OMGEVINGSDIENST ZUIDOOST-BRABANT

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1038

5 mei 2026

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Zuidoost-Brabant

Strategisch Informatiebeveiliging- en privacy beleid 2026-2030

Het opgestelde strategisch informatiebeveiliging en privacy beleid (Strategisch informatiebeveiliging- en privacybeleid 2026-2030) vast te stellen en dit met terugwerkende kracht met ingang van 1 januari 2026 in werking te laten treden en gelijktijdig het nog geldende informatiebeveiligingsbeleid uit 2019 (Informatiebeveiligingsbeleid ODZOB 2019-2023) in te trekken.

1. Inleiding

Digitalisering verandert onze samenleving voortdurend en biedt kansen. De grote impact van digitalisering volgt uit de grote verwevenheid ervan in alle beleidsonderdelen van de overheid, van het fysiek domein tot democratie. Daarin helpt digitalisering om de data- en informatievoorziening te verbeteren en de grote opgaven die er liggen aan te pakken. Dat gaat niet vanzelf. Er is nog veel te doen om de kansen van gisteren goed te pakken en klaar te zijn voor die van morgen.

Het is ook duidelijk dat er risico's met digitalisering meekomen. Kwetsbaarheden en dreigingen nemen in het digitale domein toe. Landelijk presenteren het Nationaal Cyber Security Center (NCSC), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Informatie Beveiligingsdienst Gemeenten (IBD) dreigingsbeelden rondom integrale veiligheid, informatieveiligheid en cybersecurity. Deze geven een duidelijk beeld van ontwikkelingen, dreigingen en risico's die ook voor de ODZOB relevant zijn. Ook uit onze eigen monitoring blijken kwetsbaarheden en dreigingen toe te nemen. Dit vraagt om continue extra inspanningen om de digitale weerbaarheid te versterken en te borgen.

De ODZOB staat gezamenlijk voor een daadkrachtige, verbindende en betrouwbare organisatie: "Een toekomstgerichte informatievoorziening, die bijdraagt aan een weerbare en wendbare organisatie". Het borgen van de informatieveiligheid is hierbij een belangrijke randvoorwaarde.

Dit beleid geldt voor de jaren 2026 tot en met 2030 en vervangt het "Informatiebeveiligingsbeleid 2019-heden".

1.1. Wat is informatieveiligheid

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 informatiebeveiligingsbeleid geldt voor alle processen van de ODZOB 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.

1.2. Risicomanagement

Risicomanagement vormt de kern van informatiebeveiliging binnen de ODZOB-context. Uitgangspunt voor informatiebeveiliging is het systematisch identificeren, analyseren en behandelen van risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie kunnen aantasten. Voor privacy geldt dat er risicobeoordelingen moeten worden uitgevoerd om de risico's voor rechten en vrijheden van betrokkenen te beoordelen. Het risicomanagement voor informatiebeveiliging is gebaseerd op de normen ISO 27001 en ISO 27005 en voor privacy op het IBD Privacy Normenkader. Deze normen bieden een gestructureerde methode voor risicoanalyse en -behandeling. De methode voor informatiebeveiliging op procesniveau is de Business Model Canvas-aanpak (BMC). BMC is een manier om in kaart te brengen hoe het te onderzoeken proces er uitziet en welke risico's daar zijn. Daarnaast wordt MAPGOOD (Mens-Apparatuur-Programmatuur-Gegevens-Organisatie-Omgeving-Diensten) methodiek gebruikt om generieke risico's in kaart te brengen. Beide zijn vooral ook een mooi communicatiemiddel naar de managers en bieden daarnaast een gestructureerde en herhaalbare aanpak om procesrisico's te vinden en te beoordelen en om passende maatregelen te bedenken. Dit is noodzakelijk voor het waarborgen van dienstverlening, naleving van wet- en regelgeving, en bescherming van persoonsgegevens.

