Strategisch Gemeentelijk Informatiebeveiligingsbeleid

GEMEENTE MEIERIJSTAD
2020 tot 2023

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	09-10-2019	A. Hobbelen	Initiatie
0.2	26-11-2019	A. Hobbelen	Diverse reacties verwerkt
1.0	28-11-2019	A. Hobbelen	Definitieve versie

INHOUDSOPGAVE

1. INLEIDING

We leven in een informatiesamenleving. We zijn en worden in steeds grotere mate afhankelijk van betrouwbare informatiesystemen en data. Die afhankelijkheid wordt veroorzaakt door diverse ontwikkelingen die kansen bieden om de bedrijfsvoering en dienstverlening effectiever en efficiënter in te richten en te innoveren. Hierdoor kunnen we voldoen aan de (veranderende) behoeften en wensen van onze burgers, ondernemers, instellingen, (samenwerkings-)partners en onszelf.

Nieuwe technische en innovatieve ontwikkelingen bieden onze gemeente kansen voor het bereiken van haar doelstellingen. Deze kansen brengen echter ook risico's met zich mee die gemanaged moeten worden. Er is geconstateerd dat overheden steeds vaker het doelwit worden van cyberaanvallen. Digitale spionage, verstoring van de ICT, datalekken en diefstal van informatie nemen toe. Daarom is het belangrijk om informatieveiligheid te integreren binnen de (bedrijfsvoerings-)processen. Voor een professionele gemeentelijke organisatie die hoogwaardige producten en diensten aan haar inwoners moet leveren, is informatieveiligheid een randvoorwaarde.

Dit beleid beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot 2023 en vervangt het in 2017 vastgestelde 'Informatiebeveiliging en privacy beleid Meierijstad 2017-2020'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Het College van B&W geeft middels dit beleid op strategisch niveau duidelijk richting aan informatiebeveiliging.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023' 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 B. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG.

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 Informatiebeveiligingsplan (vastgesteld door het directieteam) worden de tactische en operationele richtlijnen en maatregelen verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de proceseigenaren, 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 alle andere gegevens

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

In 2018 is het informatiebeleid Gemeente Meierijstad vastgesteld. Het informatiebeleid beschrijft hoe de informatievoorziening bijdraagt aan de realisatie van de gemeentelijke doelstellingen. Het informatiebeleid geeft een lange termijnvisie op de ontwikkeling van de informatievoorziening van de gemeente, vormgegeven vanuit de visie en ambities van de gemeente Meierijstad (gewenste situatie) en het uitvoeren van wettelijke taken (wat moet).

In het informatiebeleid is de visie van de gemeente vertaald naar strategische uitgangspunten en doelen voor het informatiedomein. Vanuit doelen, ambities en wettelijke verplichtingen zijn een vijftal beleidssporen geïdentificeerd om de informatievoorziening te ontwikkelen. Een van die sporen is spoor 5: Informatievoorziening op orde. In dit spoor is de opgave Informatiebeveiliging opgenomen waarbij de volgende richtlijnen en ambities zijn beschreven:

De gemeente voert de BIO in.
Met de Baseline Informatiebeveiliging Overheid (BIO) hebben gemeenten een hulpmiddel om aan alle eisen voor informatiebeveiliging te voldoen. Informatiebeveiliging is een integraal onderdeel van de bedrijfsvoering en van de keuzes die het directieteam maakt.

Bewustzijn informatieveiligheid in organisatie is hoog.
Omdat informatieveiligheid en privacy ten dele technisch kunnen worden geborgd en afhankelijk is van menselijk handelen is bewustzijn op dit gebied erg belangrijk.

Meierijstad zorgt voor een balans tussen veiligheid, functionaliteit en bruikbaarheid, zodat gegevens en de informatiesystemen meetbaar betrouwbaar, integer en beschikbaar zijn.
Bij elke ontwikkeling op gebied van informatievoorziening spelen gebruik en beheer een voorname rol. Ook worden eisen gesteld aan de robuustheid van technologie, of de oplossing toekomst vast is, dat de informatiebeveiliging op orde is, privacy gewaarborgd is en dat bij datalekken snel inzichtelijk gemaakt kan worden aan wie welke data gelekt is. De gegevens en de informatiesystemen zijn hierdoor meetbaar betrouwbaar, integer en beschikbaar.

Deze richtlijnen en ambities zijn opgenomen en verwerkt in dit informatiebeveiligingsbeleid. Hierdoor wordt de visie van Meierijstad via het informatiebeleid verder uitgewerkt naar concretere richtlijnen en maatregelen op het gebied van informatiebeveiliging.

2. STRATEGISCH BELEID

2.1 Doel

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

2.2 Ontwikkelingen

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

2.2.1 De BIO

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

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging[1] zijn een bestuurlijke aanvulling op het normenkader [2] 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.

[1] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
[2] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

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

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[3] 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 (IBP)’.

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 AVG, BRP, PNIK en SUWI . Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende)

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

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.
Privacy specifieke beleidsaspecten zijn opgenomen in een apart privacy beleid. In dit beleid is wel rekening gehouden met dit beleid.

2.6 Uitgangspunten

Het bestuur, het directieteam en de proceseigenaren spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het directieteam 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 directieteam dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
Het bestuur, het directieteam en de proceseigenaren geven 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.

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Het college van B en W eindverantwoordelijke voor de informatiebeveiliging.
- Het opstellen en de uitvoering van de informatiebeveiligingsbeleid is een verantwoordelijkheid van de gemeentesecretaris.
- De proceseigenaren zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.

- Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Meierijstad 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.
- De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader dat we hanteren. Op basis van risicomanagement worden de prioriteiten bepaald.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Dit beleid is van toepassing op:
  - alle medewerkers die bij of namens de gemeente werkzaam zijn (ook uitzend- en inhuurkrachten, stagiaires en trainees);
  - alle bedrijfsvoering processen, onderliggende informatiesystemen en informatie van de gemeente (in de meest brede zin van het woord);
  - alle (fysieke) ruimten van het gemeentehuis en aanverwante gebouwen zoals de neven- en dislocaties. Alsmede op de apparatuur die door gemeente ambtenaren gebruikt worden bij de uitoefening van hun taak op diverse locaties.
  - alle informatiesystemen waarop informatie verwerkt wordt door of namens gemeente ambtenaren (zowel binnen als buitenhuis).
  - de Algemene Verordening Gegevensbescherming (AVG), het normenkader Suwinet (SUWI), de basisregistratie Adressen en Gebouwen (BAG), de basisregistratie Grootschalige Topografie (BGT), de basisregistratie Ondergrond (BRO), de paspoort uitvoeringsregeling (PUN), het regelement rijbewijzen, de basisregistratie Personen (BRP), de basisregistratie WOZ en de archiefwet.
- 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.
- Dit beleid is locatie-onafhankelijk. Indien medewerker of derden zich op een locatie bevindt anders dan een van de gebouwen van de gemeente Meierijstad, maar wel met informatie of informatievoorziening van de gemeente Meierijstad werkt (thuiswerken, webmail, onderhoud buiten), dient men dit beleid te respecteren.
- Bij samenwerking met derden waarbij sprake is van uitwisseling van gegevens, waarvan de gemeente eigenaar of beheerder is, moet informatiebeveiliging een onderdeel zijn in de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente Meierijstad.
- Bewustwording van informatiebeveiliging creëren en vergroten is nodig voor het verbeteren van de houding ten opzichte van informatiebeveiliging en het willen veranderen van onveilig gedrag naar veilig gedrag.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt elke 3 jaar als eindverantwoordelijke het strategisch gemeentelijk informatiebeveiligingsbeleid vast.
- Jaarlijks wordt het informatiebeveiligingsplan herijkt en door het directieteam vastgesteld.
- De jaarlijkse evaluatie over de uitvoering van het informatiebeveiligingsbeleid (via ENSIA) wordt vastgesteld door het college van B&W.
- Het directieteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het directieteam ziet erop toe dat de proceseigenaren adequate maatregelen nemen of 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 het directieteam, voorafgaand aan de P&C-gesprekken.
- In bijzondere gevallen waarbij de veiligheid van de organisatie in het gedrang komt of dreigt te raken zal de CISO rechtstreeks rapporteren aan de gemeentesecretaris of portefeuillehouder.
- 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.
- Aan alle medewerkers van de gemeente wordt actief kennis bijgebracht over informatiebeveiliging en worden terugkerend getraind in het gebruik van beveiligingsmaatregelen en -procedures.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Proceseigenaren voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement.
- De rollen, taken en verantwoordelijkheden van de organisatiestructuur die betrekking heeft op informatiebeveiliging (zie bijlage A) worden onderschreven en ingevoerd.
- Kennis en bewustzijn van informatiebeveiliging binnen de organisatie dienen periodiek actief bevorderd en geborgd te worden.
- 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.
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.

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 zijn de proceseigenaren verantwoordelijk voor de eigen processen. De tweede lijn (CISO) 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. In bijlage A wordt de governance structuur met betrekking tot informatiebeveiliging verder uitgewerkt.

3.1 Aansturing: directieteam

Het directieteam zorgt dat alle processen en informatiesystemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een proceseigenaar. Het directieteam zorgt dat de proceseigenaren zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het directieteam 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.

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

3.2 Uitvoering: proceseigenaren

Informatiebeveiliging valt onder de verantwoordelijkheden van alle proceseigenaren. 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. Proceseigenaren rapporteren aan het directieteam over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de werkateliers over inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in de werkatelieroverleggen.

Taken van de proceseigenaren in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen processen en werkateliers uitdragen van het beveiligingsbeleid en 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.

3.2.1 Informatiebeveiligingsplan

Na vaststelling van dit beleid zal het informatiebeveiligingsplan opgesteld worden. Het informatiebeveiligingsplan wordt opgesteld op basis van een Risico Inventarisatie & Evaluatie en een GAP analyse. De GAP-analyse is een 0-meting. De uitkomst van de analyse laat zien waar onze organisatie staat ten opzichte van de Baseline Informatiebeveiliging Overheid (BIO). In deze baseline staan beheersmaatregelen op het gebied van informatiebeveiliging die moeten worden uitgevoerd. Jaarlijks toetsen wij waar we staan ten opzichte van de maatregelen uit de BIO. Wij actualiseren op basis daarvan jaarlijks het Informatiebeveiligingsplan die vervolgens door het directieteam wordt vastgesteld.

In het informatiebeveiligingsplan wordt beschreven welke maatregelen geïmplementeerd moeten worden en welke niet. Er wordt beschreven op welke manier de maatregelen geïmplementeerd moeten worden en door wie (planning). De structuur van het plan is tevens afgestemd op de structuur van de BIO. Indien van toepassing worden activiteiten uit het informatiebeveiligingsplan verder uitgewerkt in afzonderlijke projectplannen. Het voldoen aan de BIO zal een behoorlijke inspanning vereisen. Daarom zullen de werkzaamheden in jaarplannen worden opgesplitst.

Het informatiebeveiligingsplan wordt elk jaar herijkt en vastgesteld door het directieteam. Het informatiebeveiligingsplan is gebaseerd op:

- uitgevoerde risicoanalyses;
- beveiligingsincidenten die hebben plaatsgevonden;
- nieuwe ontwikkelingen;
- de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA).

3.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente Meierijstad. De bestuurders en directeuren van de gemeente Meierijstad 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.
Het directieteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het directieteam 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 is aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaren. De proceseigenaren leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

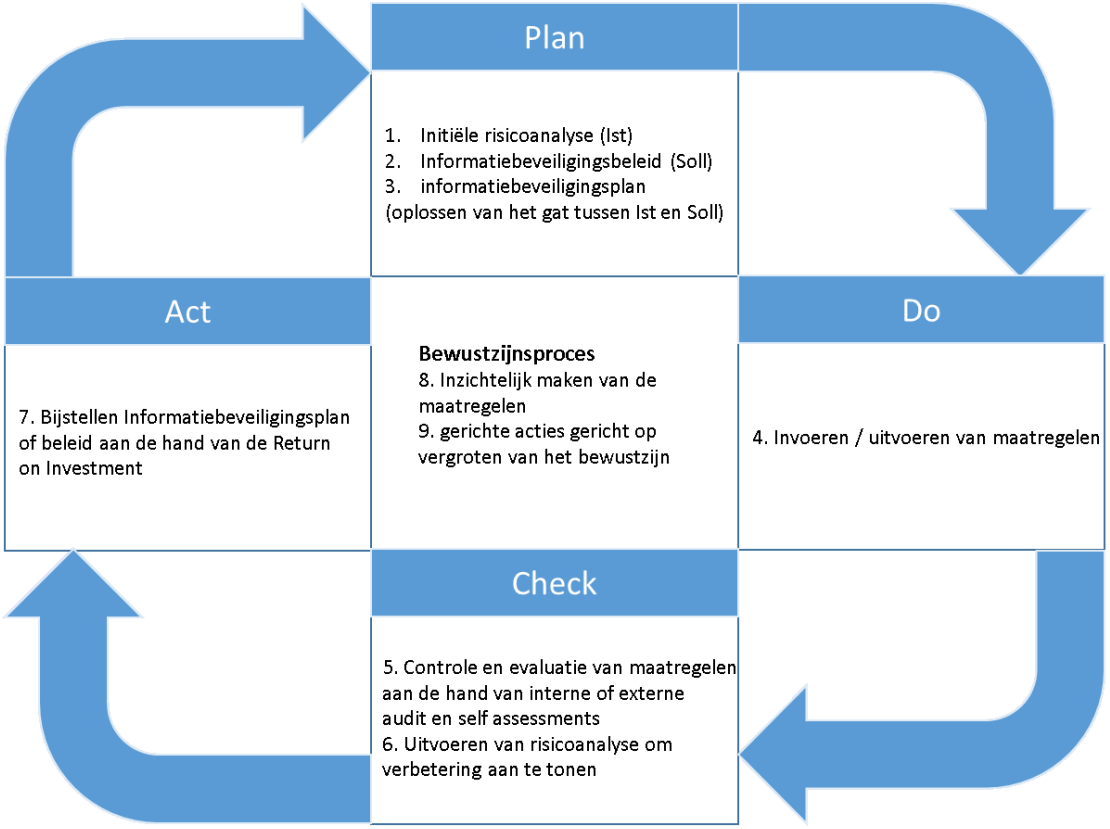
De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording

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

3.3.2 Borging informatiebeveiligingsbeleid

Om borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen, onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Hoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA cyclus:



Bijlage A GOVERNANCE STRUCTUUR INFORMATIEBEVEILING

Doelstelling

In de governance structuur benoemen we het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en verankeren we de hieraan verbonden verantwoordelijkheden.

Verantwoordelijkheidsniveaus binnen de gemeente Meierijstad

Het college van Burgemeester en Wethouders is eindverantwoordelijk voor informatiebeveiliging binnen de gemeente Meierijstad. Met het bekrachtigen van het beleid ten aanzien van informatiebeveiliging belegt het college van B&W de uitvoering en naleving hiervan bij het ambtelijk apparaat.

Binnen de gemeente Meierijstad worden de volgende verantwoordelijkheid- en takenniveaus met betrekking tot informatiebeveiliging onderscheiden:

Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het College van B&W van de gemeente Meierijstad draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatiebeveiligingsbeleid en stimuleert het directieteam om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan de gemeentesecretaris. De gemeentesecretaris draagt de ambtelijke eindverantwoordelijkheid voor de informatiebeveiliging en continuïteit. De verantwoordelijk portefeuillehouder draagt de bestuurlijke verantwoordelijkheid.

Controlerende verantwoordelijkheden op bestuurlijk niveau
De gemeenteraad heeft een controlerende rol. Zij kunnen, bijvoorbeeld naar aanleiding van incidenten en berichten uit de media, het college van B&W bevragen ten aanzien van risico beperkende maatregelen welke getroffen zijn binnen de organisatie. Ook kunnen zij regulier vragen om, of geïnformeerd worden over de staat van informatiebeveiliging binnen de organisatie. Voor raadsleden is het belangrijk om te weten dat eventuele financiële-, technische, en imagoschade van de geïnventariseerde risico's bij een incident beperkt blijft en dat de privacy van burgers of de integriteit van de gemeente nooit in het geding zijn.

Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de gemeentesecretaris. Deze stelt met het directieteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst samen met het directieteam voor ieder proces een proceseigenaar aan. De verantwoordelijkheid voor de informatie, de systemen en informatieprocessen binnen de verschillende processen is belegd bij de proceseigenaren op organisatieniveau.

Verantwoordelijkheden en taken op werkatelier en procesniveau
Alle informatiebronnen en –systemen hebben een proceseigenaar welke de waarde bepaalt van de informatie die ze bevatten. De proceseigenaren zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun bedrijfsproces. Applicatie-, systeem-, gegevens-, archief en procesbeheerders zijn expliciet geen proceseigenaren, maar zijn uitvoeringsverantwoordelijk voor een belangrijk deel van de informatiebeveiliging. De proceseigenaren zijn verantwoordelijk voor de uitvoering van de informatiebeveiligingsbeleid door de werkateliers.

Functies, rollen en werkateliers die betrokken zijn bij informatiebeveiliging

College van Burgemeester en Wethouders
Het College van B&W is bestuurlijk verantwoordelijk voor informatiebeveiliging en stelt als eindverantwoordelijke het strategisch gemeentelijk informatiebeveiligingsbeleid vast. Door middel van dit beleid geeft zij op strategisch niveau duidelijk richting aan informatiebeveiliging. Met betrekking tot informatiebeveiliging legt het College tevens jaarlijks verantwoording af aan de Raad.

Gemeente secretaris
Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de gemeente secretaris verantwoordelijk voor de uitvoering van organisatie brede vraagstukken ten aanzien van informatiebeveiliging.

Themadirecteuren
De themadirecteuren zijn samen met de secretaris verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid in de organisatie.

Chief Information Security Officer (CISO)
De CISO is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico’s evenals het opstellen van rapportages.

Proceseigenaren
De proceseigenaar is de eigenaar en verantwoordelijke van een of meerdere ketenprocessen. Hij of zij organiseert medewerkers, procescoaches en procesbeheerders in een project. Is de opdrachtgever voor de aanpassingen binnen een ketenproces en verantwoordelijk voor het behalen van de vooraf opgestelde doelen, continu verbeteren en te behalen resultaten. Is ook verantwoordelijk voor de borging van informatiebeveiliging in het desbetreffende proces.

Procesbeheerders
De procesbeheerder is verantwoordelijk van een proces op gebied van de inhoud. Is inhoudsdeskundige van het proces: direct betrokken en weet waar de knelpunten zitten. Zorgt voor tijdige bijsturing van het proces in de PDCA-cyclus wanneer nodig (feedback, houding en gedrag). Verantwoordelijk voor doorvoeren van veranderingen in het proces en bijkomende zaken. Uitvoerende van 2e lijncontroles op het gebied van rechtmatigheid en kwaliteit.

De beveiligingsbeheerder
Deze rol geldt ten aanzien van de specifieke gegevensverzamelingen of deelgebied. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen of deelgebieden. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling of deelgebied toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de gegevensverzamelingen en deelgebieden waarbij een beveiligingsbeheerder is aangewezen: BRP, Reisdocumenten, Rijbewijzen, BAG, SUWI, BGT, WOZ, DigiD, Informatiebeheer, P&O, Vastgoed, ICT en Inkoop.

Het werkatelier ICT
Het werkatelier ICT-beheer beheert de werkplekken, serverplatformen, lokale netwerken, WiFi verbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de proceseigenaar voor (informatie)systemen afgelegd.

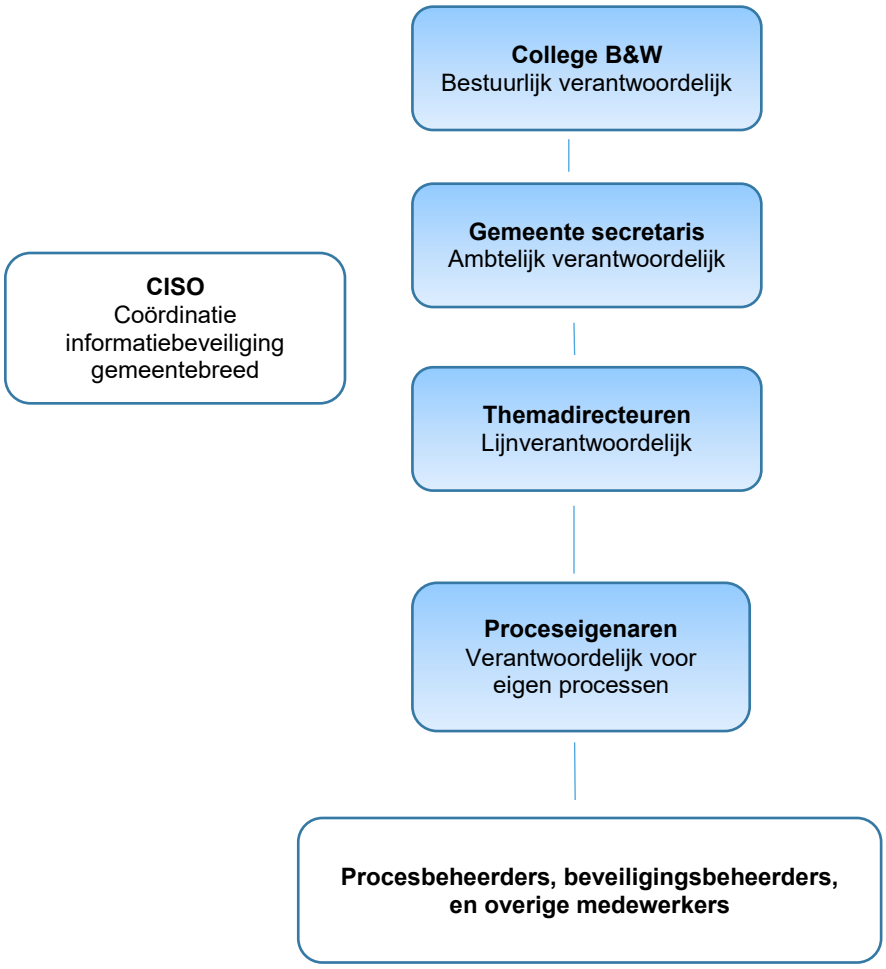
Werkatelier Vastgoedbeheer en werkatelier Facilitaire diensten
Het werkatelier Vastgoed is verantwoordelijk voor de fysieke toegangsbeveiliging (beleid en implementatie). Het werkatelier facilitaire zaken voor de kantoorinrichting (archiefkasten, kluizen enzovoort).

Werkatelier P&O Advies en Beleid
Het werkatelier P&O is verantwoordelijk voor de advisering en deels uitvoering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke rol op het gebied van organisatie en informatieprocessen.

Werkatelier Inkoop
Het werkatelier Inkoop is verantwoordelijk voor de advisering inzake alle inkoop aspecten bij de gemeente en speelt hiermee een belangrijke rol bij het inkoopproces waar informatiebeveiliging een van de meegenomen aspecten is.

Werkatelier Functioneel beheer
De applicatiebeheerders zijn verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.

De medewerkers
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien de betrouwbaarheid, de integriteit en de beschikbaarheid van de informatieprocessen waarbij zij zijn betrokken.



Figuur 1: Functies en rollen in informatiebeveiligingsorganisatie

Toewijzing verantwoordelijkheden voor informatiebeveiliging

Verantwoordelijkheden gemeentesecretaris en themadirecteuren (het directieteam):
- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op concern risico's;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging;
- Het aanwijzen van de CISO.

Verantwoordelijkheden proceseigenaren:
- Het uit (laten) voeren van maatregelen uit het informatiebeveiligingsplan die binnen de werkateliers van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de informatiesystemen van de werkateliers;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de CISO, over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages.

Taken en verantwoordelijkheden CISO
- Stelt samen met werkatelier IS en andere i-betrokkenen het informatiebeveiligingsbeleid op en actualiseert deze elke 3 jaar.
- Stelt het jaarlijks informatiebeveiligingsplan op en monitort de uitvoering van de informatiebeveiligingsmaatregelen uit het plan.
- Houdt toezicht op de in- en uitvoering van de beveiligingsmaatregelen.
- Voert samen met de proceseigenaren de GAP analyses uit en adviseert waar en wanneer extra maatregelen nodig zijn
- Evalueert en rapporteert jaarlijks in de P&C management rapportages over de informatiebeveiliging van de gemeente.
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatiebeveiliging;
- Is verantwoordelijk voor het inrichten van het proces rondom beveiligingsincidenten, het adequaat handelen hierin, het evalueren en het documenteren hiervan.
- Is aanspreekpunt en geeft ondersteuning aan de hele organisatie met kennis over informatiebeveiliging.
- Bevordert het bewustzijn met betrekking tot informatiebeveiliging.
- Ondersteunt het directieteam, proceseigenaren en de werkateliers met kennis over informatiebeveiliging.
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

Plaats in de organisatie
De rol van CISO wordt vervuld door een informatie adviseur van het werkatelier Informatiestrategie. De CISO rapporteert over de uitvoering van het informatiebeveiligingsbeleid en -plan aan het directieteam. Om de continuïteit en kwaliteit te waarborgen is een collega uit hetzelfde atelier aangewezen als back-up van de CISO. Deze persoon treedt op als vervanger bij afwezigheid van de CISO.

Onafhankelijke rol/signaalfunctie
De CISO heeft een onafhankelijke positie tegenover zowel het lijnmanagement als het bestuur van de gemeente. De CISO staat midden in de organisatie, heeft een directe rapportagelijn naar de (eindverantwoordelijke) gemeentesecretaris, het directieteam en de (bestuurlijk) portefeuillehouder en heeft daarmee periodiek overleg. Daarnaast is de CISO verbonden met de ambtelijke organisatie en heeft inzicht in het primaire proces. De CISO heeft als uitdaging om soms tegengestelde bedrijfs- en beveiligingsbelangen met elkaar te verenigen. Dat vereist een generalistische kijk op informatiebeveiliging en een flexibele benadering van verschillende stakeholders binnen de organisatie.

Bijlage B BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO)

Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Rijk, Gemeenten, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. Helder, actueel en veilig.

Het volledige normenkader is te vinden via de volgende link:
https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Meierijstad zijn we samen!