Strategisch informatiebeveiligings- en privacybeleid 2025-2029

Datum: 4 december 2025
Versie: 0.92
Opsteller: Arno Lammers
Advies: Helmi Martens

Gemeente Helmond

Inhoudsopgave

1 Inleiding 4

1.1 Algemeen & leeswijzer 4

1.2 Positionering van het strategisch IB&P beleid 4

1.3 Scope van het strategisch IB&P beleid 4

1.4 Definities informatiebeveiliging en privacy 5

2 Context en grondslagen 6

2.1 Aansluiting bij algemeen gemeentelijk beleid 7

2.1.1 Ambitie gemeente Helmond 7
2.1.2 Beleidskaders 8
2.1.3 Stakeholders 8

2.2 Ontwikkelingen 8

2.2.1 De BIO2 8
2.2.2 NIS2 en Cyberbeveiligingswet 8
2.2.3 De Cybersecurity Implementatie Richtlijn (CSIR) 9
2.2.4 De Algemene verordening gegevensbescherming (AVG) 9
2.2.5 De Wet politiegegevens (Wpg) 9
2.2.6 Toename van complexe en onvoorspelbare dreigingen 9
2.2.7 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 9
2.2.8 Structuur en samenstelling organisatie 9
2.2.9 AI Verordening 10
2.2.10 Digitale agenda Gemeenten 2028 10
2.2.11 Nederlandse Digitaliseringsstrategie 10

3 Strategisch beleid informatiebeveiliging & privacy 11

3.1 Visie 11

3.2 Strategie 11

3.3 Strategische speerpunten & doelstellingen 12

3.3.1 Bewustwording 12
3.3.2 Risicomanagement 12
3.3.3 IB&P beleidskader 12
3.3.4 IB&P programma (mede) op basis van thema architectuur 13
3.3.5 ISMS gebaseerde aanpak 13
3.3.6 IB&P aspecten van incident management, crisis management & BCM. 14
3.3.7 Doorontwikkeling IB&P organisatie 15

3.4 Uitgangspunten en randvoorwaarden 15

4 Organisatie, taken & verantwoordelijkheden van IB&P 17

4.1 Bestuur 17

4.1.1 Gemeenteraad 17
4.1.2 College van Burgemeester en Wethouders 17
4.1.3 De burgemeester 17

4.2 Ambtelijke organisatie 17

4.2.1 De gemeentesecretaris 17
4.2.2 Directieteam 18
4.2.3 Afdelingsmanagers 18

4.2.4 IB & P organisatie 18
4.2.5 Medewerkers 19
4.2.6 Interne audit 19
4.2.7 CISO 19
4.2.8 Functionaris voor gegevensbescherming (FG) 20
4.2.9 Overige medewerkers 20
4.2.10 De toekomst/strategie 20
4.3 Visie op interne beheersing 20
4.3.1 4-lines of defense 20
4.3.2 PDCA cyclus 22
5 Van beleid naar praktijk 23
5.1 Plan- & beleidvorming 23
5.2 Werken onder architectuur 23
5.3 IB&P Jaarplan & -programma 23
5.4 Communicatie van dit beleid 24
6 Bijlagen 25
6.1 Bijlage A: Afkortingenlijst 25

Tabellen & figuren

Figuur 1: Context en positionering van strategisch IB&P beleid 6
Figuur 2: Volwassenheidsniveaus zoals gehanteerd bij jaarverantwoording IB&P.....14

1 Inleiding

1.1 Algemeen & leeswijzer

Dit document betreft het strategische informatiebeveiliging en privacy (hierna: IB&P) beleid van gemeente Helmond voor de periode 2025-2029 en bestaat uit de volgende onderdelen:

- Hoofdstukken 1 en 2 beschrijven het 'waarom' element van het beleid. Ze verklaren en onderbouwen de strategische beleidskeuzes.
    - Deze inleiding beschrijft de scope en de positionering van het beleid en definieert de begrippen informatiebeveiliging en privacy.
    - Hoofdstuk 2 beschrijft de context en de grondslagen voor het bepalen van het strategische beleid.
- Hoofdstukken 3 en 4 bevatten de kern van het strategisch IB&P beleid en beschrijven het 'hoe'-element.
    - Hoofdstuk 3 beschrijft de visie, strategie, speerpunten & doelstellingen en randvoorwaarden, uitgangspunten en principes.
    - Hoofdstuk 4 beschrijft de IB&P organisatie waaronder taken, verantwoordelijkheden & bevoegdheden om de strategische doelstellingen te realiseren en beleidsontwikkeling & -implementatie vorm te geven.
- Hoofdstuk 5 geeft aanzet tot het 'wat' element. Het beleid moet op onderliggend tactisch en operationeel niveau worden uitgewerkt en geconcretiseerd in aanvullende onderwerp specifieke plan- en beleidskaders. Dit betreft de acties en detailplanningen die nodig zijn om de doelstellingen te realiseren.

1.2 Positionering van het strategisch IB&P beleid

In dit strategische IB&P beleid worden de strategische richting, doelstellingen en prioriteiten op het gebied van informatiebeveiliging en privacy voor de periode 2025-2029 uitgewerkt. Dit beleid ondersteunt daarmee het bestuur, management en de organisatie in het algemeen bij de besturing, coördinatie, besluitvorming, middelverstrekking, het beheer, de uitvoering, en inbedding van IB&P.

1.3 Scope van het strategisch IB&P beleid

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente 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.

Het strategisch IB&P 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 wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld voor SUWI, gemeentelijke basisregistraties en DigiD). 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 IB&P beleid gelegd.

