Omgevingsdienst Rivierenland

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 849

17 augustus 2020

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Rivierenland

Strategisch Informatiebeveiligingsbeleid ODR 2020-2023

Samenvatting

Deze notitie beschrijft het strategisch informatiebeveiligingsbeleid van de Omgevingsdienst Rivierenland (ODR) voor de jaren 2020 tot 2023. Deze notitie is richtinggevend en kaderstellend.

Informatieveiligheid gaat over de beschikbaarheid, integriteit en de vertrouwelijkheid van informatie.

De komende jaren zet de ODR in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveilingsfunctie in de organisatie.

Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de ODR en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

De ambitie van de ODR is te voldoen aan het BIO-normenkader; het realiseren daarvan is voor de ODR al een forse inspanning. Dat wordt veroorzaakt door de nadruk op schriftelijke verantwoording en vastlegging van procedures en uitvoeringspraktijk.

Hierbij is het uitgangspunt dat de bereikte veiligheid in verhouding moet staan tot de kosten. De organisatie is zich ervan bewust dat, alle inspanningen ten spijt, 100% garantie niet geboden kan worden.

Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging. Het MT is verantwoordelijk voor de uitvoering van het strategisch informatieveiligheidsbeleid en stelt jaarlijks het informatiebeveiligingsplan vast. De primaire verantwoordelijkheid voor de bescherming van informatie ligt bij de eigenaar, de afdelingshoofden.

Dit strategische beleid wordt door het Dagelijks Bestuur vastgesteld. Alle onderliggende beleidsstukken, handleidingen en protocollen worden door het MT vastgesteld.

1. Inleiding

Deze notitie beschrijft het strategisch informatiebeveiligingsbeleid van de Omgevingsdienst Rivierenland (ODR) voor de jaren 2020 tot 2023. Dit document legt de basis voor informatieveiligheid binnen de ODR. Deze notitie is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten (voor informatiebeveiliging op tactisch niveau) en werkinstructies (op operationeel niveau).

Met dit 'Strategisch Informatiebeveiligingsbeleid 2020-2023' zet de ODR een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de organisatie te continueren en voort te gaan met de implementatie van de Baseline Informatiebeveiliging Overheid (BIO).

De basis voor dit strategisch beleid is Baseline Informatiebeveiliging Overheid (BIO)[1]. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG [2].

[1] *https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/*
[2] *https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/*

1.1 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 en vertrouwelijkheid (BIV) van persoonsgegevens en andere informatie.

- *Beschikbaarheid (of continuïteit)*: het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor gebruikers (tijdigheid en continuïteit);
- *Integriteit (of juistheid)*: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverstrekking;

- *Vertrouwelijkheid (of exclusiviteit)*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Hier blijkt ook de rechtstreekse relatie met privacy. Zowel informatiebeveiliging als privacy gaat over het beschermen, beheren en beheersen van informatie. Waarbij privacy specifiek aandacht vraagt voor de bescherming van persoonsgegevens. Bij informatiebeveiliging gaat het juist om de bescherming van álle relevante organisatiegegevens.

1.2 Waarom informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van de ODR, zowel bij de uitvoering, voor de sturing en voor het afleggen van verantwoording. Toegankelijke en betrouwbare informatie is daarom een kritische succesfactor voor het functioneren van de organisatie.

De ODR wil in alle opzichten een betrouwbare partner zijn. Een betrouwbare informatievoorziening waarbij de informatie, van al onze klanten, partners en onze eigen bedrijfsgegevens, wordt beschermd en de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van gegevens is hierbij noodzakelijk.

De 'bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden. Informatieveiligheid is hiermee een integraal onderdeel van onze dagelijkse bedrijfsvoering en dienstverlening.

1.3 Ambitie en visie ODR op het gebied van informatieveiligheid

<u>Koers ODR</u>
De ODR wil zijn taken de komende vijf jaar steeds beter doen door meerwaarde te bieden met onze dienstverlening. Daarom stellen we kwaliteit en innovatie centraal. En handelen we flexibel en transparant. We willen een dienstverlening die betrouwbaar, snel, persoonlijk, duidelijk en toegankelijk is.

<u>Visie</u>
De komende jaren zet de ODR in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveilingsfunctie in de organisatie.

Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de ODR en de basis voor het beschermen van rechten van burgers en bedrijven. Met betrouwbaarheid wordt bedoeld:
- beschikbaarheid (continuïteit van de bedrijfsvoering),
- integriteit (juistheid, volledigheid) en
- vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.

Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een 'kans'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken.