1.3. Privacy & Gegevensbescherming (AVG)

De ODZOB werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens heeft de ODZOB om de wettelijke taken goed uit te kunnen voeren.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben uitvoeringsorganisaties, zoals de ODZOB, een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van de ODZOB, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De maatschappij moet erop kunnen vertrouwen dat de ODZOB zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.4. Wet Politie Gegevens (Wpg)

De Wet politiegegevens (Wpg) is een wet die regelt hoe politiegegevens, zoals persoonsgegevens van verdachten en slachtoffers, mogen worden verwerkt bij politietaken, inclusief opsporing en de uitvoering van justitiële taken. De Wpg bepaalt onder andere welke gegevens de politie mag verzamelen, hoe deze bewaard en doorgegeven mogen worden, en hoe burgers hun privacy rechten kunnen uitoefenen, zoals het opvragen van hun gegevens. De ODZOB heeft handhavers in dienst (BOA's). Zij dienen zich te houden aan de Wpg.

1.4.1. Basis op orde

Voor informatiebeveiliging en privacy is het van groot belang om de fundamenten voor deze onderdelen te borgen in de organisatie. Een passende beheersing van informatiebeveiligings- en privacy risico's is rand voorwaardelijk voor het bereiken van de strategische organisatiedoelen. Door de komende periode verder te investeren in een stabiele fundering wordt de kans op incidenten (storingen, hacks, onderbrekingen van de dienstverlening, datalekken etc.) verkleind.

1.4.2. Voldoen aan wet- & regelgeving

Voor informatiebeveiliging is onder andere de volgende wet- en regelgeving belangrijk:

- Baseline Informatiebeveiliging Overheid 2.0 (BIO2)
- Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG)
- Cyberbeveiligingset (Cbw) – Nederlandse implementatie Network and Information Security (NIS2)
- Wet Politiegegevens (Wpg)
- Cyber Resilience Act (CRA)
- AI Act

1.4.3. Inzetten op digitale weerbaarheid

Digitalisering van de diensten is niet meer weg te denken in de dienstverlening. Dit zorgt echter voor een afhankelijkheid van externe factoren (stroomvoorziening, leveranciers etc.). Door in te zetten op digitale weerbaarheid wordt er structureel aandacht besteed aan:

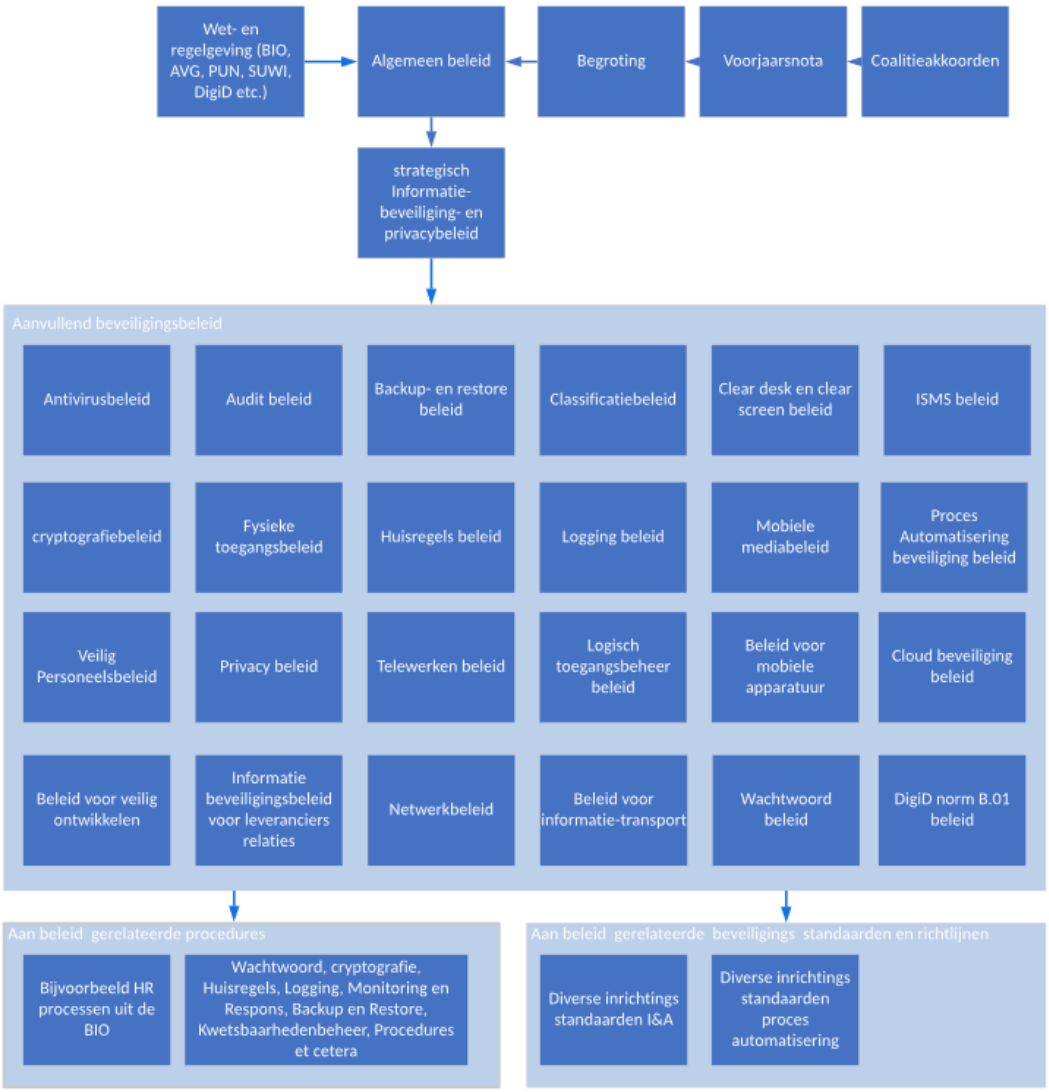
- inzicht hebben op cyberincidenten, -dreigingen en risico's en hoe hiermee om te gaan.
- bescherming tegen digitale risico's: Het minimaliseren van negatieve effecten voor onze organisatie(s) en onze afnemers, toeleveranciers of anderen.
- in staat zijn om adequaat te reageren, te herstellen en snel te leren op en van cyberincidenten en –crises: Periodieke oefeningen zijn voor de digitale weerbaarheid (net als het herhalen van brand- en BHV oefeningen) van cruciaal belang.