1.4 Definities informatiebeveiliging en privacy

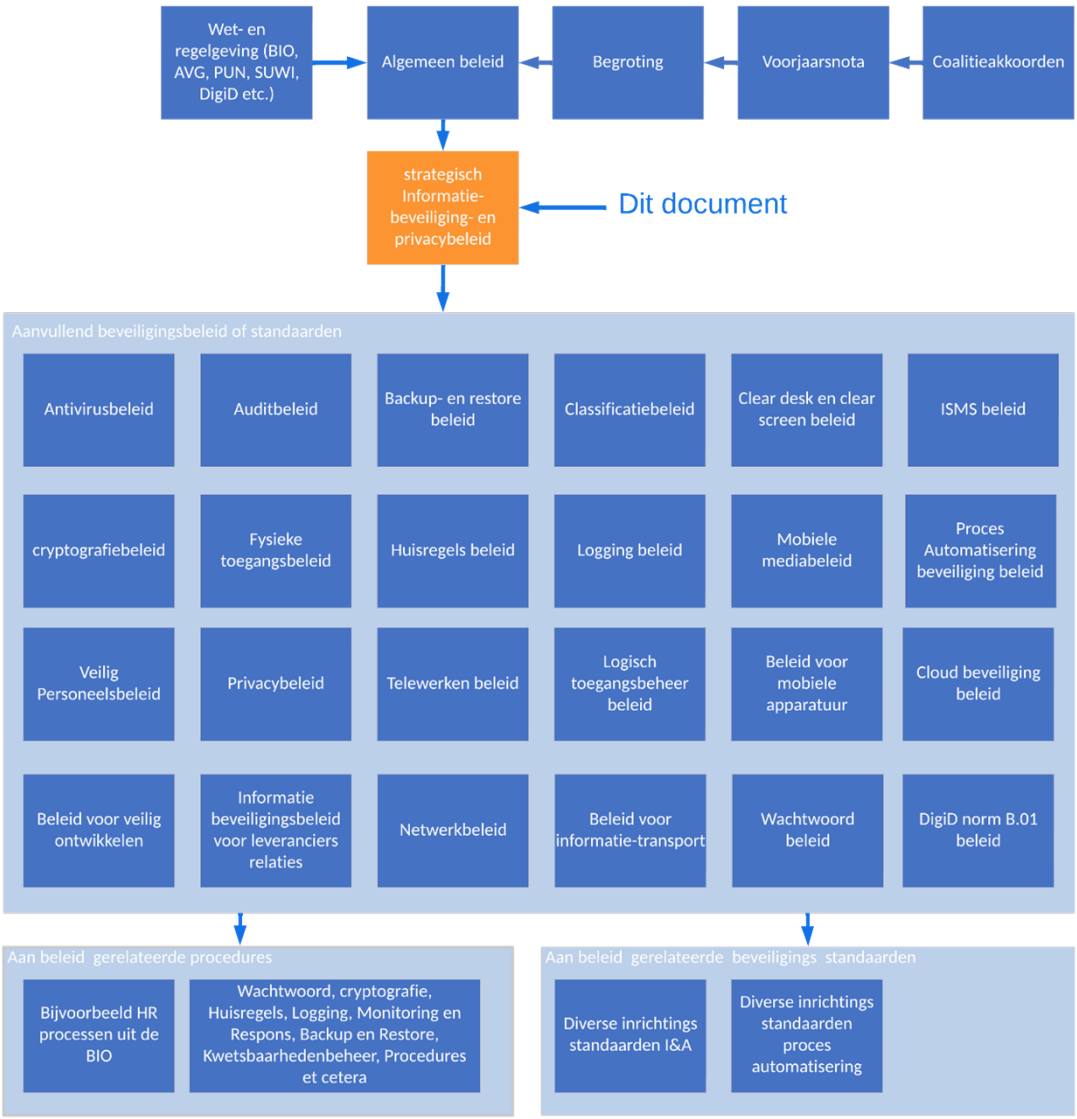
Informatiebeveiliging
Onder *informatiebeveiliging* wordt verstaan het risico gestuurd treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie en (digitaal) weerbaar zijn tegen interne en externe dreigingen en verstoringen.

Privacy
Met *privacy* wordt gedoeld op het zorgvuldig omgaan met persoonsgegevens[1] door de gemeente. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoners, medewerkers en andere betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met hun persoonsgegevens omgaat. Uitgangspunt is dat de organisatie kan aantonen dat zij zich houdt aan de basisprincipes. Dit zijn: Rechtmatig, behoorlijk en transparant, Doelbinding, Gegevensminimalisatie, Juistheid, Opslagbeperking en Passend beveiligd.

[1] Waar in dit beleid wordt gesproken over een persoonsgegeven, wordt ook een politiegegeven bedoeld. Een politiegegeven is namelijk een specifieke versie van een persoonsgegeven.

2 Context en grondslagen

Het strategisch IB&P beleid maakt onderdeel uit van een breder raamwerk voor het bestuur, management, beheer en uitvoering van IB&P. Dit zorgt voor de verbinding naar de bredere gemeentelijke strategie, beleidskaders & processen. Zie, voor een niet uitputtend overzicht, onderstaande figuur, die is overgenomen uit de door de informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten opgestelde handreiking voor strategisch IB&P beleid:



Figuur 1: Context en positionering van strategisch IB&P beleid

2.1 Aansluiting bij algemeen gemeentelijk beleid

2.1.1 Ambitie gemeente Helmond

Dit beleid moet aansluiten bij de gemeentelijke, visie, ambities, doelen en kernwaarden zodat deze herkenbaar zijn voor het bestuur en alle medewerkers. Ook zullen hierdoor strategische IB&P doelstellingen correct de gemeentelijke doelstellingen ondersteunen en faciliteren. In het ambitieakkoord, de visie Helmond 'Ambitie 2040' en de voorjaarsnota 2025 worden ambities beschreven en uitgewerkt die richtinggevend zijn voor IB&P, maar ook waar IB&P randvoorwaardelijk is voor het succesvol realiseren van de doelstellingen.

Helmond, stad van makers!
Helmond is een echte makersstad. De makersmentaliteit uit Helmonds industriële verleden maakt dat we barsten van de doeners. En dat is mooi, want hiermee verwerft Helmond een unieke én complementaire positie in de regio. We koppelen onze makersmentaliteit via innovatie, vakkundigheid en samenwerking aan een kwalitatieve transformatie. Dat werkt door in onze strategische positionering en in de keuzes die we maken. Bijvoorbeeld op het vlak van onderwijs, bedrijvigheid en cultuur en recreatie.

We leven in een tijd van grote opgaven en transities. Denk aan de woningkrapte, de mobiliteitstransitie, de energietransitie en de digitale transformatie die plaatsvindt. Ook in Helmond en in de regio zijn dit belangrijke ontwikkelingen, met zowel uitdagingen als kansen. Daarnaast is er onzekerheid door de geopolitieke spanningen. De maatschappij verandert snel en dat vraagt veel van inwoners, ondernemers, organisaties en de gemeente. Hierbij moet de gemeente scherpe keuzes maken. De kunst is daarbij om continu te schakelen tussen wat vandaag nodig is voor Helmonders en wat nodig is om Helmond toekomstbestendig te laten zijn. Brede welvaart geldt als leidend principe, als de basis voor een inclusieve, leefbare en gezonde stad.

De strategische koers is verder uitgewerkt in de voorjaarsnota 2025.Onderstaande ambities zijn daarbij vooral vanuit het perspectief van IB&P van belang (en dit is dus niet een uitputtend overzicht). De gemeente ambieert onder andere:

- Het verbeteren van haar betrouwbaarheid en haar dienstverlening, door in te zetten op verbeteren van processen en systemen zodat we efficiënter kunnen werken en beter kunnen sturen;
- Het voorzien van en vooroplopen in energie- en mobiliteitstransitie, de digitale transformatie, technologische innovaties en slimme toepassingen;
- Het voorzien van samenwerking bij grote opgaven, het betrekken van bewoners en andere organisaties en verzorgen dat iedereen kan meekomen in de toenemende digitalisering van de samenleving;
- Het verzorgen van een gemeentelijke organisatie die de ambities kan dragen, dus die zodanig kan meebewegen en meegroeit met de uitdagingen en opgaven dat deze doelmatig beheerst kunnen blijven, ambities gerealiseerd worden en de gemeente haar kerntaken uit kan blijven voeren en aan de wet kan blijven voldoen;
- De uitrol van het werken onder architectuur in de hele organisatie, zodat we wendbaar zijn en snel kunnen inspelen op innovatievraagstukken.

Daarbij benadrukt gemeente Helmond dat bij het maken van de (soms lastige) keuzes IB&P onderdeel zijn van het afwegingskader. En dat we transparant zijn over de gemaakte belangenafweging tussen de diverse publieke waarden, zoals het recht op privacy en het waarborgen van informatieveiligheid.

2.1.2 Beleidskaders

Het strategische IB&P beleid moet aansluiten op de beleidskaders vanuit de bredere gemeentelijke context. Het strategische IB&P beleid heeft niet alleen een raakvlak met de overkoepelende gemeentelijke strategie. Het heeft vooral ook een verbinding met de visie en strategie op digitalisering.

