ODMH
Omgevingsdienst Midden-Holland

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 2026
25 oktober
2024

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Midden-Holland

Strategisch Informatiebeveiligings- en Privacy Beleid 2024-2027

1 **Samenvatting**
Deze beleidsnota beschrijft het Strategisch Informatiebeveiligings- en Privacy Beleid voor de jaren 2024-2027.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.
Met dit 'Strategisch Informatiebeveiligings- en Privacy Beleid 2024-2027' zet de Omgevingsdienst Midden-Holland een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de Omgevingsdienst Midden-Holland te continueren en daarmee 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 (zie BIJLAGE A) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG (zie 0) en de beginselen uit de AVG voor het verwerken van persoonsgegevens (zie BIJLAGE B).

1.1 **Leeswijze**r
In hoofdstuk 3 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks door de CISO uit te brengen Informatiebeveiligings- en privacy plan[1] (vastgesteld door het Managementteam) zullen deze tactische en operationele aspecten van de informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd[2]. Dit wordt gedaan op basis van input van de coördinatoren, de CISO, de privacyfunctionarissen (PO en FG), het dreigingsbeeld van de IBD en de uitkomsten van risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 4 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

[1] Meer hierover is terug te vinden in paragraaf 4.3.
[2] Op dit moment wordt hiervoor de Actielijst uit ControlBee voor gebruikt.

2. Inleiding
2.1 Wat is informatiebeveiliging?
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het strategisch informatiebeveiligingsbeleid geldt voor alle processen van de Omgevingsdienst Midden-Holland en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen. Dit ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT maar heeft ook betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

2.2 Privacy & Gegevensbescherming (AVG)
De Omgevingsdienst Midden-Holland werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de dienst voor het goed kunnen uitvoeren van de wettelijke en andere taken. Denk hierbij onder andere aan de taken die de Omgevingsdienst Midden-Holland in mandaat namens de gemeenten en provincie uitvoert. Naast de mandaattaken voert de Omgevingsdienst Midden-Holland ook adviestaken uit voor de gemeenten en provincie. Om als Omgevingsdienst Midden-Holland deze taken goed uit te voeren is de verwerking van persoonsgegevens noodzakelijk.
Naast de uitvoering van deze taken verwerkt de Omgevingsdienst Midden-Holland ook persoonsgegevens van de eigen medewerkers.
Bij de omgang met persoonsgegevens van inwoners en personeel hebben omgevingsdiensten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van omgevingsdiensten, de gegevensuitwisseling met (keten)partners en de technische mogelijkheden en veranderende wetge-

ving. Privacy raakt de hele organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet er immers op kunnen vertrouwen dat de dienst zorgvuldig en veilig met deze persoonsgegevens omgaat.

2.3 Ambitie en visie van de Omgevingsdienst Midden-Holland op het gebied van informatieveiligheid en privacy
Door het implementeren van de BIO wil de Omgevingsdienst Midden-Holland de volgende doelstellingen bereiken:
- Een aantoonbaar informatieveilige organisatie;
- Dreigingen op het gebied van cybercrime het hoofd kunnen bieden;
- Voldoen aan de bepalingen uit de AVG die zien op informatiebeveiliging.

Om de volwassenheid op het vlak van informatiebeveiliging te kunnen duiden, heeft de NOREA[1] een model ontwikkeld, waarmee de volwassenheid op het vlak van informatiebeveiliging op een schaal van 1 tot 5 (laag tot hoog) kan worden aangeduid.
Om de doelstellingen ten aanzien van informatieveiligheid te behalen, dient de Omgevingsdienst Midden-Holland op alle aspecten van het NOREA-model[2] de komende periode te investeren om te werken naar niveau 3[3].
Het streven van de Omgevingsdienst Midden-Holland is om de gewenste score te behalen op alle aspecten. De verantwoordelijkheid voor het behalen van deze doelstelling ligt breed binnen de gehele organisatie.
Het behalen van een volwassenheidsniveau 3 – en zelfs behoud van het huidige niveau – vergt continue verbetering.