1.4.4. Inzetten op bewustwording (awareness)

Investeren in onze collega's is van cruciaal belang om informatiebeveiliging en privacy te kunnen borgen in onze organisatie(s). Hierop zetten we al in en we kunnen kennis en ervaring delen. Door periodiek verschillende onderdelen te trainen wordt de kans op incidenten en interrupties van de dienstverlening steeds kleiner (voorbeelden hiervan zijn naast trainingen, e-learnings, phishing testen, uitnodigen van sprekers, omgaan met nieuwe ontwikkelingen, etc.).

1.5. Beleidssamenhang

Dit Strategisch informatiebeveiligings- en privacy beleid (IB&P) maakt onderdeel uit van het integrale informatieveiligheidsbeleid van de ODZOB. Het is de kapstok voor alle overige beleid, richtlijnen en procedures op het gebied van informatieveiligheid en privacy:



2. Strategisch beleid

2.1. Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligings- en privacy beleid'. 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). Het beleid op informatiebeveiliging en privacy 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. Ambitie en visie van de ODZOB op het gebied van informatieveiligheid en privacy

Digitalisering zit steeds meer in het hart van onze organisaties. De maatschappelijke relevantie van de lokale overheid richting inwoners en ondernemers is sterk afhankelijk van de inzet van digitale middelen. Daarom zullen wij de komende jaren hierin moeten (blijven) investeren. Doen wij dit niet dan vormt dit een rechtstreekse bedreiging voor onze bedrijfsvoering en (publieke) dienstverlening en maatschappelijke waarde van onze organisatie.

Ambitie:
De ODZOB wil een digitaal veilige organisatie zijn die het vertrouwen van inwoners, bedrijven en deelnemers waarborgt (landelijk volwassenheidsniveau 3, basis op orde[1]).

1) Landelijke overheidsorganisaties streven ernaar om eind 2026 volwassenheidsniveau 3 (gestructureerd en gedocumenteerd) te bereiken voor hun informatiehuishouding en informatiebeveiliging. Dit niveau is noodzakelijk om te voldoen aan de Wet open

Visie:
Privacy en informatieveiligheid zijn een gedeelde verantwoordelijkheid binnen de hele organisatie. Niet alleen technologie, maar ook menselijk gedrag speelt hierin een cruciale rol. Door risico's vroegtijdig te herkennen, bewust vragen te stellen over gegevensgebruik en passende maatregelen te treffen, wordt informatieveiligheid een continu en integraal onderdeel van het werk. Voorbeeldgedrag van medewerkers, leidinggevenden en bestuur is daarbij essentieel.

Missie:
De ODZOB beschermt dagelijks privacygevoelige gegevens van inwoners, organisaties en deelnemers door zorgvuldig, veilig en verantwoord met deze informatie om te gaan. Medewerkers worden ondersteund in het veilig uitvoeren van hun werk, zodat de continuïteit van processen gewaarborgd blijft

2.2.1. Strategische en tactische doelen

Strategische doelstellingen voor informatieveiligheid richten zich op het beschermen van informatie en informatiesystemen tegen ongeautoriseerde toegang, gebruik, openbaarmaking, verstoring, wijziging of vernietiging. Belangrijke doelstellingen voor de ODZOB:

- Bescherming van vertrouwelijkheid: Zorgen dat gevoelige informatie alleen toegankelijk is voor geautoriseerde personen.
- Integriteit waarborgen: Garanderen dat informatie accuraat en volledig blijft en niet ongeautoriseerd wordt gewijzigd.
- Beschikbaarheid verzekeren: Zorgen dat informatie en systemen beschikbaar zijn wanneer nodig door geautoriseerde gebruikers.
- Risicomanagement: Identificeren, evalueren en mitigeren van risico's die de informatieveiligheid kunnen bedreigen.
- Naleving van wet- en regelgeving: Voldoen aan relevante wetten, regelgeving en normen zoals de AVG (Algemene Verordening Gegevensbescherming) en de BIO2 (Baseline Informatiebeveiliging Overheid).
- Bewustwording en training: Bevorderen van een cultuur van veiligheid door middel van regelmatige training en bewustwordingscampagnes voor medewerkers en bestuurders.

Deze doelstellingen helpen de ODZOB om een robuuste en veerkrachtige informatiebeveiligingsstrategie te ontwikkelen en te onderhouden.

Tactische doelstellingen voor informatieveiligheid zijn meer specifiek en gericht op de implementatie van strategische doelstellingen. Voor de ODZOB:

- Beveiligingsmaatregelen implementeren: Uitvoeren van technische en organisatorische maatregelen zoals firewalls, antivirussoftware, en toegangscontrole.
- Incidentbeheer: Opzetten van procedures voor het identificeren, melden, en reageren op beveiligingsincidenten.
- Continuïteitsplanning: Ontwikkelen van plannen om de continuïteit van kritieke bedrijfsprocessen te waarborgen in geval van een beveiligingsincident.
- Vulnerability management: Regelmatig uitvoeren van kwetsbaarheidsscans en penetratietests om zwakke plekken in systemen te identificeren en te verhelpen.
- Training en bewustwording: Organiseren van trainingen en campagnes om medewerkers bewust te maken van beveiligingsrisico's en best practices.
- Compliance monitoring: Controleren en rapporteren van naleving van interne en externe beveiligingsnormen en regelgeving

Deze doelstellingen helpen de ODZOB om de informatieveiligheidsstrategie effectief uit te voeren en te onderhouden.

2.3. Kaders en ontwikkelingen

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

2.3.1. NIS2 en Cyberbeveiligingswet (Cbw)

Eind 2022 is de NIS2 richtlijn in Europa vastgesteld. Hierbij ligt de nadruk op de zorgplicht waarbij elke organisatie verplicht is risicobeoordelingen uit te voeren en passende maatregelen te treffen. De NIS2 wordt door elke Europese lidstaat vertaald naar eigen wetgeving (Cyberbeveiligingswet). Voor Nederland staat deze gepland voor Q2 2026)

overheid (Woo), de Cyberbeveiligingswet, en de BIO2 (Baseline Informatiebeveiliging Overheid). Het houdt in dat maatregelen organisatiebreed zijn geborgd, aantoonbaar en toetsbaar zijn

2.3.2. De BIO2
De BIO2 (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO2 is gericht op risicomanagement. Dat wil zeggen dat de managers 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.
De BIO is met ingang van eind 2025 opgevolgd door de BIO2. Deze is eind 2025 bestuurlijk verankerd, en daarmee verplicht voor de ODZOB. Met de komst van de Cyberbeveiligingswet (Cbw) zal deze verankering ook wettelijk zijn (naar verwachting Q2 2026).

2.3.3. 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 ODZOB 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).

2.3.4. De WPG
De ODZOB heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (WPG). Hiervoor moet de organisatiebeleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risicoinschatting, registratie en logging, meldplicht en documentatieplicht.

2.3.5. Artificial Intelligence (AI)
AI wordt ook vanuit de informatiebeveiligingsbril een steeds groter risico. Zo kunnen persoons- en/of gevoelige gegevens ingevoerd worden in openbare AI-modellen, en op die manier openbaar en wellicht misbruikt worden. Zie het voorbeeld van de gemeente Eindhoven dd. december 2025. Ook zijn bijvoorbeeld d.m.v. AI veel betere phishingmails e.d. te genereren. Belangrijk is dan ook dat medewerkers ook op dit aspect bewust gemaakt worden.

2.3.6. De 10 principes voor informatiebeveiliging
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op de 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 en directie bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen de directie bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de ODZOB. Daarmee is informatiebeveiliging ook een onderwerp voor op de bestuurstafel.

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

2.3.8. Informatie uit incidenten en inbreuken op de beveiliging
De ODZOB kent naast het hierboven genoemde dreigingsbeeld 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.

2.4. Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2023. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2023 genomen.

Voor de ondersteuning van gemeenten en uitvoeringsorganisaties bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek6 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 nota zijn al afgestemd op die van de BIO2. Ook het Informatiebeveiligings- en privacy plan zal deze structuur volgen.

Binnen de ODZOB wordt naast IT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering (PA). Het beveiligingsbeleid van de organisatie is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsafdelingen die zich met PA bezighouden.

2.5. Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om een kader te geven en de basis te leggen voor de onderwerp specifieke beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks op te stellen 'IB&P-plan'. Input voor dit plan wordt verkregen van de clustermanagers, de CISO, het dreigingsbeeld van de IBD en uit uitkomsten van jaarlijkse interne audits controle jaarrekening, interne controle IB-P, controleverslag FG, et cetera.)

2.6. Scope informatiebeveiliging
De scope van deze beleidsnota omvat alle processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de ODZOB en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt ook aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG en WPB. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld WBP). 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 tactische beleid gelegd.
- Alle informatie en informatiesystemen zijn van belang voor de ODZOB, bepaalde informatie is van vitaal en kritiek belang. Het DB/Directie is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle informatiesystemen ongeacht waar deze worden gehost.
- Alle Proces Automatiseringssystemen (PA) die binnen de gebouwen die van de ODZOB zijn, zoals inbraak- en toegangssystemen en bijvoorbeeld camera technologie.

2.7. Uitgangspunten
Het bestuur, de directie en het clustermanagement 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 ODZOB heeft, de (privacy) risico's die de ODZOB 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 organisatie. 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 ODZOB en de relevante landelijke en Europese wet- en regelgeving.

2.7.1. Belangrijkste elementen van informatiebeveiliging
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.

2.7.2. Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een lijnverantwoordelijkheid van het clustermanagement. Alle informatiebronnen en -systemen die gebruikt worden door de ODZOB hebben als eigenaar de clustermanager ICT, die de vertrouwelijkheid, privacy eisen 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 (proceseigenaar). Bij de ODZOB is dit de clustermanager ICT voor alle organisatie-brede systemen (zaaksysteem, M365, archief, checklisten,..).
- De clustermanager ICT is verantwoordelijk voor het ter beschikking stellen van de organisatie-brede informatiesystemen. Alle clustermanagers zijn lijnverantwoordelijk voor het correct gebruik van deze systemen
- Door periodieke controle, organisatie brede 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 privacybescherming. In het IB&P plan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatie breed 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 ODZOB 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 risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.7.3. IB&P governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Dagelijks Bestuur stelt als eindverantwoordelijke het strategisch IB&P beleid vast.
- De directie stelt jaarlijks het IB&P plan vast.
- De directie is verantwoordelijk voor vaststellen en 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 door de ODZOB aangewezen syste(e)m(en)
- De directie is verantwoordelijk voor het vragen om informatie bij de clustermanagers en ziet erop toe dat de clustermanagers adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringssystemen 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 jaarlijks rechtstreeks aan de directie in de vorm van een managementreview
- De Privacy Officer (PO) ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de privacy. De PO functie is nog niet ingevuld bij de ODZOB.

- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van de directie 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.
- Tijdens team- en individuele gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO, PO en/of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De clustermanagers zijn lijnverantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De clustermanagers zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De clustermanagers zijn lijnverantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit. Het initiatief hiertoe ligt bij de directie
- Alle medewerkers 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.
- Clustermanagers 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. De CISO en PO laten quickscans informatiebeveiliging uitvoeren op basis van de BIO2 en bij verwerken van persoonsgegevens ook (Pre-)DPIA's op basis van de AVG 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.
- Informatiebeveiliging en privacybescherming volgt de begrotingscyclus van de ODZOB.

2.7.4. 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 een IB&P plan opgesteld, gebaseerd op:
  - Dit IB&P beleid;
  - Andere audit resultaten interne en financiële controle;
  - Het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risicoanalyses en DPIA's
  - De door de proceseigenaren 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, 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.

3.1. Aansturing: algemeen directeur

De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een clustermanager. De directie zorgt dat de clustermanagers zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het Dagelijkse Bestuur 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 DB zich ook verantwoorden naar het Algemeen Bestuur.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacy beleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO (indien aanwezig, anders de FG) van de ODZOB. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt binnen de ODZOB gezien als een integraal onderdeel van risicomanagement.

3.2. Toezicht: Dagelijks bestuur
Het Dagelijks bestuur stelt het strategisch IB&P beleid vast en houdt toezicht dat dit beleid conform afspraken uitgevoerd wordt. Het DB laat zich gevraagd en ongevraagd informeren over de stand van zaken aangaande informatieveiligheid en privacy en stuurt daar waar nodig bij.

3.3. Uitvoering: clustermanager ICT en overige clustermanagers
Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle clustermanagers. 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. Binnen de ODZOB betekent dit dat de clustermanager ICT verantwoordelijk is voor de ODZOB brede informatiesystemen. Deze informatiesystemen dienen te allen tijde te voldoen aan eisen op het gebied van informatieveiligheid (BIV), privacy (AVG), architectuur(principes) en aan de vakinhoudelijke eisen.

Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het MT.

Taken van de clustermanager ICT in het kader van informatiebeveiliging en privacybescherming zijn:
- Het leveren van organisatie-brede informatiesystemen die voldoen aan de eisen gesteld door de BIO2, ISO27001 en Cbw. Dit geldt voor de aanschaf-, beheer- en exit-fase.

Taken van alle clustermanagers 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 teams 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/FG bij nieuwe of gewijzigde processen conform het wijzigingsproces.
- Het tijding melden van voortgang van bijvoorbeeld mitigerende maatregelen aan de CISO en/of FG.
- 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.
- Feedback geven en medewerkers aanspreken op rapportages uit de bewustwordingstrainingen.
- Informatieveiligheid en privacy vast onderwerp maken in de individuele (jaar)gesprekken.
- Informatieveiligheid en privacy vast onderwerp maken in de teamoverleggen.
- Clustermanagers zullen in samenspraak met, en met instemming van clustermanager ICT, CISO, PO en/of FG, verzoeken indienen tot het aanschaffen van IT of OT middelen.

3.4. Uitvoering: Medewerker
Alle medewerkers zijn schakels in de informatiebeveiliging en privacy. Zij dienen deel te nemen aan bewustwordingstrainingen op deze gebieden, en dienen dagelijks alert te zijn als het gaat om informatie- en privacy-veilig omgaan met ODZOB informatie. Zo gebruiken zij alleen die informatie die nodig is voor de vraag, zorgen zij zelf voor een correcte vastlegging van informatie, delen ze geen informatie via onveilige of privé kanalen, laten geen informatie onbeheerd achter, vergrendelen zij de werkplek als deze verlaten wordt, spreken zij onbekenden aan in het gebouw en zijn zij extra alert als het gaat om openen van bijlagen in mails of het klikken op links.

Alle medewerkers hebben de verantwoordelijkheid om incidenten op het gebied van informatiebeveiliging en/of privacy direct te melden.

3.5. Controle en verantwoording

Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het Dagelijks Bestuur en directie van de ODZOB. De bestuurders en directeuren van de ODZOB 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 directie 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.