De visie op digitalisering stelt dat Helmond een digitaal weerbare stad is waarin alle vitale infrastructuur en slimme apparaten, die voor haar publieke taken worden ingezet, goed zijn beveiligd. Inwoners en ondernemers, maar ook verbonden partijen en medewerkers van de gemeente, kunnen erop vertrouwen dat de gemeente hun privacy beschermt door zorgvuldig en veilig met (persoons)gegevens om te gaan. Inwoners en ondernemers mogen verder verwachten van de gemeente dat zij betrouwbare en goed beveiligde computersystemen heeft zodat de dienstverlening aan hen niet wordt verstoord of stilvalt. Zij mogen er ook vanuit gaan dat de gemeente alle gegevens zo veilig mogelijk bewaart en beschermt tegen bijvoorbeeld datalekken en hacks, zodat zij niet door toedoen van de gemeente geraakt worden door mogelijke negatieve gevolgen zoals identiteitsdiefstal of oplichting.

IB&P vervult een belangrijke ondersteunende rol bij het kunnen realiseren van deze bredere digitaliserings- en de overkoepelende beleidsdoelstellingen.

2.1.3 Stakeholders

Er zijn veel belanghebbenden die met het strategische IB&P beleid geraakt worden. Afdelingen moeten het strategische IB&P beleid implementeren en doen een beroep op de uitvoerbaarheid. Beleidsmedewerkers en architecten bewaken en doen een beroep op de integraliteit met overige beleidskaders en technologische oplossingen door de gehele organisatie. IT-beheer doet een beroep op de technologische beheersmaatregelen en de implementatie op de IT architectuur. Leveranciers en partners moeten zich aan het beleid en de procedures houden en doen ook een beroep op uitvoerbaarheid en gepastheid. Vanuit het beheer op IB&P, waaronder vanuit de strategische afstemming, moet dit beleid rekening houden met deze stakeholders.

2.2 Ontwikkelingen

Ontwikkelingen en dreigingen op het gebied van IB&P gaan snel. Wet -en regelgeving probeert daar een goed antwoord op te geven. Dit vraagt om een permanente alertheid op onze weerbaarheid. Met dit beleid anticiperen we op (toekomstige) wet- en regelgeving en andere ontwikkelingen. Van belang voor het strategisch IB&P beleid is onder andere het volgende:

2.2.1 De BIO2

De BIO2 is het vernieuwde normenkader voor de overheid en richt zich op risicomanagement. Proceseigenaren (afdelings- en teammanagers) moeten werken volgens de aanpak van ISO 27001 en continu afwegingen maken over risico’s en de beveiliging van informatie.

2.2.2 NIS2 en Cyberbeveiligingswet

NIS2 is een Europese richtlijn die als doel heeft om cybersecurity binnen de EU te verhogen. De Nederlandse uitwerking van NIS2 is de Cyberbeveiligingswet. Gemeenten zijn aangewezen als essentiële entiteiten en moeten voldoen aan strengere beveiligingsnormen en meldingsvereisten. De Cyberbeveiligingswet treedt, op basis van de laatst bekende planning, niet eerder dan het derde kwartaal van 2026 in werking.

2.2.3 De Cybersecurity Implementatie Richtlijn (CSIR)

Onze organisatie gebruikt de BIO als beveiligingsnorm voor de beveiliging van onze kantoorautomatisering. Voor het beveiligingen van industriële automatisering en/of procesautomatiseringssystemen bestaan aanvullende beveiligingseisen die niet in de BIO staan. Voor de bescherming van proces automatisering is met name de Cybersecurity Implementatie Richtlijn (CSIR) van toepassing. Deze richtlijn is speciaal ontwikkeld om objecten (waterzuiveringsinstallaties, gemalen, bruggen, keringen, sluizen, etc.) te beveiligen.

2.2.4 De Algemene verordening gegevensbescherming (AVG)

Nieuwe technologische ontwikkelingen en een steeds digitaler wordende overheid maken het omgaan met persoonsgegevens complexer en noodzakelijker. De gemeente wil aangeven hoe zij invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy. Dit vergt continu aandacht.

2.2.5 De Wet politiegegevens (Wpg)

De gemeente heeft BOA's in dienst die gegevens verwerken die onder de Wpg vallen. Hiervoor moet de gemeente beleid en procedures hebben voor toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

2.2.6 Toename van complexe en onvoorspelbare dreigingen

Door geopolitieke spanningen, verschuivende internationale machtsverhoudingen en technologische innovaties (zoals artificiële intelligentie ("AI") en de komst van quantum computers) worden organisaties steeds kwetsbaarder. Weerbaarheid tegen de risico's die hier uit voortkomen omvat niet meer alleen een aanpak gericht op het voorkomen van schade. Het omvat ook het vermogen om onverwachte, positieve mogelijkheden te benutten om de veiligheid te verbeteren en te kunnen reageren op, te herstellen van én zich aan te passen aan ongunstige gebeurtenissen of activiteiten.

2.2.7 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Aanvullend op de vorige geschetste ontwikkeling, geeft het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst en helpt bij het actualiseren van beleid en plannen. Recentelijk is het geactualiseerd Dreigingsbeeld 2025-2026 uitgebracht.

2.2.8 Structuur en samenstelling organisatie

Juli 2024 is een belangrijke wijziging van de structuur van de organisatie gerealiseerd. De IB&P-organisatie is daarbij ook aangepast: het team van security en privacy officers (SPO-team) is toegevoegd aan het regie team van de afdeling Informatievoorziening en Automatisering. De FG en CISO rapporteren rechtstreeks aan de gemeentesecretaris en zijn geplaatst bij de Unit Concern Control. Bij de organisatiewijziging is verder het afdelingsmanagement (proceseigenaren) voor een behoorlijk gedeelte vernieuwd. Ook vond in 2024 een burgemeesterswissel plaats en in mei 2025 is de nieuwe gemeentesecretaris gestart. Tenslotte is recentelijk de definitieve invulling en rolverdeling binnen de directie gerealiseerd. Allemaal kansen om de komende jaren door te pakken op IB&P en belangrijk voor de governance daarop.

2.2.9 AI Verordening

AI, in welke vorm dan ook ontwikkelt zich snel. Deze snelle ontwikkeling heeft invloed op de beveiliging van onze data en de privacy van onze inwoners. De AI-verordening biedt (onder meer) aanbieders en gebruiksverantwoordelijken duidelijke eisen en verplichtingen met betrekking tot de toepassing van AI in hun producten en systemen.

2.2.10 Digitale agenda Gemeenten 2028

De Digitale Agenda Gemeenten 2028 laat zien hoe het collectief van gemeenten de komende jaren de kansen benut die digitalisering biedt, voor grote maatschappelijke opgaven, het verdienvermogen van Nederland en om de dienstverlening nog beter aan te laten sluiten bij de eisen en verwachtingen van de samenleving. Gemeenten doen dit o.a. door te zorgen dat digitalisering past binnen onze normen, democratie en rechtsstaat. Gemeenten beschermen de grondrechten van onze inwoners en onze publieke waarden zoals transparantie, veiligheid en privacy en bestrijden discriminatie. Daarnaast moet dienstverlening aansluiten bij de behoeften van inwoners en bedrijven. Deze moet laagdrempelig, veilig en betrouwbaar zijn. Ten derde, zetten gemeenten digitalisering in voor maatschappelijke vraagstukken zoals bestaanszekerheid, wonen of klimaat en energie. Met de juiste data op het juiste moment kunnen we samen met andere gemeenten grote stappen zetten.

2.2.11 Nederlandse Digitaliseringsstrategie

Recent (medio 2025) is de Nederlandse Digitaliseringsstrategie (NDS) gepresenteerd. Met de NDS prioriteren Rijksoverheid, provincies, gemeenten, waterschappen en publieke dienstverleners de onderwerpen waar de urgentie en impact het grootst is.
Afgesproken is dat de Rijksoverheid, provincies, gemeenten, waterschappen en publieke dienstverleners als 1 overheid gaan werken aan 6 met elkaar samenhangende prioriteiten om daarop te versnellen. De volgorde van de 6 prioriteiten van de Nederlandse Digitaliseringsstrategie (NDS) staat los van het belang of gewicht dat eraan wordt toegekend. Een NDS uitvoeringsprogramma was bij het afronden dit strategisch IB&P beleid nog niet beschikbaar, maar dit zal de komende jaren zeker zijn invloed hebben.
De 6 prioriteiten zijn:

1. Cloud;
2. Data;
3. Artificiële Intelligentie;
4. De overheid stelt burgers en ondernemers centraal in (digitale) dienstverlening;
5. Versterken digitale weerbaarheid en autonomie van de overheid;
6. Digitaal vakmanschap en een moderne werkomgeving.

3 Strategisch beleid informatiebeveiliging & privacy

Dit hoofdstuk beschrijft op hoofdlijnen de visie en strategie van de gemeente omtrent IB&P en de speerpunten die prioriteit hebben en extra aandacht verdienen de komende jaren.

3.1 Visie

Gemeente Helmond is een betrouwbare dienstverlener voor haar inwoners, medewerkers, ondernemers, partners en andere betrokkenen. Wij zorgen ervoor dat er zorgvuldig met hun (persoons)gegevens wordt omgegaan en dat deze adequaat worden beveiligd. Wij kunnen laten zien wat er met hun gegevens gebeurt en kunnen aantonen dat de beveiliging gewaarborgd wordt en dat we daarbij voldoen aan de basisprincipes van de AVG.
Informatiebeveiliging zien wij vooral ook als het vermogen om onverwachte, positieve mogelijkheden te benutten als kansen om de kwaliteit van onze dienstverlening en bedrijfsvoering te waarborgen en verbeteren. Dus als een cruciaal aspect voor een digitaal weerbare, wendbare en toekomstbestendige organisatie.
Wij dragen vanuit de aspecten IB&P bij aan continuïteit. Als betrouwbare dienstverlener kunnen wij kerntaken uit blijven voeren, omdat we op het juiste moment beschikken over de juiste gegevens. Als betrouwbare bedrijfsvoerder waarborgen wij de uitvoering van primaire bedrijfsprocessen en informatievoorziening, zodat de kwaliteit van de dienstverlening op niveau blijft.

3.2 Strategie

De strategie zorgt voor het worden, zijn en blijven van de betrouwbare dienstverlenende organisatie zoals beschreven in de visie.

Daarvoor is het volgende nodig:

1. Het op orde krijgen van alle basis randvoorwaarden voor IB&P en het borgen daarvan. De randvoorwaarden komen terug in paragraaf 4.4;
2. Het bewegen van reactief beleid en onbewust risico lopen naar proactief beleid, en bewust & beheerst risico nemen. Waarbij we ook oog hebben voor de risico's van onze inwoners (en andere betrokkenen);
3. Het zodanig borgen van IB&P in de bedrijfsprocessen dat de juiste verantwoordelijkheden en het beheer van risico's belegd zijn bij de correcte rollen en deze personen in staat zijn hun verantwoordelijkheid te nemen en bewuste keuzes te kunnen maken;
4. Het verzorgen van een basis voor het kunnen groeien in volwassenheid op het gebied van IB&P en het blijven leren en continu verbeteren van de processen;
5. Het kunnen beoordelen van getroffen beheersmaatregelen en IB&P inspanningen op kosteneffectiviteit en deze bij te stellen op basis van beoordeling en herijking, alsmede de investering hierop beter te kunnen verantwoorden;
6. Het aantoonbaar blijven voldoen aan de verplichtingen uit wet- en regelgeving;
7. Grip houden op het implementeren van maatregelen door een risico- en governance gestuurde aanpak waardoor al onze privacy en beveiligingsinspanningen worden bestuurd;
8. Het verhogen en aanvullen van het bewustzijn en de cultuur rondom IB&P met oog op de rol en impact van de verschillende stakeholders;
9. Het verkrijgen en houden van overzicht van al onze middelen zoals onze processen, de informatie die in deze processen wordt verwerkt en onze applicaties.

3.3 Strategische speerpunten & doelstellingen

Om de strategie vorm te geven en de visie te ondersteunen, moeten prioriteiten worden gesteld. De speerpunten betreffen de meest belangrijke onderwerpen die aandacht nodig hebben en vormen daarmee de kern van de IB&P strategie.

3.3.1 Bewustwording

Een fundamenteel onderdeel van de digitaal weerbare gemeentelijke organisatie is bewustwording omtrent IB&P. De 3 belangrijke aspecten hiervan zijn *kennis, houding* en *gedrag*. Training, bewustwordingscampagnes en zorgen voor een veilige cultuur waarin het doen van meldingen aangemoedigd wordt, dragen bij aan het verlagen van het aantal incidenten door menselijk gedrag. In het op 18 maart 2024 vastgestelde bewustwordingsplan 2024-2027[2] is dit speerpunt verder uitgewerkt. Op basis van dat bewustwordingsplan en een jaarlijkse meting wordt de jaarlijkse planning van bewustwordingsactiviteiten vastgesteld.

3.3.2 Risicomanagement

Risicobeheer is de kern van IB&P en sluit aan bij onze architectuurprincipes. We zorgen ervoor dat van al onze processen, diensten en producten en informatiesystemen de risico's bekend zijn. We zoeken goede oplossingen en treffen beheersmaatregelen, zodat privacy problemen zich niet of nauwelijks voordoen. De restrisico's voor betrokkenen én onze organisatie zijn laag.

Het is daarom belangrijk voor gemeente Helmond om een robuust risicomanagement proces op te zetten voor IB&P. Dit proces biedt een gestructureerde aanpak om risico's te identificeren, beoordelen, beheersen en monitoren. De risicobeheersingsmaatregelen kunnen opgenomen worden in een framework vanuit waar deze maatregelen ontworpen, geïmplementeerd, beheerd en onderhouden kunnen worden.

Het IB&P risicomanagement moet kunnen aansluiten op het gemeente brede integraal risicomanagement proces dat op dit moment vanuit de Unit Concern Control wordt geactualiseerd. Het resultaat daarvan is een vastgestelde herijkte kadernota risicomanagement, geïmplementeerd en geborgd in de organisatie. Voor 2026 is het updaten van het daaraan gerelateerde tactisch kader risicomanagement IB&P een belangrijke te realiseren doelstelling.

3.3.3 IB&P beleidskader

Het IB&P beleidskader is het geheel van het ontwikkelen, implementeren, beoordelen, evalueren en bijstellen van beleid en onderliggende kaders op het gebied van IB&P. Figuur 1 geeft dit illustratief weer. De beleidskaderstructuur betreft de lijn die de formele beleidsontwikkeling doorloopt vanaf de strategie tot de operationele uitwerking en uitvoering. Kadervorming vindt op strategisch, tactisch en operationeel niveau plaats. Onderdeel van de strategie is het actualiseren en aanvullen van het huidige beleidskader op noodzakelijke onderwerpen en het opstellen van bruikbare onderliggende operationele kaders, met ook oog op wat de *ander* nodig heeft.

Onderdeel van het beleidskader is de continue evaluatie en bijstelling van beleid & onderliggende kaders, op basis van processen zoals de uitkomsten van het risico management proces, de uitvoering/implementatie van beheersmaatregelen, veranderingen in wet- &

[2] Besluit in Management Team-Directie Team overleg, zie document 52017421 in de zaak met nummer 51908275

regelgeving, uitkomsten van het incident management proces en de afstemming met de bredere business. Een formeel beleidskader is vereist vanuit de BIO2, de AVG en de Wpg en verzorgt consistente en uniforme uitvoering van risicobeheersmaatregelen.