[1] NOREA is de beroepsorganisatie van IT-auditors in Nederland
[2] Voor een korte uitleg zie BIJLAGE B.
[3] Wanneer dit niveau is bereikt kan de uitvoering van controles worden aangetoond, is deze getest en effectief.

3. Strategisch beleid

3.1 Doel
Het doel van deze beleidsnota is het formuleren van het "Strategisch Informatiebeveiligings- en Privacy Beleid voor de jaren 2024-2027". De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen Informatiebeveiligings- en privacy plan.
Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het managementteam en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

3.2 Ontwikkelingen
De ontwikkelingen die van belang zijn voor het Strategisch Informatiebeveiligings- en Privacy Beleid zijn de volgende:

3.2.1 De BIO
De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat iedereen 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.

3.2.2 De NIS2
De NIS2-richtlijn (Network and Information Systems Directive) introduceert aanvullende maatregelen en vereisten boven op de BIO. De Cyberveiligheidswet implementeert de Europese NIS2-richtlijn. De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Het doel wordt in Nederland bereikt door deze richtlijn te implementeren in de Cyberveiligheidswet, waarbij onder meer verplichtingen worden opgelegd aan die entiteiten, zoals het treffen van adequate beveiligingsmaatregelen en het melden van ICT-incidenten.
In BIJLAGE C zijn enkele aanvullende maatregelen uit de NIS2 opgenomen.

3.2.3 De AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De Omgevingsdienst Midden-Holland is zich hiervan bewust en wil daarom, aanvullend op de eerder in het privacy beleid van de Omgevingsdienst Midden-Holland vastgestelde uitgangspunten (Blad gemeenschappelijke regeling 2018, 667) met dit beleid aangeven hoe zij in algemene zin invulling

geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

3.2.4 De Wpg

De Omgevingsdienst Midden-Holland heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (Wpg). Hiervoor moet de Omgevingsdienst Midden-Holland beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

3.2.5 De 10 principes voor informatiebeveiliging [1]

De 10 principes voor informatiebeveiliging zijn een aanvulling op het normenkader BIO en gaan over de waarden die het managementteam oplegt. De principes zijn als volgt:

1. Het managementteam bevordert 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 managementteam controleert en evalueert

De principes gaan vooral over de verantwoordelijkheid van het managementteam bij het waarborgen van informatiebeveiliging in de organisatie. Ze ondersteunen het managementteam bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen van de dienst, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de dienst. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

3.2.6 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.

3.2.7 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De dienst kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten (datalekken) 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.
Een datalek wordt altijd beschouwd als een informatiebeveiligingsincident (zie BIJLAGE F voor meer informatie hierover). Een datalek treedt op wanneer gevoelige informatie wordt blootgesteld aan ongeautoriseerde personen, hetgeen een inbreuk is op de beveiliging van die informatie.

3.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van *goede werkwijzen* bij omgevingsdiensten en NEN-ISO/IEC 27002:2017 genomen.
Voor de ondersteuning bij het formuleren en realiseren van hun strategisch informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de BIO uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligings- en privacy plan zal deze structuur volgen.

[1] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
[2] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

3.4 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 en privacy op tactisch en operationeel niveau.
Deze nota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden door de CISO uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligings- en privacy plan'[1].

3.5 Scope informatiebeveiliging en privacy

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de Omgevingsdienst Midden-Holland en externe partijen (bijvoorbeeld gemeente en 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 Informatiebeveiligings- en Privacy Beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit specifieke wetgeving af zoals voor AVG en UAVG.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

3.6 Uitgangspunten

De directie, het managementteam en de teamleiders en coördinatoren spelen een cruciale rol bij het uitvoeren van dit Strategisch Informatiebeveiligings- en Privacy Beleid. De teamleiders en coördinatoren maken een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de Omgevingsdienst Midden-Holland heeft, de (privacy) risico's die de dienst hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het managementteam dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Hierbij wordt ondersteuning verleend aan de organisatie vanuit de werkgroep AVG[2].
Directie, managementteam, teamleiders en coördinatoren geven een duidelijke richting aan informatiebeveiliging en privacy en demonstreren dat zij informatiebeveiliging en privacybescherming ondersteunen en zich hierbij betrokken voelen, door het uitdragen en handhaven van een beleid van en voor de hele Omgevingsdienst Midden-Holland. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het beleid is in lijn met het algemene beleid van de Omgevingsdienst Midden-Holland en de relevante landelijke en Europese wet- en regelgeving.

[1] Zie paragraaf 4.3 voor een nader uitleg hiervan.
[2] Deze werkgroep zal daarmee hernoemd gaan worden naar Werkgroep Informatiebeveiliging en Privacy.

3.7 Strategische doelen

De strategische doelen van het Strategisch Informatiebeveiligings- en Privacy Beleid zijn:
Het managen van de informatiebeveiliging;

- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens
- Het toepassen van dataminimalisatie
- Het minimaliseren van risico's van menselijk gedrag
- Het voorkomen van ongeautoriseerde toegang
- Het garanderen van correcte en veilige informatievoorzieningen
- Het beheersen van de toegang tot informatiesystemen
- Het waarborgen van veilige informatiesystemen
- Het adequaat reageren op incidenten
- Het beschermen van (kritieke) bedrijfsprocessen
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen
- Het waarborgen van de naleving van dit beleid

3.8 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van management, teamleiders en coördinatoren. Alle informatiebronnen en -systemen die gebruikt worden door de Omgevingsdienst Midden-Holland hebben een eigenaar[1] die de vertrouwelijkheid, privacy eisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt derhalve bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie[2] wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het Strategisch Informatiebeveiligings- en Privacy Beleid vormt samen met het Informatiebeveiligings- en privacy plan het fundament onder een betrouwbare informatievoorziening en privacybescherming. In het Informatiebeveiligings- en privacy plan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.

- Informatiebeveiliging en privacybescherming is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De dienst stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het Strategisch Informatiebeveiligings- en Privacy Beleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Het borgen van privacy in de uitvoering van de processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting. Toetsing hiervan wordt belegd bij de werkgroep Informatiebeveiliging & Privacy.

[1] Zie BIJLAGE E voor de eigenaren van de processen en applicaties.
[2] Dit is nader uitgewerkt in paragraaf 4.3.2 Evaluatie van de prestaties.

3.9 Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- De directie keurt het Strategisch Informatiebeveiligings- en Privacy Beleid goed.
- Het DB ODMH stelt als eindverantwoordelijke het Strategisch Informatiebeveiligings- en Privacy Beleid vast.
- Het managementteam stelt jaarlijks het Informatiebeveiligings- en privacy plan vast.
- Het managementteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming[1].
- Het managementteam is verantwoordelijk voor het vragen om informatie bij de teamleiders en coördinatoren en ziet erop toe dat de teamleiders en coördinatoren adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen die onder hun verantwoordelijkheid vallen.
- 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 managementteam.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van de directeur, het managementteamen andere collega's over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin de FG zijn bevindingen en aanbevelingen vastlegt.
- Het managementteam en de teamleiders en coördinatoren stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de functionaris voor gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- Tijdens de Sturingsbijeenkomsten dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De teamleiders en coördinatoren zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teamleiders en coördinatoren zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister[2].
- De teamleiders en coördinatoren zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Alle medewerkers van de Omgevingsdienst Midden-Holland worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Teamleiders en coördinatoren dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, opdat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.

- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Proceseigenaren voeren quickscans informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG om deze risico-afwegingen te kunnen maken.

- Informatiebeveiliging en privacybescherming maakt deel uit van de functionerings- en beoordelingssystematiek (Het Goede Gesprek) en wordt besproken tussen de manager en de medewerker.

[1] Op dit moment wordt hiervoor ControlBee gebruikt, Er wordt in overleg met kwaliteitsmanagement, gezocht naar een eventueel ander managementsysteem.
[2] Binnen de ODMH is één verwerkingsregister aanwezig. Daarin zowel verwerkingen namens bevoegd gezag als eigen verwerkingen (bedrijfsvoering).

3.10 Randvoorwaarden
Belangrijke randvoorwaarden zijn:
- Informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners en leveranciers en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
-
- Jaarlijks wordt een Informatiebeveiligings- en privacy plan opgesteld door de CISO, gebaseerd op:
  1. Dit Strategisch Informatiebeveiligings- en Privacy Beleid
  2. De uitkomsten van relevante audit resultaten
  3. Het dreigingsbeeld gemeenten van de IBD
  4. Uitkomsten risicoanalyses en DPIA's
  5. De door teamleiders en coördinatoren ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA)

- Om uitvoering te kunnen geven aan dit strategisch beleid en het Informatiebeveiligings- en privacy plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld[1]

[1] Op dit moment is dit geborgd middels het akkoord op het Plan van Aanpak. In die toekomst wordt dit geregeld door het jaarlijks opstellen en goedkeuren van het Informatiebeveiligings- en Privacy Plan.

4. **Organisatie, taken & verantwoordelijkheden**
In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defence'). In dit model is het lijnmanagement (teamleiders en coördinatoren) verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO en PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering.

4.1 Aansturing: Het managementteam
Het managementteam zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamleider of coördinator. Het managementteam zorgt dat de teamleider of coördinator zich verantwoordt over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het managementteam stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het managementteam draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO[1] van de dienst. Het managementteam autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de Omgevingsdienst Midden-Holland gezien als een integraal onderdeel van risicomanagement.

4.2 Uitvoering: Teamleiders en coördinatoren

Informatiebeveiliging en privacy vallen onder de verantwoordelijkheden van alle teamleiders en coördinatoren. Om deze verantwoordelijkheden waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheden kunnen zij niet delegeren, uitvoerende werkzaamheden wel. Alle processen, systemen, (persoons)gegevens en applicaties hebben altijd minimaal één eigenaar; er moet dus altijd iemand verantwoordelijk zijn[2]. Teamleiders en coördinatoren rapporteren aan hun afdelingshoofd over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. De inhoudelijke aanpak met betrekking tot het onderwerp informatiebeveiliging en privacy wordt minimaal 2 keer per jaar besproken in een Sturingsbijeenkomst.
Taken van de teamleiders en coördinatoren in het kader van informatiebeveiliging en privacybescherming zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is
- Het binnen de eigen afdeling uitdragen van het Strategisch Informatiebeveiligings- en Privacy Beleid, de daaraan gerelateerde procedures
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld
- Het vroegtijdig betrekken van CISO en FG bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen

[1] Op dit moment is er nog geen PO aanwezig binnen de [Bedrijf]. Deze rol moet nog ingericht worden.
[2] Binnen het KMS worden deze benoemd.

4.3 Werkgroep Informatiebeveiliging & Privacy

Op dit moment is er een werkgroep AVG actief binnen de Omgevingsdienst Midden-Holland waarin nu ook (naast privacy) informatiebeveiliging behandeld wordt. Deze werkgroep zal omgedoopt worden naar Werkgroep Informatiebeveiliging & Privacy en, voor wat betreft informatiebeveiliging, evaluaties van de prestaties gaan uitvoeren. Daarbij controleert de werkgroep de voortgang van het door de CISO opgestelde Informatiebeveiligings- en privacy plan (IB&P).
In het IB&P dienen de volgende zaken minimaal behandeld te worden:

- Operationele planning en
- Evaluatie van de prestaties.

4.3.1. Operationele planning

In dit Strategisch Informatiebeveiligings- en Privacy Beleid zijn onder andere de informatiebeveiligingsdoelstellingen vastgesteld. In het IB&P wordt een planning opgenomen voor het bereiken van de informatiebeveiligingsdoelstellingen.
Daarnaast zal jaarlijks een risicobeoordeling voor informatiebeveiliging uitgevoerd worden. Eventuele maatregelen, welke daaruit voortkomen, worden meegenomen in het IB&P.

4.3.2 Evaluatie van de prestaties

Om de prestaties van de informatiebeveiliging en de doeltreffendheid van het managementsysteem voor informatiebeveiliging te evalueren, moeten een aantal zaken jaarlijks uitgevoerd worden. Dit zijn:

- Monitoren, meten, analyseren en evalueren van de KPI's
- Monitoren, meten, analyseren en evalueren van de Leveranciers
- Uitvoeren interne audit
- Uitvoeren management review

KPI's
In het IB&P moet daarvoor vastgesteld worden

- wat moet worden gemonitord en gemeten, met inbegrip van processen en beheersmaatregelen voor informatiebeveiliging
- de methoden voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren om valide resultaten te bewerkstelligen. Om als valide te worden te beschouwd behoren de resultaten van de geselecteerde methoden te kunnen worden vergeleken en gereproduceerd
- wanneer moet worden gemonitord en gemeten
- wie moet monitoren en meten
- wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd
- wie deze resultaten moet analyseren en evalueren

Leveranciers
De ODMH beoordeelt jaarlijks de vijf grootste leveranciers in euro's die we nog niet eerder of als laatst hebben beoordeeld. Als ervaringen in de praktijk daar aanleiding toe geven, kunnen we besluiten extra of andere leveranciers beoordelen. Voor de leveranciersbeoordeling gebruiken we een vragenlijst die door verschillende medewerkers die regelmatig met de leverancier werken, wordt ingevuld. De resultaten met eventueel advies worden in de werkgroep Informatiebeveiliging en Privacy besproken en gerapporteerd aan het MT. Bij een negatieve beoordeling stellen we een verbeterplan op. Eventuele corrigerende of preventieve maatregelen, nemen we op in de verbetermaatregelenlijsten.

Interne audit
Jaarlijks zal er een interne audit worden uitgevoerd. Dit is cruciaal voor het waarborgen van een robuust en effectief informatiebeveiligingssysteem dat niet alleen voldoet aan de BIO en dit beleid, maar ook bijdraagt aan de algemene veerkracht en veiligheid van de Omgevingsdienst Midden-Holland.
Door jaarlijks te auditen kan de organisatie proactief risico's beheren en incidenten voorkomen in plaats van reactief te handelen. Het helpt ook het MT bij het aantonen van haar verantwoordelijkheid en betrokkenheid bij informatiebeveiliging. Daarnaast kunnen informatiebeveiligingsrisico's snel veranderen. Jaarlijkse audits helpen de organisatie zich aan te passen aan deze veranderingen.
Als onderdeel van het IB&P zal het auditprogramma voor het betreffende jaar in detail worden uitgewerkt. Corrigerende en preventieve maatregelen worden vastgelegd in de verbetermaatregelenlijsten. Per verbetermaatregel wordt geregistreerd wie de voortgang bewaakt. De werkgroep Informatiebeveiliging en Privacy coördineert de algemene opvolging van de audits, bijvoorbeeld door (te ondersteunen bij) het opstellen van een plan van aanpak.

Management review
Naast de interne audit dient ook jaarlijks een management review te worden uitgevoerd. In de management review wordt het ISMS, de bijbehorende informatiebeveiligingsdoelstellingen en de voortgang van de strategische koers jaarlijks geëvalueerd en vastgelegd. Het ondersteunt het MT bij het bepalen van de strategische richting voor informatiebeveiliging binnen de Omgevingsdienst Midden-Holland. Daarnaast demonstreert dit aan de stakeholders dat de dienst informatiebeveiliging serieus neemt en continu streeft naar verbetering.

4.4 Controle en verantwoording
Dit Strategisch Informatiebeveiligings- en Privacy Beleid is de verantwoordelijkheid van het managementteam van de Omgevingsdienst Midden-Holland. Het Managementteam zal handelen volgens de tien principes voor informatiebeveiliging en de beginselen voor de verwerking van persoonsgegevens. Zij benadrukt het belang van informatiebeveiliging en privacy door voorbeeldgedrag te tonen en om informatie te vragen.
De directie rapporteert over de mate waarin zij uitvoering heeft gegeven aan het uitwerken van tactische deelbeleidsonderwerpen die aanvullend zijn op dit strategisch beleid.

5. Bijlagen

BIJLAGE A Baseline Informatiebeveiliging Overheid
Externe bijlage

BIJLAGE B Basisprincipes (beginselen) AVG
De AVG kent 6 basisprincipes, in de AVG 'beginselen' genoemd. Die staan in artikel 5 van de AVG[1]. Iedereen die persoonsgegevens verwerkt, moet zich hieraan houden. En dit kunnen aantonen. Dat is het zevende, overkoepelende beginsel van de AVG: de verantwoordingsplicht[2].

De 6 AVG-beginselen zijn:

1. Rechtmatigheid, behoorlijkheid en transparantie
2. Doelbinding
3. Dataminimalisatie
4. Juistheid
5. Opslagbeperking
6. Vertrouwelijkheid en integriteit

B.1. Rechtmatigheid, behoorlijkheid en transparantie

Om rechtmatig te zijn, moet een verwerking[3] in elk geval zijn gebaseerd op een grondslag[4] uit de AVG. Maar ook mag de verwerking niet in strijd zijn met andere wetgeving, zoals een wettelijke geheimhoudingsplicht.
De verwerking moet ook 'behoorlijk' zijn. Dat betekent dat die niet (op een niet te rechtvaardigen manier) nadelig, discriminerend, onverwacht of misleidend mag zijn voor de betrokkenen[5].
Verder moet het transparant zijn voor betrokkenen hoe en waarom een organisatie hun persoonsgegevens verwerkt. Dat betekent dat de organisatie hier open en duidelijk over moet communiceren.

B.2. Doelbinding
Organisaties mogen persoonsgegevens alleen verzamelen met een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. Organisaties mogen dus niet alvast persoonsgegevens gaan verzamelen omdat die misschien ooit van pas gaan komen.
Het doel waarvoor een organisatie persoonsgegevens gaat verwerken, moet verenigbaar zijn met het doel waarvoor deze gegevens zijn verzameld. Oftewel: de organisatie mag de gegevens niet ineens voor een ander doel gaan gebruiken.

B.3. Dataminimalisatie
Als organisaties persoonsgegevens verwerken, moeten ze daarbij uitgaan van het principe ‘zo min mogelijk’. Dat houdt bijvoorbeeld in dat de verwerking van de gegevens moet passen bij het doel. En dat de organisatie niet meer gegevens mag verwerken dan noodzakelijk is om dat doel te bereiken.

B.4. Juistheid
Organisaties moeten ervoor zorgen dat de gegevens juist zijn. En de gegevens actualiseren als dat nodig is. Mensen kunnen ook aan organisaties vragen hun persoonsgegevens aan te passen als deze niet kloppen.

B.5. Opslagbeperking
Organisaties moeten persoonsgegevens verwijderen zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld. Organisaties mogen gegevens dus maar een bepaalde tijd bewaren.

B.6. Vertrouwelijkheid en integriteit
Organisaties moeten hun gegevensverwerkingen goed beveiligen. Er gelden extra strenge regels voor bijzondere persoonsgegevens[1].

[1] Bijzondere persoonsgegevens zijn gegevens die zo privacygevoelig zijn dat het een grote(re) impact op iemand kan hebben als een organisatie deze gegevens verwerkt. Bijvoorbeeld gegevens over iemands gezondheid of politieke voorkeur. Daarom krijgen bijzondere persoonsgegevens extra bescherming in de AVG.

[1] Zie Artikel 5 Beginselen inzake verwerking van persoonsgegevens
[2] Zie Verantwoordingsplicht | Autoriteit Persoonsgegevens
[3] Een verwerking van persoonsgegevens is alles wat een organisatie met persoonsgegevens kan doen, van verzamelen tot en met vernietigen.
[4] Organisaties mogen alleen persoonsgegevens verwerken als zij daar een goede reden voor hebben. De juridische term hiervoor is ‘grondslag’. In de AVG staan 6 mogelijke grondslagen.
[5] De persoon of personen van wie een organisatie persoonsgegevens verwerkt.

BIJLAGE C NIS2
De NIS2-richtlijn (Network and Information Systems Directive) introduceert aanvullende maatregelen en vereisten boven op de BIO.
Onderstaan enkele specifieke maatregelen en werkzaamheden die NIS2 toevoegt:

1. Uitgebreidere Risicoanalyse en Beoordeling

- **NIS2** vereist een meer gedetailleerde en frequente risicoanalyse en beoordeling van de kritieke infrastructuren en digitale diensten.
- **Werkzaamheden**: Uitvoeren van uitgebreide risicoanalyses, regelmatig bijwerken van de risicobeoordelingen en documenteren van bevindingen.

2. Incidentrapportage
- **NIS2** stelt strengere eisen aan de rapportage van beveiligingsincidenten, inclusief een korte meldingstermijn.
- **Werkzaamheden**: Inrichten van systemen en processen voor snelle detectie en rapportage van incidenten binnen 24 uur aan de bevoegde autoriteiten.

3. Toezicht en Handhaving
- **NIS2** introduceert strengere toezichts- en handhavingsmechanismen door de nationale autoriteiten.
- **Werkzaamheden**: Voorbereiden op regelmatige audits en inspecties door toezichthoudende instanties en zorgen voor naleving van opgelegde maatregelen.

4. Leveranciersbeheer
- **NIS2** legt meer nadruk op het beheer van de beveiliging van toeleveringsketens en derde partijen.
- **Werkzaamheden**: Implementeren van strengere contractuele eisen en evaluaties voor leveranciers, en continu toezicht houden op de beveiligingspraktijken van derde partijen.

5. Personeelsopleiding en Bewustwording
- **NIS2** vereist gerichte en regelmatige beveiligingstrainingen en bewustwordingsprogramma's voor alle medewerkers, met speciale aandacht voor kritieke functies.
- **Werkzaamheden**: Ontwikkelen en uitvoeren van geavanceerde training- en bewustwordingsprogramma's voor personeel, gericht op specifieke bedreigingen en beveiligingsprotocollen.

6. Beleid en Procedures voor Incidentrespons
- **NIS2** verlangt uitgebreidere beleids- en procedureontwikkelingen voor incidentrespons en continuïteitsbeheer.
- **Werkzaamheden**: Opstellen en testen van gedetailleerde incidentresponsplannen, inclusief crisisscenario's en herstelplannen.

7. Verplichte Meldingsdrempels
- **NIS2** introduceert specifieke meldingsdrempels voor incidenten die aanzienlijke verstoringen of schade kunnen veroorzaken.
- **Werkzaamheden**: Instellen van criteria en processen om te bepalen wanneer een incident meldingsplichtig is en zorgen voor tijdige en accurate meldingen.

BIJLAGE D Volwassenheidsmodel Informatiebeveiliging
Het volwassenheidsmodel informatiebeveiliging biedt een handreiking om te beoordelen hoe het staat met de informatiebeveiliging binnen een organisatie.

Daarmee geeft het model het Managementteam goed inzicht in het actuele volwassenheidsniveau en een handreiking met stappen welke een organisatie nog moet nemen om tot het gewenste volwassenheidsniveau te komen.

Het model onderkend 5 niveaus van volwassenheid:
1. **Initieel**: Controles zijn niet of slechts gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd en zijn sterk afhankelijk van individuen.
2. **Herhaalbaar**: Controles zijn aanwezig en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.

3. **Gedefinieerde**: Controles zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van controles kan worden aangetoond, is getest en effectief.
4. **Beheerd en meetbaar**: De effectiviteit van de beheersing wordt periodiek beoordeeld en waar nodig verbeterd. Deze beoordeling wordt gedocumenteerd.
5. **Continue verbetering**: Een bedrijfsbreed risico- en controleprogramma zorgt voor een continue en effectieve oplossing van controle- en risicoproblemen.

BIJLAGE E Processen en systemen
In Tabel 1 zijn de hoofdprocessen van de ODMH weergegeven met per proces de eigena(a)r(en). Deze lijst is aangevuld met de processen om de BIO geïmplementeerd te kunnen houden.
Vervolgens is in Tabel 2 de applicaties met de bijbehorende eigenaren opgenomen.

Code	Proces	Eigenaar	Document
P1	Vergunningen	Afdelingshoofden Milieu en BWT	
P2	Toezicht milieu	Afdelingshoofd Milieu	
P3	Toezicht BTW	Afdelingshoofd BWT	
P4	Projecten	Afdelingshoofd Expertise	
P5	Meldingen	Afdelingshoofden Milieu en BWT	
P6	Adviseren	Afdelingshoofd Expertise	
	Bedrijfscontinuïteitsmanagement en incidentbeheer	Coördinator ICT	Back-upbeleid Bedrijfscontinuïteitsbeheer
	Beheer van ICT bedrijfsmiddelen	Coördinator ICT	Beleid voor mobiele apparatuur (incl. Telewerken)
	Compliance en naleving	FG	Privacy beleid
	Informatieclassificatie en bescherming informatie	Coördinator FAB	Beleid voor informatietransport
	Leveranciersbeheer		Informatiebeveiligingsbeleid voor leveranciersrelaties
	Logische toegangsbeveiliging	Coördinator ICT	Beleid voor (logische) toegangsbeveiliging Wachtwoordbeleid
	Netwerk en communicatie beveiliging	Coördinator ICT	Cryptografiebeleid
	Organisatie ISMS	CISO	Strategisch Informatiebeveiligings- en Privacy beleid
	Personeel / HR	Coördinator HR	'Clear desk'- en 'clear screen'-beleid Screeningsbeleid

Tabel 1. Hoofdprocessen ODMH

Tabel 2. Applicaties

BIJLAGE F Informatiebeveiligingsincident
Een informatiebeveiligingsincident is wanneer er iets misgaat met de beveiliging van informatie. Dit kan verschillende dingen betekenen, zoals een cyberaanval, een verloren USB-stick met gevoelige gegevens, of zelfs een medewerker die per ongeluk vertrouwelijke informatie deelt.
Een datalek is een specifiek type informatiebeveiligingsincident waarbij gevoelige, vertrouwelijke of persoonlijke informatie onbedoeld wordt blootgesteld aan ongeautoriseerde personen. Dit kan gebeuren door hackers die inbreken in een systeem, door een slecht beveiligde website, of zelfs door een gestolen laptop.
Het belangrijkste verschil tussen een informatiebeveiligingsincident en een datalek is dat een datalek specifiek gaat over het lekken van gegevens, terwijl een informatiebeveiligingsincident een bredere term is die allerlei soorten beveiligingsproblemen omvat.
Een overeenkomst tussen beide is dat ze allebei potentieel schadelijk zijn voor individuen, bedrijven of organisaties. Ze kunnen leiden tot verlies van vertrouwen, financiële schade en zelfs juridische problemen. Daarom is het belangrijk om goede maatregelen te nemen om zowel informatiebeveiligingsincidenten als datalekken te voorkomen en te beheren. Dit omvat het gebruik van sterke wachtwoorden, het regelmatig bijwerken van beveiligingssoftware en het trainen van medewerkers over het belang van informatiebeveiliging.
Een datalek wordt altijd beschouwd als een informatiebeveiligingsincident. Een datalek treedt op wanneer gevoelige informatie wordt blootgesteld aan ongeautoriseerde personen, wat een inbreuk is op de beveiliging van die informatie. Dit valt onder de bredere categorie van informatiebeveiligingsincidenten, die verschillende situaties omvatten waarbij de vertrouwelijkheid, integriteit of beschikbaarheid

van informatie wordt aangetast. Dus, terwijl niet alle informatiebeveiligingsincidenten datalekken zijn, zijn alle datalekken wel informatiebeveiligingsincidenten.
Hoewel alle datalekken als informatiebeveiligingsincidenten worden beschouwd, geldt dit niet voor alle informatiebeveiligingsincidenten.
Informatiebeveiligingsincidenten kunnen verschillende vormen aannemen, zoals een mislukte inlogpoging, een malware-aanval die systemen verstoort zonder dat er gegevens worden gelekt, of een fysiek beveiligingsprobleem zoals het verlies van een toegangsbadge.

Bijlage G Privacybeleid
Het Privacybleid Omgevingsdienst Midden-Holland is te vinden op de website van de Omgevingsdienst Midden-Holland onder Verwerking persoonsgegevens - Omgevingsdienst Midden-Holland (odmh.nl):
https://zoek.officielebekendmakingen.nl/bgr-2018-667.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dBladGemeenschappelijkeRegeling%26vrt%3dprivacy%26zkd%3dInDeGeheleText%26dpr%3dAlle%26spd%3d20180509%26epd%3d20180509%26sdt%3dDatumPublicatie%26ap%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4

Vastgesteld op 2 oktober 2024 door het Dagelijks Bestuur van de Omgevingsdienst Midden-Holland.