<u>Ambitie informatieveiligheid</u>
De ambitie van de ODR is te voldoen aan het BIO-normenkader; het realiseren daarvan is voor de ODR al een forse inspanning. Dat wordt veroorzaakt door de nadruk op schriftelijke verantwoording en vastlegging van procedures en uitvoeringspraktijk.

Hierbij is het uitgangspunt dat de bereikte veiligheid in verhouding moet staan tot de kosten. De organisatie is zich ervan bewust dat, alle inspanningen ten spijt, 100% garantie niet geboden kan worden.

Bij informatieveiligheid is de medewerker vaak de zwakste schakel. De ODR heeft dan ook als doelstelling zowel de technische als de organisatorische (menselijke) aspecten op een acceptabel (vastgesteld door het MT) veilig niveau te brengen.

1.4 Reikwijdte en afbakening informatiebeveiliging

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen

(de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen.

Dit beleid is van toepassing op de gehele organisatie, alle organisatieonderdelen, alle processen, informatiesystemen, informatie en gegevens van de ODR en externe partijen (bijvoorbeeld veiligheidsregio's), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

De AVG is geen onderdeel van het Informatiebeveiligingsbeleid; de beveiligingsnormen van de Baseline Informatiebeveiliging Overheid (BIO) voldoen wel aan de wettelijke eisen die de AVG aan overheidsorganisaties stelt. Opzet, bestaan en werking van een actueel informatiebeveiligingsbeleid zijn vereisten voor het voldoen aan de AVG.

1.5 Plaats van het strategisch informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de ODR, het informatiebeveiligingsbeleid van de gemeente Buren (hier nemen we onze ICT-voorzieningen af) en de relevante landelijke en Europese wet- en regelgeving.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en zal worden vertaald in tactische en operationele richtlijnen en maatregelen. Bewust nemen we in het strategisch beleid geen limitatief overzicht op van onderliggende documenten. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd, bijvoorbeeld wachtwoordenbeleid.

In het jaarlijks uit te brengen Informatiebeveiligingsplan (vast te stellen door het MT) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de informatiemanager en de jaarlijkse AVG-toetsing (door FG). Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.

1.6 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

2. Strategisch beleid

2.1 Doel

De doelen van het informatiebeveiligingsbeleid zijn:
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers
- Het borgen van de continuïteit van kritische bedrijfsprocessen en bedrijfsvoering
- Het managen van de informatiebeveiliging door het toekennen van rollen, taken en verantwoordelijkheden.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang tot systemen, gegevens en gebouwen.
- Het waarborgen van correcte en veilige informatievoorzieningen -systemen.
- Het waarborgen van de naleving van dit beleid.

2.2 Ontwikkelingen

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

2.1 Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is het nieuwe normenkader voor de gehele overheid. Dit normenkader is gebaseerd op de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. De BIO bestaat uit een aantal normen en bijbehorende maatregelen. De BIO heeft voor elke norm drie basisbeveiligingsniveaus (BBN) 1, 2 en 3. Het BBN wordt bepaald met behulp van drie aspecten. Dit zijn de mate van beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Het BBN-niveau wordt voornamelijk bepaald door de vertrouwelijkheid. Aan de hand van deze drie aspecten wordt bepaald welke maatregelen nodig zijn in verhouding tot de grootte van het risico. De omvang van het risico is bepalend voor de te nemen maatregelen.

Keuze ODR: Processen worden standaard als BBN 2 ingeschaald; het is aan de proceseigenaar om hiervan af te wijken door BBN 1 (geen risico) of BBN3 (hoog risico) aan het proces toe te kennen door middel van een risico-analyse. De adequate invulling en uitvoering van het informatiebeveiligingsbeleid is daarmee nauw verbonden met een actuele procesinrichting van de organisatie en weloverwogen risicomanagement. De werkwijze van deze BIO is meer gericht op risicomanagement. Dit houdt voor het management en coördinatoren in, dat zij op voorhand keuzes maken en continu afwegingen maken of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Het toekennen van classificatieniveaus aan data is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen In bijlage 2 staan de niveaus van beschikbaarheid, integriteit en vertrouwelijkheid uitgewerkt. Samen vormen zij het betrouwbaarheidsniveau waarin de informatiebeveiliging moet voldoen.

2.2.2 De 10 bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes voor informatiebeveiliging [1] zijn een aanvulling op de BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes gaan vooral over de rol van de bestuurder bij het borgen van informatiebeveiliging in de organisatie. De principes zijn:

- Bestuurders bevorderen een veilige cultuur
- Informatiebeveiliging is van iedereen
- Informatiebeveiliging is risicomanagement
- Risicomanagement is onderdeel van de besluitvorming
- Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
- Informatiebeveiliging is een proces
- Informatiebeveiliging kost geld
- Onzekerheid dient te worden ingecalculeerd
- Verbetering komt voort uit leren en ervaring
- Het bestuur controleert en evalueert

Kortom, 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 ODR (bijvoorbeeld datalekken), dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

[1] *Deze principes zijn gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)*

2.2.3 De AVG

De Algemene Verordening Gegevensbescherming (AVG) stelt hoge eisen aan de verantwoording die organisaties moeten afleggen over hoe we met (persoons-)gegevens omgaan. Art. 32 van de AVG verplicht een organisatie passende technische en organisatorische maatregelen te nemen ‘:. om vertrouwelijkheid, integriteit en beschikbaarheid [..] te garanderen. Uit deze drie aspecten is ook informatiebeveiliging opgebouwd. Om AVG-compliant te zijn moet de ODR daarom zijn informatiebeveiliging op orde hebben.

2.2.4 ICT-beleid gemeente Buren

De ODR neemt zijn ICT af bij de gemeente Buren. Hierdoor is de ODR voor een groot deel afhankelijk van het informatiebeveiligingsbeleid van de gemeente Buren.

2.2.5 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. Aan de hand van dit dreigingsbeeld brengt de gemeente Buren focus aan in het actualiseren van beleid en plannen voor informatiebeveiliging.

Samenwerking met de gemeente Buren op het gebied van informatiebeveiliging ligt voor de hand: in het delen van kennis, het delen van standaardprotocollen/-documenten en incidenteel het samen aanbesteden van software.

2.2.6 Informatie uit incidenten en inbreuken op de beveiliging

De ODR 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

2.3.1 NEN-ISO/IEC 27001:2017

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. Waar beschikbaar neemt de ODR de landelijke normen over, voor zover die als zodanig zijn vastgesteld of door de VNG aangenomen. Een voorbeeld hiervan is de NTA 7516 (veilig mailen in de zorg), die naar verwachting in 2020 of 2021 als algemene norm door de VNG/IBD zal worden geaccepteerd.

2.3.2 Landelijke standaardmodellen

Met het oog op standaardiseren en het gebruik van *best practice* gebruiken we net als onze gastheer, de gemeente Buren, zoveel mogelijk de landelijk beschikbare standaardmodellen zoals die voor privacy (verwerkersovereenkomsten en dergelijke), als voor tactisch beleid zoals toegangsbeleid.

2.4 Uitgangspunten

Voor informatiebeveiliging hanteert de ODR een aantal strategische uitgangspunten en randvoorwaarden. De uitgangspunten leggen kernachtig het belang van informatie vast en hoe deze in hoofdlijnen wordt beheerd.

- Alle informatie en informatiesystemen zijn van belang voor de ODR, bepaalde informatie is van vitaal en kritiek belang. *Het belang bepaalt het vereiste niveau van bescherming, dat wordt vastgesteld op basis van het waargenomen risico*.
- Alle informatiebronnen en -systemen die gebruikt worden door de ODR hebben een afdelingshoofd als interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt bij de eigenaar van die informatie.
- Door periodieke controle, organisatiebrede planning en coördinatie wordt de kwaliteit van de informatievoorziening verankerd 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. De jaarlijkse AVG-toetsing is hierbij leidend. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Het onderwerp informatiebeveiliging wordt bij de ODR gezien als een integraal onderdeel van risicomanagement.

2.5 Randvoorwaarden

Om informatieveiligheid in de organisatie te borgen hanteert de ODR een aantal randvoorwaarden. Deze randvoorwaarden benoemen de inbedding in, en afstemming op andere vormen van beleid binnen de organisatie.

- De ODR stelt de benodigde mensen en middelen beschikbaar om zijn eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden *door bestuur en leidinggevende (MT en coördinatoren)*.

- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de informatiemanager gebaseerd op:

  - de jaarlijkse AVG-toetsing (door FG);
  - informatiebeveiligingsbeleid gemeente Buren;
  - De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.
  - Input informatiemanager.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie.

Het dagelijks bestuur, het MT en de coördinatoren spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het MT maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de ODR heeft, de risico's die de ODR hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het MT dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het MT geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele ODR.

De tweede lijn (FG,CISO gastheer, informatiemanager, privacycoördinator, organisatiejurist) ondersteunt, adviseert, coördineert en bewaakt of het MT zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

De rollen, taken en verantwoordelijkheden zijn samengevat in bijlage 1, governance gegevensbescherming. De inrichting van de governance op de gebieden van informatieveiligheid en privacy (AVG) overlapt zodanig dat hiervoor één governancedocument is opgesteld.

