Gemeente Bergen op Zoom

GEMEENTEBLAD

Officiële uitgave van de gemeente Bergen op Zoom

Nr. 327824

23 september 2021

Strategisch Informatiebeveiligingsbeleid 2021-2024 Gemeente Bergen op Zoom

Samenvatting

We zien een steeds verdergaande digitalisering en ketenintegratie binnen de publieke sector. We willen groeien naar een data gedreven organisatie. Hiermee wordt de afhankelijkheid van een betrouwbare informatievoorziening steeds groter. De hack bij gemeente Lochem (juni 2019) laat zien dat ook een gemeente slachtoffer kan zijn van een geraffineerde cyberaanval , met als doel het eisen van losgeld. Het beveiligingslek in Citrix (december 2019/januari 2020) laat zien dat we de beschikbaarheid van onze ICT-infrastructuur moesten aanpassen. De gijzeling van data bij de Universiteit van Maastricht (januari 2020), waardoor duizenden medewerkers en studenten niet bij hun gegevens konden, toont aan dat internetcriminelen steeds verder gaan. En het meest recent is de ransomware-aanval, waardoor de gemeente Hof van Twente wekenlang 'out of service' was, en nog maandenlang bezig zal zijn met herstel met een gigantische financiële schade. Echter, ICT is een onderdeel van informatieveiligheid; het gaat in veel gevallen om de mens in de organisatie en de manier waarop de organisatie met risico's omgaat. Uit diverse onderzoeken blijkt dat tussen de 70% en 80% van de beveiligingsincidenten wordt veroorzaakt door de medewerker.

Het College van Burgemeester en Wethouders (hierna aangeduid als College) heeft een cruciale rol voor informatieveiligheid. Het College is bestuurlijk verantwoordelijk en de gemeentesecretaris/algemeen directeur is ambtelijk verantwoordelijk voor de uitvoering. Zij worden daarbij ondersteund door de Chief Information Security Officer (CISO). Het College geeft met het vaststellen van dit beleid een duidelijke richting aan informatieveiligheid en laat zien dat zij informatieveiligheid voorwaardelijk vindt voor een betrouwbare en veilige informatievoorziening.

Doel van informatiebeveiliging

Het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening om zo een optimale dienstverlening aan burgers, bedrijven en samenwerkingspartners te kunnen leveren.

Informatieveiligheid is geen doel op zich, maar een belangrijke randvoorwaarde voor de bescherming van (vitale) maatschappelijke functies, die afhankelijk zijn van een betrouwbare informatievoorziening. Denk hierbij o.a. aan WMO, jeugdzorg, waterbeheer, registratie van geboorte en overlijden en de openbare orde & veiligheid.

Risicomanagement centraal

Onze organisatie is volledig afhankelijk van informatieverwerking. Daarbij lopen we het risico, de 'kwade kans', dat informatie niet op het juiste moment beschikbaar zijn, niet juist of volledig zijn of in verkeerde handen terecht komen. Daar richt informatiebeveiliging zich op. Eigenaren, lijnmanagers, zullen zich dus een beeld moeten vormen van de kwetsbaarheden in hun processen en systemen: hoe groot is de kans dat zo'n kwetsbaarheid wordt misbruikt en wat zijn de gevolgen (impact) daarvan? En aan de andere kant: met welke dreigingen moeten we rekening houden. Precies daar tussenin bevindt zich de vraag: welke maatregelen wil een eigenaar treffen om de kwetsbare informatie beschermen tegen de kwaadwillenden. En juist daarom is risicomanagement de basis voor informatiebeveiliging, waar de lijnmanager beslist en de CISO adviseert.

Lijnmanagement centraal

Het lijnmanagement is integraal verantwoordelijk voor de resultaten van haar cluster – en daarmee dus ook voor informatieveiligheid. Risico-management en het instellen / borgen van maatregelen horen daar expliciet bij. Veel maatregelen worden concernbreed vanuit Bedrijfsvoering voorzien, maar met

name de organisatorische / producerele maatregelen blijven bij het cluster. Expertise wordt doorgaans geboden door kwaliteitsmedewerkers of procesbeheerders. Bergen op Zoom stuurt haar clusters duaal aan via een resultaatmanager en een HR-manager.

Verspreidingstabel
Functie Actie Datum
CISO Concept opstellen 2020-Q3
CISO Concept definitief maken 2021-januari
Functionaris Gegevensbescherming Afstemmen tav privacy 2020-Q3 en 2021-januari
Privacy Officer Afstemmen tav privacy 2020-Q3 en 2021-januari
ConcernTeam manager Bedrijfsvoering 2020-december
2021-januari
CT MT's Kennis nemen van de inhoud en belangrijkste wijzigingen 2020-december
CT Kennis nemen van de inhoud en belangrijkste wijzigingen 2021-januari
Portefeuillehouder Afstemming voorafgaand aan besluitvorming 2021-januari
College Vaststellen en besluiten de raad te informeren 2021-februari

Review tabel
Versie Door Opmerkingen
20-dec M. van Bavel (CT BV) Bij de uitwerking aandacht aan aanbevelingen IT Audit schenken
25-jan M. van Bavel (CT BV)
18-jan S. Izeboud (FG) Meer integratie IB & P in Local Governance
19-jan O. Engelen (PO) Meer integratie IB & P in Local Governance
18 mei 2021 H. Baaten (CISO) Minor updates nav actualiteit
2 juli 2021 H. Baaten (CISO) Minor updates nav actualiteit

Inleiding

Dit document is het Strategisch Informatiebeveiligingsbeleid (IB Beleid) voor de jaren 2021 tm 2024 van de gemeente Bergen op Zoom en vervangt het 'Gemeentelijk Informatiebeveiligingsbeleid 2017-2020'. Het is richtinggevend en kaderstellend en wordt uitgewerkt in onderwerpspecifieke beleidsdocumenten op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2021-2024' borgt de gemeente de beveiliging van gemeentelijke informatie, waaronder persoonsgegevens. De basis voor dit beleid is de NEN-ISO/IEC 27002:2017 en de daarop gebaseerde Baseline Informatiebeveiliging Overheid (BIO) (bijlage A). De principes zijn gebaseerd op de 10 Bestuurlijke principes voor Informatiebeveiliging zoals uitgewerkt door de VNG (bijlage B).

1.1 Leeswijzer

In hoofdstuk 2 wordt de ambitie en visie van de gemeente Bergen op Zoom ten aanzien van informatieveiligheid uiteengezet. Dat doen we op basis van de doelstellingen in het Focusakkoord. De kern van het strategisch beleid wordt in hoofdstuk 3 uitgewerkt: wat zijn de uitgangspunten, principes en randvoorwaarden. Tenslotte beschrijft hoofdstuk 4 de belangrijkste onderdelen van de organisatie die nodig is om het beleid ten uitvoer te brengen.

1.2 Definitie en scope van 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.

- Informatie moet beschikbaar zijn op het moment dat we de gegevens nodig hebben. Voorkomen dat applicaties niet beschikbaar zijn.
- Informatie is integer (gegevens zijn actueel, juist en volledig). Voorkomen dat informatie onvolledig of onjuist is.
- Informatie is vertrouwelijk, dit betekent alleen toegankelijk voor de personen die dit mogen gebruiken voor het werk. Voorkomen dat vertrouwelijke informatie in verkeerde handen valt.

Het IB Beleid 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.

Informatieveiligheid draait om risicobeheersing. Op basis van een risico-afweging gaan we bewust bepaalde maatregelen wel of niet nemen om de kwetsbaarheden in de dienstverlening en bedrijfsvoering te minimaliseren.

2 Ambitie en visie van de gemeente

Om de continuïteit in de dienstverlening en bedrijfsvoering te borgen is een solide inrichting van informatiebeveiliging nodig. Het College en het Concernteam (CT) maken hierbij op basis van risicomanagement bewuste keuzes om informatieveiligheid te borgen en om kwetsbaarheden in de bedrijfsvoering te minimaliseren. Risico op dataverlies en -manipulatie van gegevens van inwoners en bedrijven worden hiermee verkleind. Veiligheids- en imagorisico's voor de organisatie - zoals afpersing, diefstal van persoon- en bedrijfsgegevens, uitval van ICT-diensten- worden hiermee verkleind.

2.1 Ambitie: volwassen worden in informatieveiligheid

Een solide inrichting van informatiebeveiliging aan de voorkant voorkomt extra tijdsinvestering en herstelkosten achteraf. Om deze inrichting te bereiken is het noodzakelijk om op het gebied van informatiebeveiliging te professionaliseren. Het huidige volwassenheidsniveau van informatiebeveiliging van de gemeente Bergen op Zoom wordt ingeschat tussen niveau 1 en 2. De ambitie is om binnen deze beleidsperiode (uiterlijk 2024) volwassenheidsniveau 3 te bereiken. Daarbij zijn de beheersmaatregelen gedocumenteerd en kan opzet en werking worden aangetoond. Daarmee voldoet Bergen op Zoom aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. We wetende risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda. Noodzakelijke randvoorwaarde om deze groei te bereiken, is de beschikbaarheid van kwalitatieve en kwantitatieve resources op de afdelingen.

2.2 Visie en Focusakkoord

De gemeente Bergen op Zoom werkt in deze bestuursperiode met het Focusakkoord . Dat is vergelijkbaar met een Collegeprogramma, ware het niet dat de gemeenteraad 3 bestuursopdrachten heeft geformuleerd. Het Focusakkoord biedt ons een extra kader voor informatieveiligheid: onze ambitie en onze grenzen. In het Focusakkoord wordt Informatiebeveiliging expliciet vernoemd:

Hier spreekt geen (hoge) ambitie en visie uit. We moeten aan wet- en regelgeving voldoen (BIO, Forum Standaardisatie en AVG), dat is ons verplichte doel. Compliancy boven security. Daarmee is het onderhavige IB Beleid kaderstellend.

2.3 Risico-management centraal

Onze organisatie is volledig afhankelijk van informatieverwerking. Daarbij lopen we het risico, de 'kwade kans', dat informatie niet op het juiste moment beschikbaar is, niet juist of volledig is of in verkeerde handen terecht kan komen. Daar richt informatiebeveiliging zich op. Eigenaren, lijnmanagers, zullen zich dus een beeld moeten vormen van de kwetsbaarheden in hun processen en systemen: hoe groot is de kans dat zo'n kwetsbaarheid wordt misbruikt en wat zijn de gevolgen (impact) daarvan? En aan de andere kant: met welke dreigingen moeten we rekening houden. Precies daar tussenin bevindt zich de vraag: welke maatregelen wil een eigenaar treffen om de kwetsbare informatie beschermen tegen de kwaadwillenden: wat is de 'risk appetite' (risico-bereidheid) en impact op ons weerstandsvermogen? En juist daarom is risicomanagement de basis voor informatiebeveiliging, waar de lijnmanager beslist en de CISO adviseert.

We voeren Information Security risico management uit op basis van de modellen van ISACA en COBIT.

3 Strategisch informatiebeveiligingsbeleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Het legt de link tussen het Focusakkoord, wet- en regelgeving en de dagelijkse operatie. Het IB Beleid is gericht op het:

Verstevigen van de governance
De verantwoordelijkheid voor informatieveiligheid is primair in de lijn belegd. Dit betekent een centrale rol voor CT- en lijnmanagers en aansluiting bij / invulling van het (Three) Lines of Defence model.

Risico gebaseerd sturen

Dit betekent dat het lijnmanagement verantwoordelijk is voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.

Integratie in de planning- en control cyclus
Informatieveiligheid wordt opgenomen in de integrale P&C-cyclus. Verantwoording vindt plaats middels ENSIA. Deze aanpak draagt bij aan een verdere professionalisering van informatieveiligheid.

3.1 Scope van het strategische informatiebeveiligingsbeleid

Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het heeft betrekking op het politiek bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen.

3.2 Grondslagen, wet- en regelgeving

Het IB Beleid is gebaseerd op:

- NEN-ISO/IEC 27001:2017
- NEN-ISO/IEC 27002:2017
- Baseline Informatiebeveiliging Overheid (BIO) en de 10 principes voor informatiebeveiliging.

Wet- en regelgeving geldt nog immer als een bepalend, verplicht kader. De AVG is een (Europese) wet en BIO is na instemming van alle overheidslagen interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO). Gemeenten zijn in dit overleg vertegenwoordigd door de VNG. De Verplichte Standaarden zijn vastgesteld door het Forum Standaardisatie (voedt het OBDO en sterk gelieerd aan het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties).

3.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het actuele normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de lijnmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO27001 en daarbij is risicomanagement de kern. Dit houdt voor hen 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.

3.2.2 De 10 principes voor informatiebeveiliging

VNG heeft aan het gemeentelijk bestuur de "10 principes van informatiebeveiliging" uitgereikt. Deze principes bieden het bestuur handvatten op welke wijze het haar rol kan invullen bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers. De 10 principes voor informatiebeveiliging4zijn 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 zijn nader uitgewerkt in bijlage B.

3.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten (IBD, VNG) 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.

3.3 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van dit IB Beleid zijn:

1. Het IB Beleid vormt samen met het tactische informatiebeveiligingsbeleid (de uitwerking) en het informatiebeveiligingsplan (IB Plan) het kader om informatieveiligheid in de organisatie te borgen.

2. Informatiebeveiliging mag niet ten koste gaan van de veiligheid van personen.

3. Het bestuur van de gemeente Bergen op Zoom, de gemeentesecretaris / algemeen directeur, de ConcernTeam-managers en de lijnmanagers dragen dit beleid actief uit en sturen aan op de implementatie en naleving van dit beleid.

4. Informatiebeveiliging is georganiseerd. Het management heeft continu aandacht voor het vergroten van het bewustzijn van medewerkers om zo de menselijke schakel te versterken.

5. De rol van Chief Information Security Officer (CISO) is structureel ingevuld volgens de Handreiking IB-profiel CISO van IBD.

6. Regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid zijn vastgesteld ('Local Governance', bijlage C).

7. Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én de coördinatie op dit proces is informatieveiligheid binnen de organisatie verankerd. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.

8. Informatiebeveiliging is onderdeel van risicomanagement.

9. 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.

10. 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.

3.4 Praktisch invulling aan de uitgangspunten

• Het college van B&W stelt als eindverantwoordelijke het IB Beleid vast.

• Het ConcernTeam (CT) stelt jaarlijks (of vaker als nodig) het IB Plan vast. In dit programma is aangegeven met welke maatregelen de grootste risico's van dat moment worden gemitigeerd.

• De gemeentesecretaris / Algemeen Directeur is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.

• De gemeentesecretaris / Algemeen Directeur is verantwoordelijk voor het vragen om informatie bij de CT-managers en lijnmanagers en ziet erop toe dat de CT-managers en lijnmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.

• De Chief Information Security Officer (CISO) ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. Indien de CISO van oordeel is dat zijn adviezen onvoldoende worden opgevolgd, rapporteert hij dat rechtstreeks aan de gemeentesecretaris / Algemeen Directeur. De keuze om van deze bevoegdheid gebruik te maken is exclusief voorbehouden aan de CISO (onafhankelijke positie).

• Er dient aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO in de beleidsvoorbereiding, besluitvorming en/of het handelen van de organisatie en in het kader van de P&C cyclus in het bijzonder. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen en – bij voldoende substantie – in de risicoparagraaf van de respectievelijke begrotingen voorzien van een risicoafweging, kwantificering en beheersmaatregelen.

• De lijnmanagers 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 zijn gesteld.

• Alle (interne en externe) medewerkers van de gemeente worden getraind/geïnformeerd in het gebruik van beveiligingsprocedures.

• Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.

• Lijnmanagers 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 zoals omschreven in het privacy beleid.
• De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Lijnmanagers voeren de baselinetoetsen uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

3.5 Randvoorwaarden

Belangrijke randvoorwaarden om dit beleid te implementeren zijn:

1. De informatiebeveiligingstaken zijn belegd binnen de bedrijfsprocessen en de benodigde kwalitatieve en kwantitatieve resources zijn beschikbaar gesteld ('Security & Privacy Professional', zie Bijlage C, Local Governance).

2. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures. Medewerkers kennen de beveiligingsprocedures en gebruiken deze procedures. Medewerkers zijn daarnaast op de hoogte van specifieke eisen die vanuit wet- en regelgeving aan hun bedrijfsprocessen gesteld worden en kennen deze kaders.

3. De informatiebeveiliging maakt deel uit van afspraken met ketenpartners en dienstenleveranciers.

4. Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd bij alle lagen binnen de organisatie, ketenpartners en externe partijen.

5. Er zijn voldoende maatregelen geïmplementeerd die zorgen dat kwetsbaarheden in bedrijfsprocessen worden verkleind. Hierdoor de kans op informatiebeveiligingsincidenten verkleind en de effecten van de incidenten beperkt.

6. Periodiek worden onafhankelijke audits uitgevoerd om vast te stellen of de vereiste maatregelen uit het beleid in voldoende mate zijn geborgd.

7. De digitale weerbaarheid wordt verhoogd door de basis op orde te brengen.

8. Security by design en privacy by design principes worden toegepast bij veranderingen en innovaties. Denk hierbij aan Common Ground, Internet of Things (IoT), Smart City en Omgevingswet, maar ook bij majeure wijzigingen in informatievoorziening (nieuwe toepassingen, nieuwe leveranciers etc).

9. Er is een werkend ISMS systeem aanwezig waarin risicomanagement volgens PDCA wordt gehanteerd, eigenaren van maatregelen zijn aangewezen én acties worden gemonitord. Het ISMS is tevens voorwaardelijk voor effectief en efficiënt afleggen van verantwoording (ENSIA).

10. Er is een werkend incident management proces en -systeem. 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. Denk hierbij aan trend-analyses.

3.6 Kwaliteitsborging: ISMS

Het Information Security Management System (ISMS) is een procesgerichte benadering voor informatiebeveiliging. Het is een managementsysteem waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd.
Het ISMS is de motor van de informatiebeveiligingsactiviteiten en wordt onderhouden middels de plan-do-check-act cyclus. Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn en of deze bijgesteld moeten worden. Het helpt ons onder andere om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid van de informatievoorziening en bedrijfscontinuïteit te waarborgen. Het ISMS (als proces) wordt beschreven in ISO27001 en voorgeschreven in de BIO. Het proces wordt ondersteund met een toolset.
De aanwezigheid van een 'levend' ISMS zorgt voor het effectief en efficiënt afleggen van verantwoording (ENSIA).

3.7 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsuitwerking en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Het legt de relatie tussen het Focusakkoord, wet- en regelgeving en de dagelijkse operatie.

4 Organisatie, taken en 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 (first en second line of defence). De derde lijn (CISO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. De ENSIA-coördinator in de derde lijn vormt een objectief oordeel voorzien met mogelijkheden tot verbetering.

4.1 Aansturing: concernteam

Het concernteam (CT) zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een lijnmanager. Het CT zorgt dat de lijnmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De eindverantwoordelijke portefeuillehouders worden door de CT-managers gevraagd en ongevraagd geïnformeerd 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.

Het CT stelt het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast. Ze draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. Het CT autoriseert de benodigde procedures en beleidsuitwerkingen (evenals uitzonderingen hierop). Het onderwerp informatiebeveiliging wordt in de gemeente Bergen op Zoom gezien als een integraal onderdeel van risicomanagement.

Wederzijds afstemmen en informeren geschiedt vier maal per jaar in het CT-overleg of zoveel vaker als de actualiteit daar om vraagt.

4.2 Uitvoering: lijnmanagers

Informatiebeveiliging valt onder de verantwoordelijkheid van de lijnmanagers . Om deze verantwoordelijkheid waar te maken, worden zij bijgestaan door een kwaliteitsmedewerker uit hun cluster / vakgroep. Hij is inhoudelijk op de hoogte van kwetsbaarheden en maatregelen en is tevens de liason tussen het cluster/vakgroep en de CISO; deze rol heet ‘Security & Privacy Specialist’. In het 3LoD model zijn deze specialisten de first of second line of defence. Het geheel van Security & Privacy Specialisten tezamen vormt het ‘Security & Privacy Forum’. Zie verder bijlage C ‘Local Government’.

Tenminste 2 keer per jaar is de CISO aanwezig bij een clusteroverleg om samen met de Security & Privacy Specialist invullling te geven aan het agendapunt ‘Informatieveiligheid’.

Taken van de lijnmanagers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen het eigen cluster uitdragen van het IB Beleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Besluiten tot het (niet) implementeren van beveiligingsmaatregelen om risico’s te mitigeren en daar ook de middelen voor beschikbaar stellen.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

4.3 Controle en verantwoording

Het vaststellen van het IB Beleid is een verantwoordelijkheid van het bestuur van de gemeente Bergen op Zoom. De bestuurders, de gemeentesecretaris/algemeen directeur en de managers in het CT geven volgens de 10 principes voor informatiebeveiliging richting en sturing aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het CT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Daarnaast rapporteert zij over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. Daartoe kunnen zij zich laten adviseren door de CISO.

4.3.1 ENSIA
De gemeente verantwoordt zich jaarlijks over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat een ENSIA-coördinator wordt aangewezen door de gemeentesecretaris / algemeen directeur. De ENSIA-coördinator is een projectmanager / procesbegeleider die zorgt dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA tijdig beschikbaar wordt gesteld namens de verantwoordelijke lijnmanagers. Zij 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 Bergen op Zoom 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 betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Bergen op Zoom informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

De ENSIA-coördinator bevindt zich in de ‘third line of defence’.
4.4 CISO mandaat
Indien het risico hierom vraagt, informeert en adviseert de CISO onverwijld de gemeentesecretaris/Algemeen Directeur in geval van (dreigende) overtreding van wet- en regelgeving of richtlijnen van hogere organen.
De CISO is bevoegd handelend op te treden en in te grijpen (dwingende instructies te geven). De CISO legt achteraf verantwoording af over dat handelend optreden. In de regels is hier sprake van bij (de dreiging van) high impact security incidents.
4.5 Inwerkingtreding
Het IB Beleid 2017-2020 wordt ingetrokken. Het IB Beleid 2021-2024 treedt in werking met ingang van de dag na bekendmaking in de B&W Besluitenlijst.
Het IB Beleid wordt aangehaald als: “Informatiebeveligingsbeleid gemeente Bergen op Zoom 2021-2024” of verkort “IB Beleid Bergen op Zoom 21-24”.

Aldus vastgesteld door burgemeester en wethouders van de gemeente Bergen op Zoom op 3 augustus 2021,

Dhr. J.L.A.M. Rutten, gemeente-secretaris a.i.
Dhr. Dr. F.A. Petter, burgemeester