omgevingsdienst Haaglanden

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 775
26 maart
2026

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Haaglanden

Strategisch Informatiebeveiligings- en privacy beleid Omgevingsdienst Haaglanden 2025 tot 2028

Het beheer van dit document berust bij de Chief Information Security Officer en dient jaarlijks te worden geëvalueerd.

1. Inleiding/Management-samenvatting

Deze beleidsnota beschrijft het strategisch Informatiebeveiligings- en Privacy beleid (IB&P-beleid) voor de jaren 2025 tot 2028 en vervangt het in eerder vastgestelde 'Informatiebeveiligingsbeleid 2020'. 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 IB&P-beleid zet de omgevingsdienst een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de omgevingsdienst 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 v1.4) 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 en de beginselen uit de AVG voor het verwerken van persoonsgegevens.

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 "Informatiebeveiligings- en Privacy plan" (IB&P-plan), die is vastgesteld door de directeur, worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd.
Het uitwerken en concreet maken van het IB&P-plan wordt gedaan op basis van input van het management, de CISO, de privacy functionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's. Om de praktijk in overeenstemming te brengen met wat in het IB&P-beleid is geëist wordt in dit plan dan ook de acties en planning vermeld.
Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie zijn belegd.

1.2 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 (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de omgevingsdienst 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 Privacy & Gegevensbescherming (AVG)

De omgevingsdienst werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de omgevingsdienst voor het goed kunnen uitvoeren van de wettelijke taken. Om als omgevingsdienst deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

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 decentralisatie van overheidstaken naar omgevingsdiensten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de omgevingsdienst zorgvuldig en veilig met deze persoonsgegevens omgaat.

omgevingsdienst Haaglanden

1.4 Ambitie en visie van de omgevingsdienst op het gebied van informatieveiligheid en privacy

Het Koersplan 2024-2028 van Omgevingsdienst Haaglanden benoemt de ambitie en visie op het gebied van informatieveiligheid en privacy in het bredere kader van digitalisering en datagedreven werken. De belangrijkste punten uit het koersplan met betrekking tot informatieveiligheid en privacy zijn:

Ambitie

ODH erkent dat een goed functionerende informatie- en datahuishouding cruciaal is voor zowel de eigen organisatie als voor de opdrachtgevers (provincie en gemeenten). De ambitie is om:

- Betrouwbare en veilige informatievoorziening te waarborgen als fundament voor vergunningverlening, toezicht, handhaving en advisering.
- Datagedreven en informatiegestuurd te werken, waarbij digitalisering verder wordt ontwikkeld om de dienstverlening en besluitvorming te versterken.
- De beveiliging van data te optimaliseren en te voldoen aan wettelijke eisen rondom informatieveiligheid en privacy.

Visie

ODH ziet informatieveiligheid en privacy als een essentiële pijler voor de organisatie en haar dienstverlening. De visie hierop omvat:

- Naleving van wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG) en informatiebeveiligingsnormen zoals de BIO (Baseline Informatiebeveiliging Overheid).
- Veilige en transparante omgang met gegevens, zodat informatie betrouwbaar, integer en beschikbaar is voor alle stakeholders.
- Digitalisering en datamanagement versterken, zodat informatie gestandaardiseerd en veilig wordt verwerkt en gedeeld binnen de omgevingsdienst en met externe partners.
- Bewustwording en verantwoordelijkheid bij medewerkers vergroten, zodat informatieveiligheid en privacy een integraal onderdeel blijven van de werkwijze.

Om deze ambitie en visie te realiseren, zet ODH in op:

1. Verdieping en ontwikkeling van informatiebeveiliging en privacy beleid, afgestemd op wettelijke kaders en maatschappelijke ontwikkelingen.
2. Investeringen in technologie en processen, zoals het verbeteren van digitale infrastructuur en cybersecuritymaatregelen.
3. Integraal kijken naar werk- en organisatorische processen, zodat de kwaliteit van data gewaarborgd blijft.
4. Samenwerking met gemeenten en provincie versterken, zodat gegevensuitwisseling veilig en efficiënt verloopt.
5. Continu bewustzijn creëren bij medewerkers, door trainingen en beleid dat informatieveiligheid en privacy waarborgt in de dagelijkse werkzaamheden.

ODH ziet informatieveiligheid en privacy als een kernaspect van haar dienstverlening en zet in op datagedreven werken met een sterke focus op beveiliging, naleving van wetgeving en digitale innovatie. Dit wordt gecombineerd met bewustwording en samenwerking om informatie optimaal te beschermen en te benutten.

2. Het strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het ‘Strategisch Informatiebeveiligings- en Privacy beleid’ (IB&P-Beleid) voor de jaren 2025 tot 2028. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen ‘Informatiebeveiligings- en Privacy plan’ (IB&P-Plan).
Dit beleid dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het IB&P beleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat het management 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 AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De omgevingsdienst Haaglanden is zich hiervan bewust en wil daarom 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).

2.2.3 De WPG
De omgevingsdienst 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 beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht

2.2.4 De 10 principes voor informatiebeveiliging[1]
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:
1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de 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 processen van de omgevingsdienst, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de omgevingsdienst. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
Het Dreigingsbeeld Informatiebeveiliging Nederlandsen 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.

2.2.6 Informatie uit incidenten, inbreuken op de beveiliging en datalekken
De omgevingsdienst 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. De maatregelen worden op dit moment op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen, dit wordt met de invoering van de BIO 2.0 de NEN-ISO/IEC 27002:2022.
Voor de ondersteuning van omgevingsdiensten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het IB&P-Plan zal deze structuur volgen.

1) ***https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf***
2) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

omgevingsdienst Haaglanden

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 en privacy op tactisch en operationeel niveau.
Deze beleidsnota beschrijft op strategisch niveau het IB&P-Beleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligings- en Privacy-plan'.

2.5 Scope informatiebeveiliging en privacy
De scope van deze beleidsnota omvat alle processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de omgevingsdienst 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 beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten geformuleerd.
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.

- Alle informatie en informatiesystemen zijn van belang voor de omgevingsdienst, bepaalde informatie is van vitaal en kritiek belang. De directeur is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle informatiesystemen ongeacht waar deze worden gehost.
- Alle Proces Automatiseringssystemen (PA) die binnen het gebouw en in de publieke ruimte van de omgevingsdienst worden gebruikt, die van de omgevingsdienst zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie.

2.6 Uitgangspunten
Het management (directeur, afdelingshoofden en teamleiders) spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de omgevingsdienst heeft, de (privacy) risico's die de omgevingsdienst hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB&P beleid van en voor de hele omgevingsdienst. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het IB&P beleid is in lijn met het algemene beleid van de omgevingsdienst en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen
De strategische doelen van het IB&P 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.

2.6.2 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Omgevingsdienst Haaglanden hebben een interne eigenaar die de vertrouwelijkheid, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met het IB&P plan het fundament onder een betrouwbare informatievoorziening en privacy bescherming. In het IB&P 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 omgevingsdienst 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 IB&P 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 processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.3 IB&P governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het bestuur stelt als eindverantwoordelijke het strategisch IB&P beleid vast.
- De directeur stelt jaarlijks het IB&P-plan vast.
- De management 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.
- De directeur is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directeur, voorafgaand aan de P&C-gesprekken.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren de directeur over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
- De directeur en de afdelingshoofden stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de functionaris gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- Tijdens Planning & Control-gesprekken 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 afdelingshoofden en teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingshoofden en teamleiders zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De afdelingshoofden en teamleiders zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Alle medewerkers van de omgevingsdienst 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.

- Afdelingshoofden en teamleiders dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden en teamleiders voeren quickscans informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG uit om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen 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 onder leiding van de CISO, door de teamleider IV een IP&P plan opgesteld gebaseerd op:
  - Dit IB&P beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - Andere audit resultaten;
  - het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risico-analyses en DPIA's
  - De door het management 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 IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. 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 het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense'). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO, Security Officers, Privacy Officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA coördinator.

3.1 Aansturing: directeur

De directeur zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De directeur zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. De directeur zorgt dat de eindverantwoordelijke portefeuillehouders binnen management team gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het managementteam zich ook verantwoorden naar de deelnemers.

De directeur stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directeur draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de Concern CISO en Privacy Officer van de omgevingsdienst. De directeur autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de Omgevingsdienst Haaglanden gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: Afdelingshoofden

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van de afdelingshoofden. 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, (persoons)gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Afdelingshoofden rapporteren aan de directeur over

omgevingsdienst Haaglanden

de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het MT-overleg.

Taken van de afdelingshoofden 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 IB&P beleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO en PO 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. Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.3 Uitvoering: Teamleiders
Teamleiders kunnen de uitvoerende taken zoals genoemd bij de afdelingshoofd overnemen voor hun respectievelijke aandachtsgebied. De werkzaamheden en uitvoering blijven daarbij identiek.

3.4 Controle en verantwoording
Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het bestuur van de Omgevingsdienst Haaglanden. De directeur en het management van de Omgevingsdienst Haaglanden zullen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
De directeur is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4.1 ENSIA
De omgevingsdienst verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingshoofden. De afdelingshoofden leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging en privacybescherming komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging en privacy. Met deze verklaring geeft het bestuur aan in hoeverre de omgevingsdienst voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging en wettelijke eisen zoals uit de AVG. Ook worden de eventuele verbetermaatregelen vermeld die de omgevingsdienst gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de verklaring aan de deelnemers.

Via ENSIA verantwoordt de omgevingsdienst zich ook aan de stelselhouders voor DIGID/WOZ/BAG/SUWI.

Middels deze verantwoording worden het bestuur van de omgevingsdienst en de leden geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de omgevingsdienst informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Vastgesteld op : 19 maart 2026

De secretaris,
Mr. C. van der Kamp

De voorzitter,
M.R. Ferwerda MSc.