3.1 Governance

De governance is ingericht volgens de onderstaande uitgangspunten:

3.1.1 Dagelijks bestuur

- Het dagelijks bestuur is eindverantwoordelijke voor de informatiebeveiliging en stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.

3.1.2 MT

- Het MT stelt jaarlijks het informatiebeveiligingsplan vast.
- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het MT stelt onderliggend tactisch beleid en protocollen vast.
- Het MT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast.
- Het MT stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie);
- Het MT stuurt op risico's;
- Het MT controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- Het MT is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het MT stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het MT rapporteert over compliance aan wet- en regelgeving en informatiebeveiligingsbeleid van de ODR in de managementrapportages.

3.1.3 Lijnmanagement

- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement.
- Het lijnmanagement is verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn

- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

- Het lijnmanagement is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;

- Het lijnmanagement stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het lijnmanagement ziet erop toe dat medewerker adequate maatregelen nemen voor de bescherming van de informatie die onder hun verantwoordelijkheid valt
- De afdelingshoofden zijn verantwoordelijk voor het zodanig inrichten van processen en rollen dat conflicterende taken en verantwoordelijkheden worden gescheiden.
- Het lijnmanagement is ervoor verantwoordelijk dat alleen daartoe geautoriseerde medewerkers persoonsgegevens inzien en verwerken.
- Het lijnmanagement dient erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De afdelingshoofden zijn verantwoordelijk voor het borgen van informatieveiligheid en continuïteit van gegevensbeheer bij projecten, ongeacht het soort project.

3.1.4 Medewerkers

Alle medewerkers, zowel vast als tijdelijk, intern of extern, hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen die voortvloeien uit dit beleid. Iedere medewerker is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

In informatieveiligheid is de mens de zwakste schakel. Daarom worden alle medewerkers van de ODR getraind in het gebruik van beveiligingsprocedures. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.

3.1.5 Informatiemanager

- De informatiemanager ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover zo nodig rechtstreeks aan het MT.
- De informatiemanager stelt het strategisch informatiebeveiligingsbeleid op
- De informatiemanager stelt jaarlijks voor het MT een Informatiebeveiligingsplan op (IPB) , op basis van:

  ° de uitkomsten van de jaarlijkse AVG-audit (door FG)
  ° het (tweejaarlijkse) dreigingsbeeld gemeenten van de IBD;
  ° De door de afdelingshoofden/coördinatoren ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.
  ° Overige ontwikkelingen zoals signalen uit de organisatie, rapportage informatieveiligheidsincidenten etc.

3.1.6 Controller

De controller richt zich op de planning en control (P&C cyclus) van financiën, processen, de doelmatigheid van beleid (zoals dit informatieveiligheidsbeleid) en doet dit op basis van risicomanagement. In de P&C cyclus is informatieveiligheid een structureel onderwerp.

3.2 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het dagelijks bestuur van de ODR. Het MT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het MT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

De controle en verantwoording van informatieveiligheid valt uiteen in twee onderdelen:
- Informatiebeveiliging

De informatiemanager rapporteert over de uitvoering van het informatieveiligheidsbeleid en het naleven van uitvoeringsrichtlijnen aan de directeur/MT.

- Privacy
  Over naleving van de AVG rapporteert de FG jaarlijks aan het dagelijks bestuur. De rapportage bevat elementen waaruit duidelijk wordt op welke onderwerpen aan de AVG wordt voldaan en waar verbetering nodig is. Hieruit volgen aanbevelingen waarbij de prioriteit is weergegeven. Door onderdelen die verbetering vereisen uit te voeren neemt de Omgevingsdienst verantwoordelijkheid om aan de AVG te voldoen.

Bijlage 1: Governance: rollen, taken en bevoegdheden

Bijlage bij:
- **Strategisch privacybeleid**
- **Strategische informatiebeveiligingsbeleid 2020-2023**

Een adequate organisatie geeft richting en advies, controleert en rapporteert. De uitvoering van het beleid is en blijft een lijnverantwoordelijkheid.

Onderstaand zijn de verschillende rollen uitgeschreven. Informatiebeveiliging en privacy (AVG) komen hierin samen.

Wie	Rollen en Taken	PB	IB
Dagelijks Bestuur	Eindverantwoordelijke	X	X
	Politiek verantwoordelijk voor een passend niveau gegevensbescherming	X	X
	Stelt beleid vast	X	X
MT	Verantwoordelijk voor uitvoering van organisatiebrede vraagstukken ten aanzien van gegevensbescherming	X	X
	Verantwoordelijk voor de inrichting en werking van beveiligingsorganisatie.	X	X
	Voert regie en houdt toezicht op zijn processen inzake Gegevensbescherming	X	X
	Aantoonbaar compliant aan wetten en kaders	X	X
	Dataclassificatie van systemen en gegevens (-verzamelingen)		X
	Risicoafweging en treffen maatregelen	X	X
	Medewerkers meenemen in hun verantwoordelijkheid	X	X
	Vaststellen gewenste niveau van gegevensbescherming en uitgangspunten (zoals bijv gebruik standaard VNG)		X
	Stelt uitvoeringsrichtlijnen vast (gedragsregels, Toepassingsregels)	X	X
Afdelingshoofd / Coördinatoren / Proceseigenaren / Procesverantwoordelijke	Operationele verantwoordelijkheid voor systemen en processen		X
	Voert regie en houdt toezicht op zijn processen inzake gegevensbescherming	X	X
	Stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesysteem vast.		X
	Het treffen van maatregelen op basis van risicomanagement		X
	Zorgen voor bewustwording onder personeel	X	X
	Beheersen van en rapporteren over incidenten	X	X
	Verantwoordelijke voor implementatie juiste beveiligingsniveau		X
	Manager kan taken opdragen aan medewerker blijft echter verantwoordelijk	X	X

Medewerkers	Zijn verantwoordelijk ten aanzien van de veiligheid van gegevens in hun dagelijkse werkprocessen	X	X
	Werken volgens en binnen richtlijnen, kaders en gedragsregels	X	X
Functionaris Gegevensbescherming	Intern toezichthouder verwerking persoonsgegevens / naleving van de AVG	X	X
	Verantwoordelijk voor het toezicht op de naleving van de privacywetten en –regels	X	X
	Adviseert en informeert de organisatie en medewerkers over allerlei privacy gerelateerde zaken	X	X
	Verantwoordelijk voor het afhandelen van vragen en klachten	X	X
	Adviseert en ondersteunt bij privacy impact assessments (PIA's)	X	X
	Contactpersoon AP	X	X
	Rapporteert aan het Dagelijks Bestuur (DB) / directeuren	X	X
Informatiemanager	Verantwoordelijk voor het implementeren van, adviseren over en toezicht houden op het informatiebeveiligingsbeleid		x
	Formuleert IB beleid		X
	t Formuleert het informatiebeveiligingsplan (IBP)		X
	Controle op uitvoering beveiligingsplan		X
Privacycoördinator	Interne contactpersoon voor privacygerelateerde zaken	X	
	Bewaakt en beheert het register van incidenten en datalekken	X	
	Contactpersoon FG bij mogelijke inbreuken, incidenten, datalekken	X	X
Organisatiejurist	Adviseert over juridische vraagstukken rondom privacy en het verwerken en beschermen van persoonsgegevens	X	
	Adviseert over het register van verwerkingen	X	
	Adviseert over en sluit verwerkersovereenkomsten af	X	
	Handelt verzoeken met betrekking tot rechten van betrokkenen af	X	
	Vormt dossiers van de achterliggende stukken	X	
	Bewaakt het inzageproces en schaalt indien van toepassing op naar de klachtenprocedure	X	X
Adviseur informatiebeheer	Verantwoordelijk voor het bewaken en beheren van het verwerkingsregister	X	X
Controller	Sparring partner voor FG, informatiemanager, privacy coordinator bewaakt koppeling privacy- en informatiebeveiligings-doelen aan organisatiebrede inspanning om 'in control' te worden	X	X

Bijlage 2 Dataclassificatie
Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie: Het toekennen van classificatieniveaus aan data is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen

Het informatiebeveiligingsbeleid van de ODR beschrijft globaal de normen voor het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Hier wordt tevens de relatie gelegd naar het BBN niveau van de BIO.

De onderscheiden niveaus van **beschikbaarheid** zijn:

- Niet nodig (0): De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
- Belangrijk (BBN1): De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen
- Noodzakelijk (BBN2): De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schade toebrengen.
- Essentieel (BBN2 met aanvullende risicoanalyse): De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van beschikbaarheid kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van **integriteit** zijn:
- Niet zeker (0): Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- Beschermd (BBN1): Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-) fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van integriteit kan enige (in-)directe schade toebrengen
- Hoog (BBN2): Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan serieuze (in)directe schade toebrengen.
- Absoluut (BBN2 met aanvullende risicoanalyse): Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade.

De onderscheiden niveaus van **vertrouwelijkheid** zijn:
- Openbaar (0): Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.
- Bedrijfsvertrouwelijk (BBN1): Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.
- Geheim (BBN2): Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.
- Geheim (BBN3): Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen.