren het belang van hun proces kennen. Dit kan men onderzoeken met de baselinetoets waarmee dan feitelijk een Business Impact Analyse (BIA) wordt uitgevoerd Binnen de BIO zijn meerdere beschermingsniveaus gedefineerd, te weten: BBN1 (BasisBeschermingsNiveau), BBN2 en BBN3. Als men niks doet (dus geen baselinetoets) dan is BBN2 het standaardniveau van de BIO dat gekozen moet worden. Wil men vaststellen of BBN1 of BBN3 van toepassing is dan kan dat door middel van het uitvoeren van een BIA met de baselinetoets, mogelijk gevolgd door een risicoanalyse.

Hier leidt de BIO-baselinetoets dus tot een beslissing over het niveau van de BIO dat gekozen moet worden en of ook nog een aanvullende risicoanalyse noodzakelijk is. Dit heeft uiteindelijk ook gevolgen voor de onderwerpen die men in het beveiligingsbeleid terug wil laten komen. Let wel op: het BBN-niveau wordt in belangrijke mate bepaald door het onderdeel vertrouwelijkheid.

Resultaten van risicoanalyses

Zoals hierboven beschreven kan een risicoanalyse worden uitgevoerd als gevolg van de uitgevoerde baselinetoets. Het kan ook gebeuren dat er een risicoanalyse moet worden uitgevoerd voor een nieuw systeem of dat er moet worden geüpdatet omdat een systeem wijzigt binnen het wijzigingsbeheerproces. De verantwoordelijkheid ligt hier weer bij de proceseigenaar of -manager. De CISO van de gemeente is adviserend.

3 https://www.vngrealisatie.nl/roadmap/de-gemeentelijke-gemeenschappelijke-infrastructuur-ggi

Input van de IBD

De IBD heeft inzicht in incidenten en trends en publiceert tweejaarlijks een Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten. Dit dreigingsbeeld is goede input voor het herijken van het gemeentelijk informatiebeveiligingsbeleid.

Uitkomsten van Audits

Er worden binnen gemeenten ook diverse interne en externe audits uitgevoerd. Hieronder scharen wij ook rekenkameronderzoeken. Als resultaat van de audit kunnen zwakheden in de beveiliging ontdekt worden en dit kan tot gevolg hebben dat er aanpassingen noodzakelijk zijn in gemeentebreed beveiligingsbeleid of aanvullend beveiligingsbeleid of een van de andere vormen van beleid.

Opgetreden incidenten

Binnen gemeenten treden informatiebeveiligingsincidenten op. Deze incidenten kunnen een indicator zijn dat bepaalde beveiligingsmaatregelen niet optimaal zijn ingericht of zelfs niet aanwezig zijn. Informatiebeveiligingsbeleid heeft zijn weerslag op het inrichten van beveiligingsmaatregelen en opgetreden incidenten hebben daarmee invloed op het informatiebeveiligingsbeleid van de gemeente. Hierbij moet wel worden opgemerkt dat dit ook betekent dat de opgetreden en gemelde incidenten ergens gelinkt kunnen worden aan een beveiligingsmaatregel en/of beleidsuitgangspunt.

Uitvoerbaarheid van beveiligingsprocessen

Er hoort een scheiding te zijn tussen beleid en uitvoering (tussen het ‘wat’ en het ‘hoe’). Het is mogelijk dat beleid iets vraagt wat niet goed realiseerbaar is. In dat geval kan men ervoor kiezen het beleid aan te passen of de ontstane situatie, met uitleg, tijdelijk te accepteren. De beleidsdoelstelling blijft dan overeind maar er wordt tijdelijk niet aan voldaan.

5. Wetgeving met beleidseisen

Gemeenten hebben ook te maken met aanvullende wetgeving die door stelselverantwoordelijken is opgelegd, waar informatiebeveiligingsbeleid en -maatregelen worden gevraagd die weliswaar ook in de BIO voorkomen, maar die bij een audit toch door de auditor 'gezien' moeten worden om te voldoen aan die specifieke wetten.

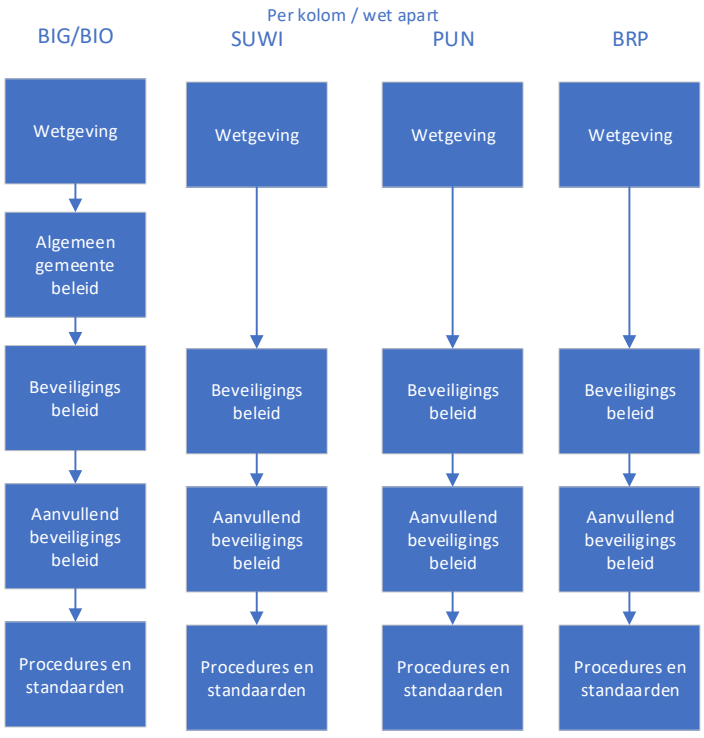
Deze wetgeving bestaat met name voor:

- Basisregistraties
- SUWInet
- DigiD

De specifieke onderdelen hiervan worden ook bij ENSIA uitgevraagd voor de jaarlijkse verticale verantwoording[4]. Als gemeente kan men met deze wetgeving op een aantal manieren omgaan:

1. Procedures beschrijven en processen inrichten voor specifieke beveiligingseisen uit de genoemde wetgeving, het beveiligingsbeleid en aanvullend beveiligingsbeleid, naast hetgeen dat er al voor de BIO gedaan wordt. Er ontstaan dan dus meerdere series documenten die specifieke onderwerpen behandelen die in wetgeving staan. Dit kan voordelig zijn omdat dan de verplichte documenten die voor wetgeving noodzakelijk zijn apart kunnen worden gemaakt, gebruikt en geaudit. Die aanvullende wetten wijzigen niet zo vaak, dus dit kan veilig gedaan worden. De verantwoordelijkheid voor de naleving van het specifieke beveiligingsbeleid ligt bij de betreffende lijnmanager.

Dan ziet dat er als volgt uit:

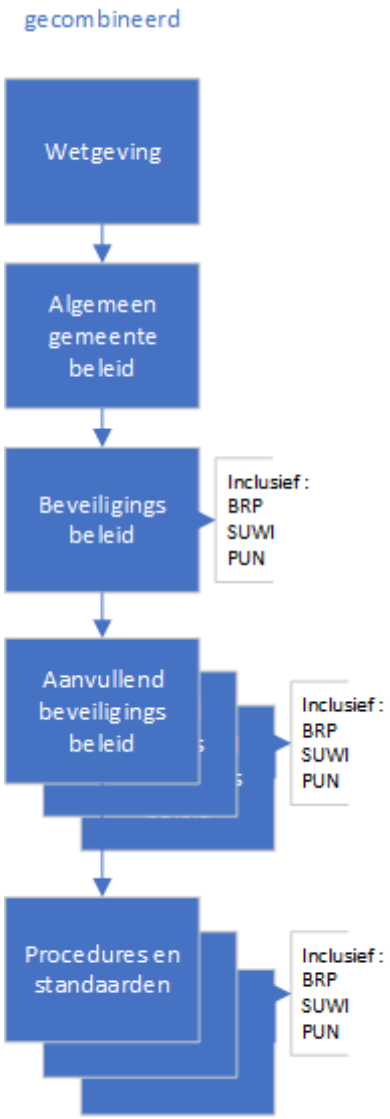


Figuur 2 Structuur beleid op basis van wet- en regelgeving

4 https://www.informatiebeveiligingsdienst.nl/project/ensia/

2. Alle beveiligingseisen voor deze aanvullende wetten opnemen in de documentatieset die voor de BIO gemaakt wordt. Een vereiste is dan wel dat dit zichtbaar is. Als bij de reikwijdte van het beveiligingsbeleid niet staat dat het beveiligingsbeleid ook voor de BRP, SUWI en PUN geldt, dan scoort men voor het toezicht op deze wetgeving onvoldoende. Ook van specifieke beveiligingseisen die benoemd worden moet men de basis hiervoor vanuit de verschillende wetten aangeven.

De nieuwe structuur wordt dan als volgt:



Figuur 3 Samengevoegde eisen in één set beleidsdocumenten

6. Implementatie van beleid

Als het overkoepelende gemeentebrede informatiebeveiligingsbeleid is geschreven en vastgesteld, zijn alleen nog maar de belangrijkste informatiebeveiligingsbeleidsuitgangspunten ‘het wat en waarom’ en verantwoordelijkheden beschreven. Dan is men er nog niet; daarna komt het aanvullende gemeentebrede beveiligingsbeleid per BIO-thema, proces en/of informatiesysteem zoals in een van de vorige hoofdstukken beschreven is.
Na beleid en procedures moet er ook nog iets worden geïmplementeerd binnen de gemeente. Het middel om dit te doen is het schrijven van het informatiebeveiligingsplan. Het plan bevat de activiteiten om met informatiebeveiliging om te gaan in de periode die het plan bestrijkt. Deze informatiebeveiligingsplannen kunnen ook systeemspecifiek zijn. In dit document gaan we hier niet verder op in.

6.1. Procedures

Uiteindelijk leidt het beleid tot iets wat moet worden gedaan binnen de organisatie: in de BIG en BIO staat welke procedures de uitvoering moet geven aan het beleid en welke er dus minimaal moeten zijn. Ook kan het voorkomen dat wetgeving specifieke procedures vereist.

Deze procedures kunnen wederom gemeentebreed, of proces- en systeemspecifiek zijn. Onderstaand een opsomming van mogelijke gemeentebrede procedures gerelateerd aan de verschillende beleidsonderwerpen uit de BIO. In de opsomming staat een verwijzing naar de BIO-beheersdoelstelling waar hier meer over te vinden is: zie bijlage B.

7. Beheersing

Strategisch beleid moet volgens de BIG en BIO-eisen minimaal om de 3 jaar worden herbeoordeeld en zo nodig worden bijgesteld. De aanvullende beleidsdocumenten kunnen aangepast worden wanneer dat nodig is. Voor de beoordeling en bijstelling van procedures wordt geen termijn gegeven, in de praktijk zullen deze vaker wijzigen.

Verantwoordelijkheden

In de BIG en de BIO is beschreven wie verantwoordelijk is voor het vaststellen van het beleid. Voor gemeenten zal dit voor het gemeentebrede beveiligingsbeleid het college zijn. Men kan ervoor kiezen om in het gemeentebrede beveiligingsbeleid op basis van hoofdstuk 5 in de BIG een mandaat voor aanvullend beleid te beschrijven. Met als doelstelling dat aanvullend gemeentelijk beveiligingsbeleid en procedures mogen worden vastgesteld door een lager niveau in de organisatie, bijvoorbeeld de gemeentesecretaris of directie. In de BIO staat dit in de kolom ‘verantwoordelijke’ beschreven.

Registratie van documentatie

Het verdient aanbeveling om beleid en procedures en aanvullende documentatie te nummeren volgens de BIG/BIO. Hierdoor is duidelijk zichtbaar waar het document voor gemaakt is. De organisatie moet een registratie bijhouden van alle BIG en BIO-gerelateerde beleidsdocumenten en procedures met daarin:

1. Naam van het document.
2. Relatie met BIG/BIO-maatregel.
3. Relatie met andere beleidsstukken en onderliggende procedures.
4. Vaststellingsdatum.
5. Herbeoordelings-/vernieuwingsdatum.
6. Versienummer.
7. Eigenaar.
8. Vindplaats.

8. Communicatie over beleid

Informatiebeveiligingsbeleid is niet iets dat wordt gemaakt om in de kast te zetten. Met goed informatiebeveiligingsbeleid wordt beoogd de basis te leggen voor goede informatieveiligheid binnen de gemeente. Het is niet voldoende om beleid te maken en te publiceren om vervolgens over te gaan tot de orde van de dag.

Hoe staat dit nu in de BIO (zie ook het eerdere hoofdstuk hierover)?

BIO:

5.1.1 Beleidsregels voor informatiebeveiliging

Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.

De beveiligingsdoelstelling heeft het over het **communiceren van beleid** aan medewerkers en relevante externe partijen. Dat lijkt eenvoudig: men plaatst het beleid op het intranet en/of het internet en klaar. Toch is dit niet helemaal juist. Binnen de gemeente werken immers ambtenaren en inhuurkrachten die allemaal verschillende rollen, functies en achtergronden hebben. Het hoeft helemaal niet zo te zijn dat alle delen van het beveiligingsbeleid van de gemeente voor iedereen even relevant is, en het hoeft ook niet zo te zijn dat iedere doelgroep van dat beleid hetzelfde kennisniveau heeft. De gemeente moet dan de verschillende delen van het beveiligingsbeleid vertalen naar betreffende doelgroepen. Als voorbeeld kunnen de volgende doelgroepen onderscheiden worden:

1. Iedereen binnen de gemeente.

2. Managers, leidinggevenden en bestuurders.

3. Beleidsmedewerkers en behandelaars.

4. IT-beheerders (technisch en functioneel beheerders).

5. Leveranciers.

Informatiebeveiligingsbeleid dat op alle medewerkers van toepassing is kan het beste worden weergegeven in een vorm die makkelijk leest en duidelijk maakt wat van iedereen wordt verwacht. Dit kan ook gekoppeld worden aan een informatiebeveiligingsbewustwordingscampagne. Basisonderwerpen die behandeld kunnen worden zijn:

- Waar is het beleid te vinden.
- Wat zijn de doelen van beveiligingsbeleid.
- Wie doet wat.
- Gedragscode, integer handelen.
- Internet en e-mailgebruik.
- Informatieclassificatie.
- Hoe omgaan met gebruikersnamen en wachtwoorden.
- Clear desk en clear screen.
- Bezoekers.

- Melden van (beveiligings) incidenten.
- Persoonsgegevens en datalekken.

Informatiebeveiligingsbeleid dat specifiek op managers en leidinggevenden van toepassing is, gaat met name over de specifieke verantwoordelijkheden van managers, leidinggevenden maar ook van bestuurders. Onderwerpen die behandeld kunnen worden zijn:

- Beveiligingsverantwoordelijkheden van de manager.
- Beveiliging en projecten.
- Risicomanagement.
- Bedrijfscontinuïteit en crisisbeheersing.
- Beveiliging en inkoop.
- Dataclassificatie en privacy.
- Personeelsprocessen en security (in dienst, uit dienst en functiewisselprocessen).
- Verantwoording over beveiliging, ENSIA.

Delen van het informatiebeveiligingsbeleid die specifiek aandachtspunten bevatten voor (IT-)beheerders zijn:

- De bijzondere positie van de IT-beheerder en de gevaren.
- Omgang met beheerdersaccounts en wachtwoorden.
- Back-up en restore.
- Beheren op afstand.
- Bedrijfscontinuïteit.
- Privacy.
- IT-beveiligingsprocessen en procedures zoals incidentmanagement, CMDB, Wijzigingsbeheer, et cetera.

Leveranciers, en eigenlijk alle externe partijen, moeten het beveiligingsbeleid van de gemeente kennen, dus de basisonderwerpen zijn van belang. Daarnaast kunnen de onderwerpen worden bepaald op basis van de soort dienstverlening voor de gemeente door de leverancier. Kijk voor onderwerpen ook naar de GibiT[5].

5 https://www.vngrealisatie.nl/gebruik-gibit-voorwaarden-voor-aankoop-van-uw-it

9. Delen op de IBD community

Alle gemeenten maken informatiebeveiligingsbeleidsdocumenten, deze zijn soms op het internet te vinden. Omdat gemeenten van elkaar kunnen leren is het verstandig om het informatiebeveiligingsbeleid, aanvullend informatiebeveiligingsbeleid, procedures en alle overige documentatie te delen met elkaar. Hierdoor kan veel werk worden bespaard voor de gemeenten en kan de bestaande documentatie worden verbeterd door feedback te geven op elkaars stukken. Dit delen kan op de IBD Community; maar daar gebruik van.

In bijlage C zit een voorbeeld informatiebeveiligingbeleid op basis van de BIO.

Bijlage A: Informatiebeveiligingsbeleid op basis van de BIO:

Tabel beleid in de BIO

BBN	Control	Soort / onderwerpen
1		**Algemeen Beleid**
1	5.1.1	Overkoepelend informatiebeveiligingsbeleid
1	6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging
2	6.1.5	Informatiebeveiliging in projectbeheer
1	6.1.2	Scheiding van taken
1	7.2.1	Directieverantwoordelijkheid ten aanzien van bewustwording
1	7.2.2.	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
1	7.2.3	Disciplinaire procedure
1	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging
1	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband
1	8.1.1	Inventariseren van bedrijfsmiddelen
1	8.1.2	Eigendom van bedrijfsmiddelen
1	8.1.4.	Teruggeven van bedrijfsmiddelen
1	18.2.2.1	Rapporteren over informatiebeveiliging
1	8.2.1	Informatieclassificatie is verantwoordelijkheid van de proceseigenaar
1	13.2.4	Geheimhoudingsovereenkomsten
		Aanvullend informatiebeveiligingsbeleid structuur
		Hoofdstuk 4 BIO: verantwoording over de BIO
		Anti-malware beleid
1	12.2.1	Anti-malware beleid
		Audit beleid
1	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging
1	18.2.2	Naleving beveiligingsbeleid en -normen
		Back-up beleid
1	18.2.3	Beoordeling technische naleving
1	12.3.1	Back-up beleid

		Classificatie beleid
1	8.2.1	Classificatie van informatie, nadere regels
	10	**Cryptografie beleid**
1	10.1.1	Beleid inzake gebruik van cryptografische beheersmaatregelen
	11	**Fysieke toegangsbeleid**
1	11.1.1	Fysieke beveiligingszones
1	11.1.2	Fysieke toegangsbeveiliging
1	11.1.3	Kantoren, ruimten en faciliteiten beveiligen
1	11.1.4	Bescherming tegen bedreigingen van buitenaf
2	11.1.5	Werken in beveiligde gebieden
1	11.1.6	Laad- en loslocatie
		Huisregels beleid
1	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen
		Incidentmanagement en responsebeleid
1	11.2.9	Clear desk- en clear screenbeleid
1	16.1.1	Verantwoordelijkheden en procedures
1	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
1	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging
1	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
1	16.1.5	Incidentmanagement en responsebeleid
2	16.1.6	Lering uit informatiebeveiligingsincidenten
2	16.1.7	Verzamelen van bewijsmateriaal
		Logging beleid
1	12.4.1	Loggingbeleid
		Mobiele media beleid
2	8.3.3	Media fysiek overdragen

1	7	**Veilig personeel beleid**
1	7.1.1	Screening
1	7.1.2	Arbeidsvoorwaarden
1	7.2.1	Directieverantwoordelijkheden
1	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
1	7.2.3	Disciplinaire maatregelen
1	7.3.1	Beëindiging of wijziging verantwoordelijkheden van het dienstverband
1	13.2.4	Geheimhoudingsovereenkomst
		Privacy beleid
	18.1.4	Privacybeleid
		Telewerken beleid
2	6.2.2	Telewerkenbeleid
		Toegangsbeleid
1	9.1.1	Beleid voor toegangsbeveiliging
		Beleid voor mobiele apparatuur
1	6.2.1	Beleid voor mobiele apparatuur
	14	**Beleid voor beveiligd ontwikkelen**
1	14.2.1	Beleid voor beveiligd ontwikkelen
1	9.4.5	Beperken toegang op programmabroncode
	15	**Informatiebeveiligingsbeleid voor leveranciersrelaties**
1	15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties
1	16.1.5	Link naar incidentmanagement en responsebeleid
1	13.2.4	Geheimhoudingsovereenkomst
	18	**ISMS-beleid**
1	18.2.1.1	ISMS-beleid
		Netwerk beleid
1	13.1.1	Beheersmaatregelen voor netwerkdiensten
	13.1.2	Beveiliging van netwerkdiensten
	13.1.3	Scheiding van netwerken

		Beleid voor informatietransport
1	13.2.1	Beleid voor informatietransport
		Wachtwoord beleid
1	9.3.1	Geheime authenticatie-informatie gebruiken
1	9.4.2	Beveiligde inlogprocedures
1	9.4.2.1	Gebruik van 2FA
2	9.3.1.1	Wachtwoordkluizen
1	9.4.3	Systemen voor wachtwoordbeheer
1	9.4.3.1	Wachtwoordeisen
1	9.4.3.2	Vernieuwen wachtwoorden

Bijlage B: Tabel met BIO procedures:

BIO : 7.2.2 - In dienst procedure

BIO : 7.2.3 - Disciplinaire procedure

BIO : 7.3.1 - Uit dienst procedure

BIO : 8.1.1 - CMDB procedure

BIO : 8.2.2 – Informatie labellingprocedure gerelateerd aan classificatie

BIO : 8.2.3 - Procedure voor behandelen bedrijfsmiddelen

BIO : 8.3.1 - Procedures voor omgang met verwijderbare media

BIO : 8.3.2 - Procedures voor opslag, verwijderen, vernietigen van media met informatie

BIO : 8.3.2 - Procedure voor wissen van informatie op media

BIO : 9.2.1 - Gebruikers aanmeld- en afmeld procedure

BIO : 9.2.2 - Gebruikers toegangsverlening procedure

BIO : 9.2.3 - Procedure voor beoordeling van uitgegeven speciale bevoegdheden

BIO : 9.2.5 - Procedure voor de beoordeling van uitgegeven toegangsrechten

BIO : 9.4.3 – Wachtwoord procedures

BIO : 11.1.5 - Procedure voor werken in beveiligde gebieden

BIO : 12.1.1 - Bedienprocedures voor systemen

BIO : 12.1.2 - Procedure voor wijzigingsbeheer

BIO : 12.1.4 – Test procedures

BIO : 12.2.1 – Anti-malware procedures

BIO : 12.3.1 - Back-up- en restore procedures

BIO : 12.4.1 – Logging procedures

BIO : 12.4.2 - Logging retentie procedure

BIO : 12.5.1 - Software installatie procedure

BIO : 12.6.1 - Patchmanagement procedures

BIO : 13.2.1 - informatie transport procedure

BIO : 14.2.2 - Wijzigingsbeheer procedure

BIO : 14.2.8 - Test procedures

BIO : 15.1.1 - Risicoanalyse procedure

BIO : 15.1.2 - Inkoop procedures

BIO : 16.1.1 - Incidentmanagement procedures

BIO : 16.1.2 - Incidentmanagement procedures

BIO : 16.1.2 - Incident meldprocedure

BIO : 16.1.3 - Responsible disclosure procedure

BIO : 16.1.7 - Forensisch onderzoek procedure

BIO : 18.1.2 - Software licentie controle procedure

Bijlage C: Voorbeeldbeleid op basis van de BIO

(dit document is ook separaat te downloaden)

INFORMATIE
BEVEILIGINGS
DIENST

Strategisch Gemeentelijk Informatiebeveiligingsbeleid [gemeente]

[jaar] tot [jaar]

[datum]
[naam]
[afdeling]

VNG Realisatie

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1			

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren [jaar] tot [jaar] en vervangt het in [jaar] vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid [jaar]'.
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 2019-2023' zet de gemeente een volgende stap 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 strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) zie bijlage C. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage B.

1.1. Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk 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, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. 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. Ambitie en visie van de gemeente op het gebied van informatieveiligheid

….. (zelf invullen, komt van lokaal beleid)

2. Strategisch beleid

2.1. Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren [jaar] tot [jaar]'. 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:

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. 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.

De 10 principes voor informatiebeveiliging (zie bijlage C)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader [6] 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 het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

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

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.

Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk ook een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft 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 gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[7] in 2018 de Baseline Informatiebeveiliging 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 zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven ‘Gemeentelijk Informatiebeveiligingsplan’.

2.5. Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, 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 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.

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

2.6. Uitgangspunten

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

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

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.

Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- 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.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de [gemeente _____)] hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.

- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W 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 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 gesteld zijn.
- Alle medewerkers van de gemeente 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.

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 CIO, gebaseerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - het dreigingsbeeld gemeenten van de IBD;
  - de door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

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 college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging 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 informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de [gemeente _____)] 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 over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

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, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.3. Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de [gemeente _____)]. De bestuurders en directeuren van de [gemeente _____)] 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 hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4. 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 afdelingsmanagers. De afdelingsmanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt 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.

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

Vastgesteld op : [datum] door het college van [Gemeente]

[Ondertekening]

De vaststelling kan natuurlijk ook door middel van ondertekening van een collegebesluit-oplegger waarmee dit beleid behandeld wordt in de collegevergadering van de gemeente, in dat geval is deze ondertekening niet nodig.

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie