Gemeente Midden-Delfland

GEMEENTEBLAD

Officiële uitgave van de gemeente Midden-Delfland

Nr. 564443

28 december 2023

Strategisch Informatiebeveiligingsbeleid Gemeente Midden-Delfland 2023-2026

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 tot 2026. Het vervangt het vastgestelde "Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Midden-Delfland 2020 -2023.

Deze nota geeft richting en stelt kaders. We geven uitvoering aan deze nota met onderwerp specifieke beleidsdocumenten en werkinstructies over informatiebeveiliging. Dit doen we op zowel tactisch als operationeel niveau.

Met dit 'Strategisch Informatiebeveiligingsbeleid Gemeente Midden-Delfland 2023-2026' zetten we de volgende stap om de beveiliging van informatie zoals persoonsgegevens binnen de gemeente te continueren. Zo gaan we door op de basis die we de afgelopen jaren hebben gelegd. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Het is daarnaast gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage 1.

Leeswijzer
In hoofdstuk 2 beschrijven we de kern van het strategisch beleid. Dit beleid vullen we op tactisch niveau aan met onderwerp specifieke beleidsregels.

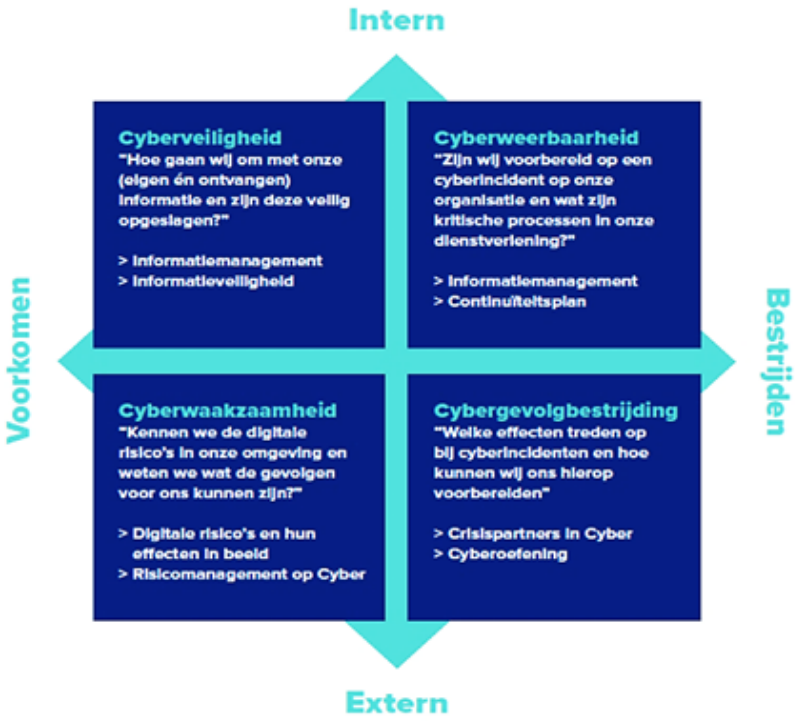
Het is onmogelijk om alle informatiebeveiligingsmaatregelen uit de BIO binnen korte tijd op orde te hebben, dit vraagt jaren waar meerdere disciplines van de organisatie bij betrokken zijn.

We stellen daarvoor jaarlijks een overzicht op van verbeterpunten op onze informatiebeveiliging. We noemen dit vervolgens ons Informatiebeveiligingsplan. Dit is als hoofdstuk opgenomen in ons jaarverslag informatiebeveiliging. Dit jaarverslag stelt het directieteam daarna vast. In het Informatiebeveiligingsplan werken we de tactische en operationele onderdelen van de informatiebeveiliging op basis van risicoanalyse verder uit met prioritering van concrete maatregelen.

Dit doen we met:
- de output vanuit ons op het BIO-normenkader gebaseerde Information Security System (ISMS)
- het IBD dreigingsbeeld
- de resultaten van de ENSIA verantwoording
- de input van de afdelingsdirecteuren en de CISO.

In het betreffende Informatiebeveiligingsplan beschrijven we ook de acties en planning. Zo brengen we de praktijk in overeenstemming met dat wat we in het beleid eisen.

In hoofdstuk 3 beschrijven we hoe we de taken en verantwoordelijkheden in de organisatie beleggen.



Figuur 1.1: Aandachtsgebieden informatiebeveiliging

2. Wat is informatiebeveiliging?

Onder informatiebeveiliging verstaan we het nemen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te beschermen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente. Het borgt daarmee de informatievoorziening tijdens 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.

3. Ambitie en visie van de gemeente op het gebied van informatieveiligheid

COALITIEAKKOORD OP HOOFDLIJNEN 2022-2026
De coalitie in Midden-Delfland wordt gevormd door de fracties CDA, VVD en D66 Midden-Delfland.

Na de gemeenteraadsverkiezingen in maart 2022 stelden de collegepartijen een hoofdlijnenakkoord op met als motto 'Midden-Delfland heeft het!'.

Twee thema's hieruit zijn 'Informatie op orde' en 'ICT'.

Informatie op orde
Door de toenemende digitalisering en de bijbehorende cyberdreigingen is digitale veiligheid van groot belang voor de gemeente. We willen slimmer werken en werken daarom vaak datagedreven. Want in een tijd waarin data in overvloed aanwezig is, kan Midden-Delfland hier gebruik van maken. Veiligheid, privacy en betrouwbaarheid staan hierbij voorop. Het is noodzakelijk dat we aandacht houden voor online veiligheid en voldoen aan de relevante informatiebeveiligingseisen. Bij het gebruik van slimme technologieën kijken we naar de waarborgen voor privacy, gelijke behandeling van personen, vrijheden en de rechtsstaat. Daarnaast willen we voorkomen dat we te afhankelijk zijn van IT-leveranciers en bestuurlijke partners.

ICT
Voor de informatievoorziening is ICT onmisbaar. De toenemende digitalisering biedt mogelijkheden om de gemeentelijke dienstverlening en bedrijfsvoering te verbeteren. In 2021 heeft de gemeenteraad ingestemd met het Informatiebeleidsplan. Dat plan is voor ons een instrument om de dienstverlening verder te verbeteren. Onlosmakelijk aan dit plan zijn lopende projecten gekoppeld, zoals de verbeteraf-

spraken binnen het sociaal domein, de implementatie van het Digitaal Stelsel Omgevingswet en het actualiseren van de dienstverleningsovereenkomst met het Westland. Wij verwachten van het college dat zij de gemeenteraad regelmatig informeert over de ontwikkelingen en voortgang.

4. Strategisch beleid

5. 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).

6. Regelgeving en Ontwikkelingen
De volgende ontwikkelingen zijn van belang voor de actualisering van het informatiebeveiligingsbeleid:

7. 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. De interbestuurlijke werkgroep Normatiek ondersteunt gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid. Deze werkgroep heeft daarvoor in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht. Deze is afgeleid van beide NEN-normen. De 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.

8. De Baseline Informatiebeveiliging Overheid
De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor de hele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat betekent dat de afdelingsdirecteuren verantwoordelijk zijn voor het werken volgens de aanpak van de ISO 27001. Hierbij is risicobeheersing belangrijk. Dit houdt voor het management in, dat zij van tevoren keuzes maakt en steeds afwegingen maakt of we informatie goed beveiligen. Daarbij gaat het om de onderdelen beschikbaarheid, integriteit en vertrouwelijkheid, in zowel nieuwe als bestaande processen.

9. De Europese Network and Information Systems Directive (NIS2)
De nieuwe Network and Information Systems Directive (NIS2-richtlijn) heeft belangrijke implicaties voor gemeenten als het gaat om toezicht op informatiebeveiliging. In tegenstelling tot de oorspronkelijke richtlijn (uit 2016) vallen (lokale) overheidsinstanties nu ook onder de NIS2.

De richtlijn is sinds begin 2023 van kracht. EU-lidstaten zijn verplicht deze uiterlijk 17 oktober 2024 in nationale wetgeving om te zetten. Eén van de vragen is alleen of en in hoeverre wij als gemeente onder deze richtlijn vallen.

Zorgplicht, meldplicht en sancties
In Nederland is het ministerie van Justitie en Veiligheid (J&V) verantwoordelijk voor het opstellen van de Wet beveiliging netwerk- en informatiesystemen (Wbni), waarin de NIS2-richtlijn is opgenomen. In het kader van de zorgplicht worden de normen uit de Baseline Informatiebeveiliging Overheid (BIO) in de Wbni opgenomen, ook voor gemeenten. Er komt een wettelijke meldplicht voor incidenten op informatiebeveiliging en er komen sanctie te staan op inbreuken op de NIS2-richtlijn.

Onduidelijkheid over de toepasselijkheid op gemeenten
De uitwerking van NIS2 vergt een nauwe samenwerking tussen verschillende ministeries, zoals BZK, J&V, I&W en VWS en lokale overheden. Een aantal zaken zijn nog onduidelijk. De belangrijkste vragen houden verband met de toepasselijkheid van de richtlijn op Nederlandse gemeenten en hoe dit zich verhoudt tot bestaande structuren als de BIO, ENSIA en de informatiebeveiligingsdienst voor gemeenten. Denk hierbij bijvoorbeeld aan verkeer, weg- en waterbeheer en de zorgsector. Dit zijn processen die in de NIS2-richtlijn met name zijn genoemd en die in Nederland lokaal georganiseerd zijn. Van deze nadere regelgeving is nog niet duidelijk wat de exacte scope wordt en dus ook niet wat de impact op gemeenten zal zijn.

Het gaat dan om:
- duidelijkheid over de scope en de verantwoordelijkheidsverdeling tussen de betrokken partijen;
- geharmoniseerd toezicht op informatiebeveiliging bij de overheid;
- vermindering van de auditlast;
- haalbare en uitvoerbare regelgeving voor lokale overheden.

Nu al aan de slag
We hebben als gemeente nu al een zorgplicht (BIO), een meldplicht (Informatiebeveiligingsdienst, IBD) en toezicht (Eenduidige Normatiek Single Information Audit, ENSIA). Daardoor is de impact van NIS2 voor ons afhankelijk van de mate waarin we nu al gedocumenteerd voldoen aan de BIO. Het is dus cruciaal dat we als gemeente door blijven gaan met de cyclus van plannen, uitvoeren, controleren en bijstellen rondom de complete BIO.

De NIS2 regeling en de uitwerking van de Wbni staat niet op zich. Tussen nu en 2026 krijgen de gemeenten te maken met 13 nieuwe regelgevende initiatieven op het gebied van digitalisering en cybersecurity. De wetten moeten in samenhang worden bekeken, niet afzonderlijk. VNG stelt hiertoe een impactanalyse op.

10. Nieuw versie BIO2.0 krijgt een wettelijke basis.
Bij het vaststellen van de landelijke Baseline Informatiebeveiliging Overheid (BIO) is afgesproken dat deze in 2023 geëvalueerd zou worden. Maar omdat er een nieuwe versie van ISO 27002 (internationale IB standaard) gepland was voor 2022, is besloten de beoordeling naar voren te halen naar 2022. Dit om te voorkomen dat er twee keer nieuwe versies van de BIO zouden worden vastgesteld. In de nieuwe BIO 2.0 worden de beoordeling van de BIO (om te bepalen hoe die herschreven moet worden) en de aanpassing van de structuur (vanwege de nieuwe ISO 27002) samengevoegd.

Het rapport over de evaluatie van de Baseline Informatiebeveiliging Overheid (BIO) is in november 2022 voltooid. Uit de evaluatie bleek dat de BIO een belangrijk instrument is waarin de overheid blijft investeren.

De komst van de Europese NIS2-richtlijn heeft de geplande opleverdatum van de BIO 2.0 veranderd. In een brief aan de Kamer in februari 2021 staat dat de overheid informatieveiligheid een wettelijke basis wil geven. De staatssecretaris van Digitalisering wil dit doen door een zorgplicht in te voeren, waarbij nadere regels kunnen worden opgesteld, zoals die in de BIO.

De BIO wordt wettelijk vastgelegd in de Wbni (Wet beveiliging netwerk- en informatiesystemen), die de NIS2 (Europese richtlijn) omzet in nationale wetgeving. De NIS2 heeft een bredere reikwijdte, waarbij ook de overheid onder de regels valt. De omzetting van de NIS2 is momenteel aan de gang. In oktober 2024 wordt de Wbni van kracht, waarin de BIO wettelijk is verankerd.

Om niet tot 2024 te hoeven wachten op een nieuwe versie van de BIO, werkt de landelijke werkgroep BIO aan een voorbereidende BIO 2.0-handleiding. Hierin worden alle goedgekeurde wijzigingen van de BIO verwerkt. Ook worden maatregelen die niet langer voldoen aan de huidige bedreigingen bijgewerkt. Bovendien worden de maatregelen afgestemd op de nieuwste versie van ISO 27002: NEN-EN-ISO 27002:2022. Hiermee wordt de toekomstige richting van de huidige BIO duidelijk.

Aangezien de ontwikkeling van BIO naar BIO 2.0 vanwege de wettelijke verankering van de NIS2 is vertraagd, worden de gerelateerde producten voor BIO 2.0 opnieuw geprioriteerd en in een lager tempo aangepast. Dit wordt gedaan om ervoor te zorgen dat de aanverwante producten tegelijkertijd kunnen worden voltooid met de implementatie van BIO 2.0 in oktober 2024.

11. Specifiek beleid op beveiliging van gemeentelijke webapplicaties
Eind 2022 is een aanvulling op het huidige informatiebeveiligingsbeleid gemaakt vanwege een toevoeging van een nieuwe beveiligingsrichtlijn (B.01) van de 'Norm ICT-beveiligingsassessments DigiD' versie 3.0 van Logius waaraan gemeenten moeten voldoen. Deze wijziging door Logius is per 1 augustus 2022 van kracht geworden. Het gaat om de volgende beveiligingsrichtlijn:

"De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer."

Deze aanvulling is op 22 december 2022 vastgesteld en blijft van kracht.

12. De 10 principes voor informatiebeveiliging
De hieronder aangegeven 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO. Zij gaan over de waarden die de bestuurder zichzelf oplegt.
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 calculeren we in.
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. Een incident met onze informatiebeveiliging binnen de gemeentelijke processen, kan directe gevolgen hebben voor onze inwoners, ondernemers en partners. Daarmee moet informatiebeveiliging beslist een belangrijk onderwerp zijn voor de bestuurders.

13. Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

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

14. Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin we incidenten vastleggen. Dit systeem geeft ook waardevolle informatie om van te leren. Zo zijn onze eigen beveiligingsincidenten uit het verleden ook beslist input bij het actualiseren van ons beleid.

15. Plaats van het strategisch beleid

Het strategisch beleid beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid vertalen we naar tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden werken we uit in het jaarlijkse ‘Informatiebeveiligingsplan’ zoals opgenomen in het jaarverslag Informatiebeveiliging.

16. Scope informatiebeveiliging

De scope van dit informatiebeveiligingsbeleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie). Daarnaast omvat het ook 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 onder andere voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI).

17. Uitgangspunten

Het bestuur, het directieteam en het afdelingsmanagement spelen een belangrijke rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang van de verschillende delen van de informatievoorziening voor de gemeente. Maar ook een inschatting van 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. Dit doet zij door het uitdragen en handhaven van het informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de hele organisatie, op 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.

18. 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.

19. 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 burgemeester en wethouders is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die we in de gemeente Midden-Delfland gebruiken, hebben een interne eigenaar. Deze bepaalt de vertrouwelijkheid en/of waarde 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, organisatie brede planning én coördinatie verankeren we de kwaliteit van de informatievoorziening 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. Dit doet zij volgens dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid moeten worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel in vaste als tijdelijke dienst, intern of extern, heeft verplichtingen aangaande informatiebeveiliging. De medewerker is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht. Bij vermeende inbreuken maakt hij hiervan melding.

20. Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van burgemeester en wethouders stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- Het directieteam stelt jaarlijks het in het jaarverslag informatiebeveiliging opgenomen informatiebeveiligingsplan vast.
- Het directieteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het directieteam is verantwoordelijk voor het vragen om informatie bij de afdelingsdirecteuren en/of teamleiders. Zij ziet erop toe dat de afdelingsdirecteuren adequate maatregelen laten nemen 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. De CISO rapporteert hierover rechtstreeks aan het directieteam, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken moet aandacht zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in de auditplannen.
- De afdelingsdirecteuren zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De basiskernregistraties (zoals Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI)) en toekomstige basisregistraties zijn belangrijk in het kader van informatiebeveiliging. Zij krijgen echter niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. De samenhang van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de gestelde doelen.
- Alle medewerkers van de gemeente trainen we in het gebruik van beveiligingsuitgangspunten en procedures.
- Medewerkers gaan veilig om met persoonsgegevens en andere informatie.

- Afdelingsdirecteuren zien erop toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd. Zo kunnen zij vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen bepalen we op basis van risicomanagement. Afdelingsdirecteuren dragen zorg voor de uitvoering van op de BIO gebaseerde quickscans om deze risico-afwegingen te kunnen maken.

21. 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 moeten actief bevorderd en geborgd worden.
- Jaarlijks stellen we een informatiebeveiligingsplan op onder leiding van de Chief Information Officer (CIO), gebaseerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - het dreigingsbeeld gemeenten van de IBD;
  - de door de afdelingsdirecteuren en teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

22. Organisatie, taken & verantwoordelijkheden

Om het beleid op het gebied van informatieveiligheid gedegen vorm te kunnen geven en in de organisatie op zowel bestuurlijk als ambtelijk niveau te borgen, heeft de gemeente een aantal rollen ingericht en verantwoordelijkheden belegd. Naast een aantal specifieke rollen, die belegd zijn in de organisatie, heeft iedere medewerker de verantwoordelijkheid om gevoelige gegevens te beschermen. Leidinggevenden hebben daarnaast de verantwoordelijkheid om daarop te sturen en bewustzijn over informatieveiligheid en privacywetgeving te creëren.

Het bestuur, het managementteam en de lijnmanagers spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening 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.

Bestuur en management worden daarbij ondersteund door de coördinator informatieveiligheid (CISO), de functionaris gegevensbescherming (FG) en de informatiebeveiligingsbeheerders binnen de diverse afdelingen en teams. Sommige teams kennen op dit gebied daarnaast nog enkele specialistische functies, zoals bijvoorbeeld de security officer Suwinet en de beveiligingsfunctionaris waardedocumenten.

De invulling van de organisatie van de informatiebeveiliging zoals die in 2015 is vastgesteld, wordt als maatregel geactualiseerd naar de huidige organisatiestructuur. Hierin is de aanwijzing van de benodigde rollen aan medewerkers bepaald. De bevoegdheid tot vaststelling van dit document "Informatiebeveiligingsorganisatie Midden-Delfland 2023" ligt bij het directieteam (DT).

Hierin nemen we tevens de taken en verantwoordelijkheden op voor specifieke taakvelden en basisregistraties zoals onder andere het sociaal domein en het KCC met burgerzaken. De wetgeving en de verantwoording vereisen dat deze specifiek zijn vastgelegd.

23. Bestuurlijke organisatie

Het college van burgemeester en wethouders is eindverantwoordelijk voor informatiebeveiliging binnen onze gemeente. Zij stelt het strategisch informatiebeveiligingsbeleid vast en toont hiermee, dat zij betrokken is bij het uitdragen en handhaven van het IB-beleid van en voor de hele gemeente. Vanuit de VNG zijn de tien principes voor informatiebeveiliging vastgesteld. Deze tien principes zoals verwoord in 2.2.6 en toegelicht in bijlage 1, zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurders zichzelf opleggen.
Voor alle gegevensverwerkende processen rond de uitgifte van waarde-documenten heeft de burgemeester daarnaast op basis van de Paspoortwet en het Reglement Rijbewijzen een eigen verantwoordelijkheid.

Het college c.q. de burgemeester stelt de kaders ten aanzien van informatieveiligheid en privacy vast op basis van landelijke en Europese wet- en regelgeving en stimuleert het management om alle noodzakelijke beveiligingsmaatregelen te nemen.

De uitvoering van dat beleid – waaronder het stellen van nadere regels en procedures – is over het algemeen gemandateerd aan het directieteam.

Het college verantwoordt zich sinds 2017 over informatieveiligheid aan de gemeenteraad en de Rijksoverheid door middel van de jaarlijkse collegeverklaring ENSIA. De collegeverklaring wordt op onderdelen getoetst door een onafhankelijke, externe, IT-auditor. Verder wordt in de jaarstukken verantwoording afgelegd over informatiebeveiliging en privacy, terwijl in de begroting de plannen voor het komende jaar worden toegelicht.

24. College van burgemeester en wethouders
Het college van burgemeester en wethouders van de gemeente Midden-Delfland 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 de afdelingsdirecteuren van de organisatieonderdelen om beveiligingsmaatregelen te nemen en te waarborgen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (bevoegdheid tot handelen) op het gebied van beveiliging gemandateerd aan het directieteam.

25. Directieteam (DT)
De ambtelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan het directieteam. Het directieteam is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij de afdelingsdirecteuren.

26. Chief Information Officer (CIO)
Deze rol/functie is verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's, evenals het opstellen van rapportages. De CIO heeft gemandateerde verantwoordelijkheid voor informatiebeveiliging ten aanzien van de organisatie.

De CIO is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en rapporteert dit naar het bestuur. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij de afdelingsdirecteuren.
De CIO is meestal iemand die dicht bij het bestuur staat (bijv. een stafmedewerker of gemeentesecretaris).

27. Chief Information Security Officer (CISO)
De CISO is verantwoordelijk voor de interne controle op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de classificatie/escalatie van beveiligingsincidenten.

De CISO is de beleidsfunctionaris die taken uitvoert op het gebied van informatiebeveiliging en de spin in het web van de logische technische informatiebeveiliging. Hij zorgt ervoor dat de door de CIO aan hem gedelegeerde verantwoordelijkheden handen en voeten krijgen binnen de informatiebeveiligingsorganisatie. Op het gebied van logisch technische informatiebeveiliging is hij het aanspreekpunt voor de CIO en voor de afdelingsdirecteuren en procesbeheerders. Hij rapporteert aan de CIO en onderhoudt nauw contact met de CIO en de beveiligingsbeheerders. De CISO is goed op de hoogte van informatiebeveiliging gerelateerde aspecten.

28. Information Security Officer (ISO)
Dit is een rol die toebedeeld is aan adviseur(s) IV met het taakveld informatiebeveiliging in hun functie.

Een Information Security Officer (ISO) is verantwoordelijk voor de beveiliging van informatie en gegevens binnen de organisatie. De rol omvat het ontwikkelen, implementeren en handhaven van beveiligingsbeleid en -procedures om ervoor te zorgen dat vertrouwelijke en gevoelige gegevens beschermd blijven tegen ongeautoriseerde toegang, datalekken en andere beveiligingsrisico's. De ISO werkt samen met de CISO, verschillende afdelingen en teams om bewustzijn over informatiebeveiliging te bevorderen, risico's te beoordelen en passende maatregelen te nemen om de integriteit, vertrouwelijkheid en beschikbaarheid van gegevens te waarborgen. De ISO houdt zich ook bezig met compliance van relevante wet- en regelgeving met betrekking tot informatiebeveiliging. Kortom, de Information Security Officer speelt een cruciale rol bij het beschermen van digitale middelen en gegevens van de gemeentelijke overheid tegen bedreigingen en risico's.

29. Contactpersonen IBD
Binnen elke gemeente is een functionaris nodig die de verantwoordelijkheid heeft beveiligingsincidenten en waarschuwingen te coördineren. Deze functionaris meldt beveiligingsincidenten vanuit de gemeente aan de IBD en stroomlijnt de coördinatie van waarschuwingen vanuit de IBD naar de gemeente. Daarnaast zijn er verschillende contactpersonen in een gemeente nodig in relatie tot de IBD.

Deze zijn:
3.7a Algemeen Contactpersoon Informatiebeveiliging (ACIB)
De ACIB krijgt algemene waarschuwingen en informatie met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten.
3.7b Vertrouwde Contactpersoon Informatiebeveiliging (VCIB)
De VCIB krijgt waarschuwingen en informatie met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten die niet met anderen gedeeld mogen worden.

De ACIB en VCIB (maximaal 2 personen) hebben als taak de impact van de ontvangen waarschuwingen af te (laten) wegen en daarop maatregelen te treffen. Deze rollen zijn ondergebracht bij de ENSIA coördinator en de CISO.

30. Functionaris Gegevensbescherming
Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming/ Europese Privacyverordening (AVG). De Functionaris Gegevensbescherming heeft contact met de CISO over zowel privacy als informatiebeveiliging. Er zit namelijk een redelijke overlap in de normen voor zowel privacy als informatiebeveiliging. De Functionaris Gegevensbescherming adviseert over privacybescherming en over activiteiten ter bescherming van persoonsgegevens. De Functionaris Gegevensbescherming heeft periodiek (eens per kwartaal) overleg met de CISO.

31. Afdelingsdirecteuren
De ambtelijke organisatie werkt vanuit het principe van integraal management. Uitgangspunt daarbij is dat de afdelingsdirecteur verantwoordelijkheid draagt voor zowel de resultaten van het primaire proces als voor de ondersteunende processen, zoals financiën, P&O, inkoop én informatieveiligheid en privacy. Het is de taak van de lijnmanager als procesverantwoordelijke om haar/zijn teamleiders afwegingen te laten maken in hoeverre risico's acceptabel zijn. Deze kennen het te beveiligen werkproces en de te beschermen informatie uiteindelijk het best.

32. Teamleiders
De uitvoerende taken zijn de verantwoordelijkheid van de teamleiders binnen de afdelingen. Specialistische functies als CISO en FG spelen een ondersteunende en adviserende rol als deskundige op het gebied van informatieveiligheid respectievelijk privacy en als coördinator van de centraal te treffen beveiligingsmaatregelen.

In praktische zin betekent dit, dat het lijnmanagement (afdelingsdirecteuren primair en teamleiders secundair) verantwoordelijk is voor de implementatie en het uitdragen van de maatregelen die voortvloeien uit het informatieveiligheids- en privacybeleid binnen het eigen organisatieonderdeel. Ook beoordeelt het lijnmanagement op basis van een expliciete risicoafweging of voor specifieke informatiesystemen aanvullende beveiligingsmaatregelen noodzakelijk zijn. Het lijnmanagement stuurt voorts op beveiligingsbewustzijn en de naleving van regels en richtlijnen en spreekt medewerkers waar nodig aan op geconstateerd onzorgvuldig gedrag.

33. Beveiligingsbeheerders (BB)
Het lijnmanagement wijst binnen haar teams een of meerdere beveiligingsbeheerder(s) aan. Deze zijn binnen het taakveld van zijn/haar team belast met de taken op het gebied van informatiebeveiliging.

De BB is, voor het toegewezen deelgebied, verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatiebeveiligingsbeleid en de onderliggende informatiebeveiligingsplannen. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker voert interne controles uit en let op de naleving van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de CIO en de CISO. Deze rol geldt ten aanzien van de specifieke gegevensverzamelingen en/of informatiesystemen. In wetgeving worden verschillende benamingen aan rollen gegeven (zoals Security Officer of gegevensbeheerder) voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van gegevensverzamelingen en informatiesystemen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de benaming gedefinieerd als beveiligingsbeheerder.

34. Verantwoordelijkheden medewerkers

Onbewust menselijk handelen is de belangrijkste bedreiging voor de gemeentelijke informatievoorziening. Ongewenste, onbewuste acties blijken een groter risico voor de privacy van burgers en de veiligheid van informatie dan bewuste en gerichte aanvallen. De mens is daarmee een belangrijke schakel in het grotere geheel van informatieveiligheid. Iedere medewerker binnen de organisatie is verantwoordelijk voor alle aspecten van informatieveiligheid en privacy binnen de eigen invloedssfeer.

Dat betekent onder andere de verplichting tot:

- het vertrouwelijk houden van informatie en wachtwoorden en andere vormen van toegangscodes in het bijzonder;
- het raadplegen en uitwisselen van (persoons) gegevens strikt te beperken tot hetgeen voor een juiste uitoefening van de eigen taken en verantwoordelijkheden noodzakelijk is;
- het op een veilige manier gebruiken van ICT middelen volgens de daarvoor geldende afspraken en procedures;
- het onmiddellijk doorgeven van elk vermoeden van het optreden van een beveiligingsincident aan de direct leidinggevende en de CISO/FG.

Investeren in het verhogen van het besef bij medewerkers dat informatieveiligheid en privacy belangrijk zijn, is een effectieve maatregel om dreigingen het hoofd te bieden. Dat is te bereiken door bewustwording, opleiding en training op de juiste manier in te zetten.

35. Het beheer van informatiebeveiligingsincidenten

Het IB-beleid heeft als doel de betrouwbaarheid van de informatievoorziening te borgen. Beveiligingsincidenten zijn gebeurtenissen die de betrouwbaarheid van de informatievoorziening (tijdelijk) verstoren. Incidenten zijn niet altijd te voorkomen; 100% beveiliging is onmogelijk. Wanneer zich een incident voordoet is het belangrijk om adequaat te reageren. Met als doel de kans op uitval van bedrijfsprocessen of het ontstaan van schade als gevolg van een incident te voorkomen of te minimaliseren.

Om informatiebeveiligingsincidenten te kunnen beheren, is het noodzakelijk dat zowel medewerkers van de gemeente als medewerkers van derde partijen waar de gemeente mee samenwerkt een vaste procedure volgen. Bij (het vermoeden van) een incident daar direct melding van maken, incidentmeldingen registeren en incidenten volgens een vastgestelde procedure afhandelen.

Iedere medewerker heeft de plicht een (mogelijk) beveiligingsincident direct te melden.

Naast het herstellen van het gewenste betrouwbaarheidsniveau van de informatievoorziening, kan het beheren van beveiligingsincidenten ook een belangrijke bijdrage leveren aan het voortdurende verbeterproces van informatiebeveiliging. Door lering te trekken uit beveiligingsincidenten kunnen beveiligingsmaatregelen aangepast of vervangen worden waardoor de kans op vergelijkbare incidenten afneemt. De procedure ten aanzien van melding en het beheren van beveiligingsincidenten is eerder al vastgelegd.

36. Computer Security Incident Response Team (CSIRT)

De gemeente heeft een Computer Security Incident Response Team (CSIRT) met vergaande bevoegdheden om snel en adequaat te kunnen reageren op beveiligingsincidenten. Deze gaan het niveau van eenvoudige afhandeling via de servicedesk te boven. Het doel van het CSIRT is om:

- een groot beveiligingsincident zo snel mogelijk te bestrijden en de oorzaak te elimineren;
- de oude situatie zo snel mogelijk te herstellen;
  de reputatieschade als gevolg van het incident te beperken en zo snel mogelijk te herstellen.

De gemeente behoort voorbereid te zijn op beveiligingsincidenten met een hoge urgentie en impact waarbij snel, adequaat en voorspelbaar handelen vereist is (informatiebeveiligingsprotocol kan hierbij ondersteunend zijn). De Information Security Officers (ISO) hebben hierbij een ondersteunde en adviserende rol. Zij helpen bij de afhandeling van beveiligingsincidenten. De leden hebben vanuit hun rol als VCIB (vertrouwelijk contactpersoon informatiebeveiliging) en ACIB (algemeen contactpersoon informatiebeveiliging) contact met de IBD bij geconstateerde kwetsbaarheden of incidenten. Ook passen zij het informatiebeveiligingsprotocol aan waar nodig. De vraag is niet zozeer of er een incident plaatsvindt maar wanneer. Immers, 100% beveiligen is niet mogelijk. Dit CSIR-team anticipeert ook in samenwerking met de privacy officer op de meldplicht datalekken. Deze is vanaf 2016 van kracht en daarbij worden eisen gesteld aan het verplicht melden van een datalek aan de Autoriteit Persoonsgegevens en eventueel aan betrokkenen (lees burger). Ook draagt het team zorg voor de nodige bewijslast. De CISO is voorzitter van het CSIR-team en belast met het proces computer security incident response (dus niet de inhoud).

Afhankelijk van aard en impact van het beveiligingsincident kan worden opgeschaald met de volgende functies:

- Gemeentesecretaris / Chief Information Officer (CIO)
- Directeur Bedrijfsvoering
- Teamleider Communicatie
- Teamleider Gebouwenbeheer / Facilitair
- Teamleider Openbare Orde en Veiligheid (OOV)
- CISO-Samenwerkingsverband (gemeente Westland)
- Hoofd ICT-Samenwerkingsverband (gemeente Westland)

De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

37. Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Midden-Delfland. De bestuurders en afdelingsdirecteuren van de gemeente Midden-Delfland geven volgens de 10 principes voor informatiebeveiliging richting en sturing aan het onderwerp informatiebeveiliging. Dit doen zij samen met de teamleiders, bijvoorbeeld 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. Hierbij gaat het om de beleidsonderwerpen die aanvullend zijn op dit strategische beleid en zowel generiek gemeentebreed als specifiek voor bepaalde domeinen, processen of teams kunnen zijn.

38. Toetsing aan regelgeving

Voor gemeenten is er de Eenduidige Normatiek Single Information Audit (ENSIA), die wordt gebruikt om het beleid op het gebied van informatieveiligheid te verantwoorden en te evalueren. ENSIA is opgezet als een systeem waarmee gemeenten in één keer verantwoording kunnen afleggen over zowel informatieveiligheid als (gedeeltelijk) privacy. Hoewel ENSIA al bestond voordat de Baseline Informatiebeveiliging Overheid (BIO) werd geïntroduceerd, is sinds 2020 de verantwoordingsplicht volledig gebaseerd op de BIO.

Bij ENSIA draait het om verantwoording via zelfevaluatie, zowel richting de gemeenteraad als de toezichthouders vanuit de Rijksoverheid. Daarnaast regelt ENSIA de rapportage aan de Rijksoverheid over verschillende registraties, zoals de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI). Met behulp van vragenlijsten en een jaarlijkse rapportage over de stand van zaken op het gebied van informatieveiligheid, krijgt de gemeente inzicht in haar beleid en kan ze verbeteringen aanbrengen en verslag uitbrengen.

Het is essentieel om naleving aantoonbaar te maken. De gemeente moet een 'geschikt informatiebeveiligingsbeleid' hebben, inclusief technische en organisatorische maatregelen, om ervoor te zorgen én te bewijzen dat gegevensverwerking in overeenstemming is met de geldende regelgeving (accountability). Deze maatregelen moeten regelmatig worden geëvalueerd en indien nodig bijgewerkt. De implementatie van informatiebeveiliging is dus geen eenmalige activiteit, maar een continu proces dat voortdurende aandacht vereist.

De rol van ENSIA-coördinator

De ENSIA coördinator is er verantwoordelijk voor dat zowel de horizontale als verticale verantwoording tijdig afgelegd wordt aan de verschillende instanties. Hiervoor is het nodig dat een brede betrokkenheid en draagvlak wordt gecreëerd binnen de organisatie.

De ENSIA-coördinator:

- Is contactpersoon/aanspreekpunt voor de verschillende domeinverantwoordelijken en benadert hen proactief voor de invulling van het Information Security Management System (ISMS) of van de vragenlijsten in het ENSIA web-portal;
- houdt toezicht op de tijdige invulling en de inhoud van de antwoorden die door de verantwoordelijken gegeven zijn;
- houdt contact met VNG Realisatie en betrokken ministeries;
- is verantwoordelijk voor het uitzoeken van en opdracht verlenen aan de auditor voor de uitvoering van de audit en het opstellen van het Assurancerapport;
- is verantwoordelijk voor het op tijd en volledig sturen van alle rapportages aan directie, college en raad en de landelijke toezichthouders.

39. 4. Uitwerking strategisch beleid

Het strategische beleid wordt als kader en basis gebruikt voor het uitwerken van de tactische beleidsplannen en operationele werkprocessen. Hiermee geeft het richting voor de verdere invulling van IB binnen de operationele doelstellingen en inspanningsverplichtingen van de gemeente Midden-Delfland. Dit wordt vertaald in tactisch en operationeel beleid, waarbij de besluitvorming bij het directieteam ligt.

De daaruit voortkomende werkzaamheden worden uitgewerkt in een Informatiebeveiligingsplan (IBP) dat als hoofdstuk is opgenomen in het jaarverslag informatiebeveiliging. Door ieder jaar een nieuw operationeel plan (IBP) te schrijven, is het mogelijk om snel te kunnen inspelen op de actualiteit en andere ontwikkelingen. Het maakt de gemeente flexibeler en daardoor veiliger.

Voor het gestructureerd bijhouden van de status rondom IB wordt gewerkt met een ISMS (Information Security Management System). Deze tool ondersteunt de jaarlijkse PDCA-cyclus.

5. Slotbepalingen

Intrekking oude regeling
Intrekking van het voorgaande Strategisch Informatiebeveiligingsbeleid Midden-Delfland 2020-2023.

Inwerkingtreding
Deze beleidsregels treden in werking:
één dag na de bekendmaking

Citeertitel
Deze beleidsregels worden aangehaald als “Strategisch Informatiebeveiligingsbeleid Midden-Delfland 2023 -2026”.

Ondertekening
Aldus besloten in de vergadering van 12 december 2023
Burgemeester en wethouders van Midden-Delfland,

drs. M.A.I Born
Gemeentesecretaris,

drs. A.P.J. van Hemmen
Burgemeester