In 2025 wordt nieuw privacybeleid uitgewerkt en vanaf 2026 wordt een jaarlijkse planning voor nieuw op te stellen en/of te actualiseren tactische en operationele IB&P beleidsdocumenten gemaakt.

3.3.4 IB&P programma (mede) op basis van thema architectuur

Het IB&P programma realiseert de doelen en doelstellingen zoals bepaald in de IB&P strategie en verder is uitgewerkt in een roadmap vanuit de thema architectuur voor IB&P. Het programma zet projecten neer zodat de doelstellingen één op één of in samenwerking met elkaar worden bereikt. Dit betreft de implementatie van specifiek beleid en beheersmaatregelen, maar ook de implementatie van benodigde onderdelen voor de IB&P bedrijfsfuncties die volgen uit de IB&P thema architectuur. De prestatie van het programma moet in een cyclus gemeten en bijgesteld worden. Hierdoor is duidelijk wat de status is van de projecten en daarmee de implementatie van het beleid. Op basis van de voortgang van de uitvoering van beleid binnen de projecten kan de strategie en het onderliggende beleid worden bijgesteld. Het programma moet voorzien worden van een methode om voortgang te monitoren, evalueren en bij te sturen.
Voor thema architectuur voor IB&P is het de doelstelling deze gereed te hebben in 2026.

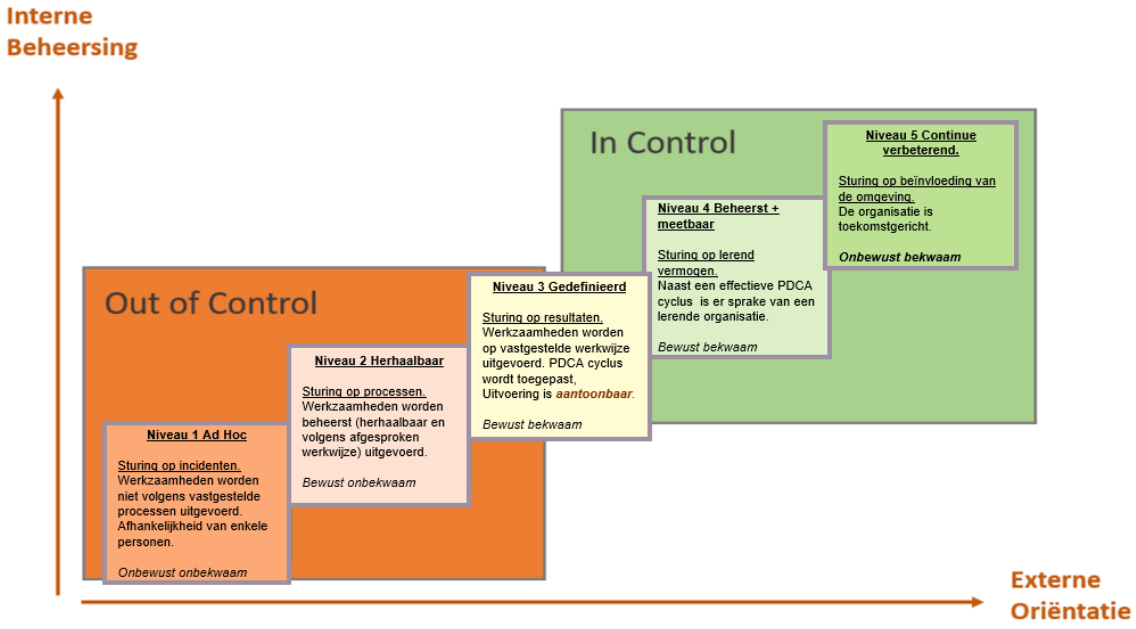
3.3.5 ISMS gebaseerde aanpak

Een ISMS (information security management systeem) gebaseerde aanpak verzorgt de gestructureerde en systematische methode voor het management, bestuur en beheer van informatiebeveiliging en privacy. Het ISMS bevat een aanpak voor het beheer van IB&P risico's en omvat een raamwerk van beleid, procedures, richtlijnen en middelen gebruikt om IB&P te beheren en verbeteren. De methode dwingt het toepassen van een PDCA-cyclus af, welke Helmond in staat stelt de beveiligingsinspanningen te plannen, organiseren en af te stemmen, uit te voeren, de resultaten te toetsen en implementatie van maatregelen te monitoren, en corrigerende maatregelen te treffen op basis van de evaluatie en behaalde resultaten.

De BIO2 beschrijft de onderdelen van een formeel ISMS. Het stelt de organisatie ook in staat om op termijn een GRC (Governance, Risk, Compliance) aanpak te hanteren voor IB&P. Een GRC aanpak betreft een geïntegreerde benadering om de beveiliging van informatie, informatiesystemen en -diensten integraal te beheren en verbeteren. *Governance* verwijst naar de structuren, beleidslijnen, het beleggen van verantwoordelijkheden en strategische aansturing van IB&P inspanningen. *Risk* verwijst naar het risico management proces vanuit waar risico wordt geïdentificeerd, beoordeeld en beheerst door het opstellen van beheersmaatregelen. *Compliance* refereert naar het aantoonbaar naleven van de beheersmaatregelen uit beleid en wet- & regelgeving en naar het verifiëren van gewenste prestaties van de beheersmaatregelen en het monitoren van de effectiviteit daarvan. Door een integrale aanpak is de organisatie in staat de beveiligingsinspanningen effectief en efficiënt toe te passen en geborgd te groeien in volwassenheid.

Een digitaal weerbare organisatie heeft minimaal een volwassenheidsniveau 3 op een schaal van 5. Op dit niveau 3 worden werkzaamheden op het gebied van privacy en informatiebeveiliging op een vastgestelde werkwijze uitgevoerd. Er kan worden aangetoond dat er wordt gewerkt volgens afspraak. De organisatie kan aan inwoners en toezichthouder laten zien dat er zorgvuldig met hun (persoons)gegevens wordt omgegaan. De organisatie is

niet alleen in staat om zich te weren tegen cyberdreigingen, ze is ook in staat om snel te herstellen of aan te passen aan nieuwe omstandigheden. Een volwassenheidsniveau van 3 is nodig om te kunnen voldoen aan de ambities van de gemeente (zie paragraaf 2.1.1) en de visie (zie paragraaf 3.1).



Figuur 2: Volwassenheidsniveaus zoals gehanteerd bij jaarverantwoording IB&P

Doelstelling is om in 2025 te starten met de ISMS aanpak, gebaseerd op de BIO2. Daarnaast wordt een slimmere wijze van verantwoording op IB&P beheersmaatregelen in het tweede kwartaal van 2026 gerealiseerd. Doelstelling is verder om vanaf 2025 daadwerkelijk groei in volwassenheid te realiseren.

3.3.6 IB&P aspecten van incident management, crisis management & BCM.

Informatiebeveiliging en bescherming van privacy gaan over weerbaarheid. Vanuit de AVG worden eisen gesteld omtrent de afhandeling van privacy gerelateerde incidenten, welke op juist wijze en binnen bepaalde tijd afgewikkeld moeten worden. De nieuwe Cyberbeveiligingswet stelt vergelijkbare eisen voor ‘significante’ informatiebeveiligingsincidenten. Dit zijn beveiligingsincidenten die de verlening van de diensten van de organisatie aanzienlijk verstoren of kunnen verstoren en kunnen leiden tot ernstige materiële of immateriële schade bij de organisatie of derden.

Bij een incident wordt de dienstverlening hersteld vanuit een keten van beheersmaatregelen die preventie, detectie, response, herstel en lering verzorgen. De oplossing voor IB&P gerelateerd incident management, crisis management en continuïteitsmanagement moet passen in de gemeente brede processen voor incident management, crisis management, disaster recovery en bedrijfscontinuïteitsmanagement (BCM).

De doelstelling is om effectieve en efficiënte incident response op te zetten die ervoor zorgt dat incidenten worden beheerst en continuïteit wordt gewaarborgd binnen vooraf gedefinieerde en afgesproken parameters. Deze parameters komen tot stand aan de hand van de risicobereidheid van de organisatie en de specifieke context van de verschillende

gemeentelijke processen. Door snelle en adequate reactie op incidenten wordt schade beperkt en kunnen diensten blijven functioneren tijdens en na een verstoring.

3.3.7 Doorontwikkeling IB&P organisatie[3]

Om de strategische IB&P doelen te bereiken en IB&P effectief en efficiënt uit te voeren is een passende en adequate IB&P organisatie nodig. Deze organisatie moet met de context van de gemeente mee groeien en in staat blijven de benodigde privacy- en beveiligingsinspanningen te kunnen blijven leveren. De strategie voor de IB&P organisatie staat in het teken van het door ontwikkelen van de SPO rol naar business partner en regie positie, het door ontwikkelen van de rol van de FG en de CISO waarbij zij de (nu nog door hen opgepakte) uitvoerende taken overdragen aan het SPO team en de ontwikkelingen op het gebied van capaciteit voor IB&P in de lijn. De IB&P organisatie in het algemeen moet continu in staat zijn de juiste maatregelen en hun beheer te adviseren en deze te evalueren t.a.v. de risico's die de gemeente loopt.

3.4 Uitgangspunten en randvoorwaarden

De organisatie hanteert strategische uitgangspunten voor IB&P en de inbedding in de organisatie en haar beleid. Deze uitgangspunten zijn veelal randvoorwaardelijk voor het succes: er moet aan voldaan worden om IB&P goed uit te voeren en waarde voor de organisatie te laten hebben.

1 IB&P is in de kern een vorm van risicomanagement. Risico's kunnen alleen effectief gemanaged worden wanneer de risico verantwoordelijke dit actief en bewust doet. Risico's kunnen nooit volledig geminimaliseerd worden en moeten altijd beheerst worden binnen voor de organisatie acceptabele parameters. Voor de privacyrisico's van een gegevensverwerking geldt dat ze zodanig beheerst worden dat de restrisico's voor betrokkenen acceptabel zijn;
2 IB&P moet bestuurd en gemanaged worden. De governance van IB&P weegt zwaar mee in het succes van goede informatiebeveiliging en privacybescherming;
3 Moderne beveiliging van informatie en bescherming van privacy is geënt op een keten van samenwerkende risicobeheermaatregelen waarbij preventie, detectie, respons, herstel en lering ieder een plaats hebben;
4 IB&P is van iedereen. Iedereen heeft een verantwoordelijkheid t.a.v. beveiliging en bescherming in meer of mindere mate. Elke medewerker handelt naar deze verantwoordelijkheid en mag vanuit de IB&P organisatie training in bewustwording verwachten;
5 Het (strategische) IB&P beleid wordt door het bestuur en management uitgedragen en gehandhaafd;
6 Beveiliging en privacy zijn een continu proces. De strategische keuzes en doelen, alsmede de tactische en operationele kaders die hieruit volgen worden periodiek bijgesteld op basis van nieuwe ontwikkelingen en de uitkomsten van de voornaamste IB&P processen waaronder risico management, incident management en beleidsimplementatie en -uitvoering (a.d.h.v. de status en voortgang van het IB&P programma). De "Plan, Do, Check, Act" cyclus vormt de kern van het managen van IB&P en maakt integraal onderdeel uit van het management systeem (ISMS). Onderdeel hiervan is het continu verbeteren van de IB&P processen en leren vanuit systematisch en gestructureerd werken;
7 Om IB&P goed te kunnen organiseren en de strategische doelstellingen te realiseren is investering in mensen en middelen nodig. Kennis en competenties op de kerngebieden

[3] zie paragraaf 4.2.4

moeten ontwikkeld worden en geborgd worden. IB&P risico's en beheersmaatregelen ontwikkelen zich continu en snel;

8 Informatiebeveiliging en privacy behoeft ook aandacht in (keten)samenwerking;

9 De gemeente is open en transparant in de verantwoording rondom de naleving van privacy wet- en regelgeving, beveiligingsinspanningen, behaalde resultaten, keuzes, en de investeringen hierin. Hierover rapporteren wij helder en traceerbaar;

10 Als uitgangspunt voldoet de gemeente aantoonbaar aan wet- en regelgeving;

11 Daar waar regelgeving de ruimte biedt om af te wijken (bijvoorbeeld bij het beleid om open standaarden te gebruiken), legt de gemeente dat onderbouwd uit ('pas toe of leg uit'). De onderbouwing bevat ten minste risico's, risico acceptatie en eventuele risicobeheersmaatregelen en is voorzien van een mechanisme voor monitoring van en het opnieuw beoordelen van de risico's na verloop van tijd.

4 Organisatie, taken & verantwoordelijkheden van IB&P

Dit hoofdstuk beschrijft op hoofdlijnen de taken en verantwoordlijkheden op het gebied van IB&P.

4.1 Bestuur

4.1.1 Gemeenteraad

De gemeenteraad heeft een toezichthoudende rol en controlerende taak richting het college van B&W. De gemeenteraad is verder verantwoordelijk voor de bescherming van de persoonsgegevens die door de gemeenteraad zelf worden verwerkt.

4.1.2 College van Burgemeester en Wethouders

Het college van B&W is verantwoordelijk voor een goede informatievoorziening, als voorwaarde voor de dienstverlening en de bedrijfsvoering en stelt het strategisch beleid voor IB&P vast. Daarnaast is het college verantwoordelijk voor de bescherming van de persoonsgegevens die door de gemeente worden verwerkt. Het college wijst daarom ook een functionaris voor gegevensbescherming aan en legt in een reglement vast op welke wijze uitvoering wordt gegeven aan de positie en de taken van de FG.

Het college legt verantwoording af aan de gemeenteraad en externe toezichthouders. Daarnaast is het college verantwoordelijk voor de allocatie van bedrijfsmiddelen, waaronder financiën, voor het realiseren van de vastgestelde strategische doelstellingen. Het college mandateert de ambtelijke verantwoordelijkheid op het gebied van IB&P aan de gemeentesecretaris.

Informatiebeveiliging en privacy valt onder de bestuurlijke verantwoordelijkheid van een van de leden van het college van B&W. Het bij het schrijven van dit beleid zittende college heeft dit belegd bij de wethouder met de portefeuille digitalisering.

4.1.3 De burgemeester

De burgemeester is verwerkingsverantwoordelijke voor de verwerking van de persoons- en of politiegegevens die onder zijn uitdrukkelijke bevoegdheid worden verwerkt. Dit geldt bijvoorbeeld voor gegevens die betrekking hebben op zijn openbare orde bevoegdheid. Hij is bovendien verantwoordelijk voor de verstrekking en beveiliging van reisdocumenten en rijbewijzen.

4.2 Ambtelijke organisatie

De ambtelijke organisatie is verantwoordelijk voor de uitvoering van het strategische IB&P beleid en vertaalt dit naar tactische/operationele kaders en doelen.

4.2.1 De gemeentesecretaris

Draagt de gemandateerde verantwoordelijkheid voor de inbedding van IB&P in de gemeente en het voldoen aan de relevante wet- en regelgeving. De gemeentesecretaris is verantwoordelijk voor de uitvoering van de strategie en verzorgt dat beleidslijnen en procedures worden geïmplementeerd en nageleefd binnen de gehele ambtelijke organisatie. De gemeentesecretaris rapporteert aan het college van B&W omtrent de voortgang en naleving van het beleid en fungeert als schakel tussen de bestuurlijke en ambtelijke

organisatie, alsmede als schakel tussen ‘business’ en IB&P. De gemeentesecretaris laat zich adviseren door de CISO, FG en een Privacy officer omtrent besluitvoering IB&P. De gemeentesecretaris stelt de verdere uitwerking van de rollen en de “Plan, Do, Check, Act cyclus” vast.

4.2.2 Directieteam

Het Directieteam is collectief verantwoordelijk voor de ambtelijke organisatie en de realisatie van de strategische doelen. De directie is verantwoordelijk voor de beheersing van concernrisico’s, waaronder IB&P. Informatiebeveiliging en privacy behoren namelijk tot de concernrisico’s met een aanzienlijke financiële of maatschappelijke impact en een hoge mate van politiek bestuurlijke gevoeligheid.

4.2.3 Afdelingsmanagers

Afdelingsmanagers zijn verantwoordelijk voor de resultaten van de afdeling en de wijze waarop deze resultaten tot stand komen. Daarmee zijn zij ook verantwoordelijk voor risicobeheer van hun assets & processen en de implementatie & realisatie van informatiebeveiliging en privacy binnen deze eigen processen. De borging van Informatiebeveiliging en privacy omvat dan ook geen extra taken, maar is onderdeel van de reguliere processen. Wel verandert de digitalisering het werk en daarmee ook de activiteiten die nodig zijn om risico's te beheersen.

4.2.4 IB & P organisatie

De afdelingsmanager is ervoor verantwoordelijk dat de medewerkers van zijn afdeling vaardigheden ontwikkelen die zijn gericht op het meegroeien met de veranderde vraag. Daarnaast is specialistische kennis nodig. Aan de andere kant kunnen de specialisten niet zonder de inzet vanuit de afdelingen. Juist daar is namelijk de kennis aanwezig over processen, producten en applicaties. Deze ondersteuning komt samen in de IB&P organisatie. Deze paragraaf beschrijft in hoofdlijnen de rollen en taken van de IB&P organisatie. Een nadere uitwerking van dit beleid bevat een uitgebreidere beschrijving van rollen, taken en verantwoordelijkheden.

4.2.4.1 Decentrale security en privacy officer (DSPO)

Afdelingsmanagers zijn verantwoordelijk voor het inrichten en borgen van informatiebeveiliging en privacy voor de processen waar zij voor verantwoordelijk zijn. Om dit te realiseren stellen zij voldoende middelen beschikbaar voor het uitvoeren van IB en P werkzaamheden. Daarbij beleggen zij binnen de afdeling de decentrale security en privacy officer rol (DSPO), bij één of meerdere medewerkers. De DSPO is ambassadeur en het eerste aanspreekpunt voor IB en P onderwerpen die de processen van de afdeling raken. Zij werken samen met de Security en Privacy officer uit het centrale team bij de uitvoering en borging van IB en P werkzaamheden binnen de afdeling. Daarbij levert de DSPO kennis over processen, producten en applicaties binnen de afdeling. Randvoorwaardelijk is dat de invulling van de DSPO rol passend is bij de afdeling en IB en P wordt gezien als onderdeel is van de bedrijfsprocessen en het dagelijkse werk.

4.2.4.2 Security en privacy officer (SPO)

Daarnaast kent de organisatie een centraal gepositioneerd team van specialisten: de security en privacy officers. Dit centrale team onderscheidt zich door specialistische kennis en competenties rondom de verschillende beveiligings- en privacyaspecten. De SPO is als business partner een verbindende schakel tussen afdelingen en gemeentebrede disciplines, ze neemt

daarbij niet de verantwoordelijkheid van de eerste lijn over. De SPO ondersteunt daarbij proceseigenaren bij hun verantwoordelijkheid voor informatiebeveiliging en privacy (IB&P), afgestemd op wet- en regelgeving en hun jaarplan. En doet dit door de proceseigenaar bewust te maken over IB&P, advies te geven en mee te denken bij beslissingen over risico's, kansen en beheersmaatregelen.

4.2.5 Medewerkers

Informatiebeveiliging & privacy is van ons allemaal. Elke medewerker draagt een verantwoordelijkheid voor het naleven van het IB&P beleid, het volgen van procedures, het melden van incidenten en risico's, alsmede het deelnemen aan trainingen en bewustwordingsprogramma's.

4.2.6 Interne audit

De IT auditor is verantwoordelijk voor het opzetten en uitvoeren van audits op het gebied van de naleving van IB&P beleid. De auditor toetst op compliance risico's, rapporteert bevindingen en doet aanbevelingen, aan bestuur, directie en management. De auditor heeft een onafhankelijke rol en is bevoegd informatie op te vragen van verschillende functionarissen binnen de gemeentelijke organisatie. De auditor voert audits uit in opdracht van de concerncontroller, directie, management, Ciso, FG, externe toezichthouders en/of regelgevende instanties, interne afdelingen, de gemeenteraad en het college van B&W..
Uitgevoerde audits kunnen in het teken staan van:

- de toepassing van informatiebeveiliging in de organisatie;
- het meten van de effectiviteit van beleidsimplementatie;
- de naleving van intern en/of extern beleid, waaronder het IB&P beleid;
- De prestaties van beveiligingsmaatregelen t.a.v. het onderkende risico.

4.2.7 CISO

De CISO is strategisch adviseur van het bestuur, de directie en het management. En geeft gevraagd en ongevraagd advies, waar alleen met gegronde motivatie van kan worden afgeweken, waarbij de consequenties van afwijking op het juiste niveau worden aanvaard.

De CISO vertaalt wetgeving en bedrijfsdoelstellingen naar een informatiebeveiligingsbeleid en rapporteert aan het bestuur, de directie en het management hoe het lijnmanagement het informatiebeveiligingsbeleid implementeert en op welke wijze wordt voldaan aan de BIO en andere relevante wet- en regelgeving, om ervoor zorg te dragen dat de bestuurder geïnformeerde besluiten kan maken over de behandeling van informatiebeveiligingsrisico's. Bij afwijking van de BIO maatregelen wordt in alle gevallen eerst advies aan de CISO gevraagd.

De CISO ondersteunt vanuit een onafhankelijke positie de organisatie met betrekking tot het borgen van informatieveiligheid en heeft de mogelijkheid om rechtstreeks aan de gemeentesecretaris en/of portefeuillehouder te rapporteren. De CISO is direct onder de gemeentesecretaris geplaatst en organisatorisch ondergebracht bij de Unit concern control.

De CISO voert geen operationele taken uit en is uitdrukkelijk niet verantwoordelijk voor informatiebeveiliging door het lijnmanagement. Hiermee is het risico geminimaliseerd dat de eigenlijke taken van de CISO blijven liggen en de onafhankelijke positie in het geding komt. De gemeentesecretaris zorgt ervoor dat de rol en positie worden vastgelegd.

De CISO is vertrouwd contactpersoon voor het Computer Emergency Response Team van de Informatiebeveiligingsdienst (CERT-IBD).

4.2.8 Functionaris voor gegevensbescherming (FG)

De FG is de wettelijke toezichthouder op de interne naleving van wet- en regelgeving en eigen beleidsafspraken op het gebied van gegevensbescherming.

De positie en taken van de FG zijn in de AVG en Wpg verankerd. Om de autonomie en de onafhankelijkheid van de FG te waarborgen en misverstanden te voorkomen is aanvullend een reglement vastgesteld.

De FG ziet er op toe dat de organisatie de AVG en Wpg naleeft en adviseert op strategisch niveau over de verplichtingen. Het advies is een vorm van preventief toezicht en is zwaarwegend. Er kan alleen gemotiveerd van worden afgeweken.

De FG voert geen operationele taken uit. Dit betekent dat ze adviseert, maar zelf geen beleid opstelt of maatregelen treft. Hiermee wordt voorkomen dat haar onafhankelijke positie in het geding komt. Om deze reden ontvangt de FG geen opdrachten of instructies over het inhoudelijk functioneren.

4.2.9 Overige medewerkers

De organisatie kent meerdere functies en rollen wiens werkzaamheden impact hebben op de borging van privacy en informatiebeveiliging. Denk bijvoorbeeld aan de coördinator business continuïteit, functioneel-, applicatie- en technisch beheerders en de architectuurfuncties en -rollen, zoals de thema architect IB&P. Maar ook de werkzaamheden van bijvoorbeeld de medewerkers informatiebeheer, de gegevensmakelaar, procesadviseurs, de portfolio manager en de chief data officer zijn van invloed op het thema IB &P.

4.2.10 De toekomst/strategie

Een veerkrachtige toekomstbestendige organisatie vraagt wendbare gemeenteambtenaren. Gemeente ambtenaren die zich zodanig ontwikkelen dat zij bijblijven en effectief willen en kunnen omgaan met veranderingen in hun werk en in staat zijn om IB&P te betrekken bij hun werkzaamheden. Deze ontwikkeling heeft effect op de inzet van afdelingen. Kennis en kunde vanuit de afdeling hoeft namelijk niet per se geleverd te worden vanuit een decentrale security en privacy officer maar kan ook anders georganiseerd worden. Voorlopig blijft echter de inzet van DSPO's (met voldoende capaciteit) noodzakelijk, aangezien de organisatie nog niet zo ver is.

Daarnaast is een doorontwikkeling van het SPO team nodig waarbij zij ook beleidsmatige privacytaken op zich nemen. Dat wil zeggen dat binnen het SPO team ook 1 of meerdere medewerkers verantwoordelijk zijn voor het opstellen van strategisch beleid op het gebied van privacy en het opstellen van organisatie brede meerjarenplannen/verbeterplannen IB&P. Door deze zogenaamde SPO+ taken bij het SPO team te beleggen, is ook geborgd dat FG en Ciso geen, niet bij hun functie, passende taken uitvoeren.

4.3 Visie op interne beheersing

4.3.1 4-lines of defense

De organisatiestructuur en de belegde taken en verantwoordelijkheden sluiten aan bij de "Visie op control van de gemeente". Helmond volgt bij deze inrichting het model van de

zogenaamde “4-lines of defense”[4]. In dit model is het lijnmanagement primair verantwoordelijk voor een goede sturing en beheersing van de organisatie en het managen van de risico’s. Dit betekent dat zij verantwoordelijk zijn voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (SPO en DSPO) ondersteunt, adviseert en coördineert. De DSPO voert interne controles binnen de afdeling uit. Deze interne controles hebben als doel om onvolkomenheden in de procesbeheersing en de uitvoering tijdig op te sporen en te corrigeren en om de manager te ondersteunen bij het afleggen van verantwoording.

In de derde lijn wordt onafhankelijk van het lijnmanagement, een objectief oordeel gegeven over de uitvoering en voorzien van een advies over de mogelijkheden tot verbetering. De medewerkers in de derde lijn zijn niet betrokken bij de uitvoering.

De 4e line of defense is de controle door een externe partner, zoals de externe accountant, het Rijk, een toezichthouder of een andere geaccrediteerde instelling.

In de Visie op control is de FG aangewezen als 3e lijns functie. De FG is echter niet noodzakelijk een interne toezichthouder maar kan net zo goed een externe toezichthouder zijn, zo zegt de AVG. Om die reden is de FG geen zuivere 3e lijns taak, maar een taak die ook in de 4e lijn gepositioneerd zou kunnen worden. Daarbij is het relevant dat de onafhankelijkheid van de FG anders dan bij de (andere) 3e lijns functies, wettelijk is verankerd.

In onderstaand schema is het in de Visie op Control[5] vastgestelde schema (in kleur) aangevuld met de IB en P rollen.

4-lines of defense			
Directieteam			
1e lijn	2e lijn	3e lijn	4e lijn
• Afdelings- en teammanagers • Programma- en projectmanagers	• Kwaliteitsmedewerkers • Medewerkers AO/IC • Businesscontrollers • Concernadviseurs van bedrijfsvoering afdelingen • DSPO • SPO • CISO	• Unit Concern control • Interne auditoren • IT auditor • FG	• Externe accountant • Rijksoverheid/ Provincie • Geaccrediteerde instellingen • Autoriteit Persoonsgegevens
• Verantwoordelijk voor sturing en interne beheersing IB&P • Managen van risico’s die samenhangen met bedrijfsvoering, waaronderde IB&P risico’s	• Inrichten processen en beheersmaatregelen • Uitvoeren van interne controles (D)SPO • Adviseren ten aanzien van bedrijfsvoerings-risico’s waaronder IB&P risico’s • CISO: Onafhankelijk rapporteren over effectiviteit van IB&P en beheersmaatregelen	• Adviseren over doorontwikkeling interne beheersing • Toetsen van geïmplementeerde beheersmaatregelen	• Controle jaarrekening • Rapporteren over bevindingen en ontwikkelingen aan Raad • Toezicht houden

[4] *Dit model is vastgelegd in het door het college vastgestelde “Beleidsplan verbijzonderde interne controle 2019-2022”.*
[5] *Visie op control, DT d.d. 11 mei 2020*

De methode dwingt het toepassen van een PDCA-cyclus af, welke gemeente Helmond in staat stelt de beveiligingsinspanningen te plannen, organiseren en af te stemmen, uit te voeren, de resultaten te toetsen en implementatie van maatregelen te monitoren, en corrigerende maatregelen te treffen op basis van de evaluatie en behaalde resultaten.

4.3.2 PDCA cyclus

De gemeentesecretaris zorgt voor verbinding tussen de verschillende organisatieonderdelen met een belang in IB&P en vormt de schakel tussen business, IT en security. Zodat IB&P onderdeel wordt van een PDCA cyclus en er kan worden gestuurd op voortgang op de status en uitvoering van het IB&P programma en het bijstellen van de IB&P verplichtingen. De wijze waarop dit gebeurt hangt samen met de doorontwikkeling van de IB&P organisatie en de verdere ontwikkeling van de besturing in de organisatie.

5 Van beleid naar praktijk

5.1 Plan- & beleidvorming

Dit strategische IB&P beleid wordt als kader en basis gebruikt voor het uitwerken van tactische en operationele kaders, waaronder planvorming en beleidsvorming. Dit betreft de IB&P (gerelateerde) kader & planvorming binnen afdelingen (decentraal) alsmede beleid & planvorming vanuit het SPO-team (centraal). Dit beleidskader en implementatiekader zijn belangrijke onderdelen voor de uitwerking, implementatie en uitvoering van beleid. Afdelingen nemen IB&P via de gemeentelijke Planning & Control cyclus als onderwerp op in hun jaarplannen en passen daarbij dit beleid, maar ook verder uitgewerkte (de)centrale kaders toe.

5.2 Werken onder architectuur

De gemeente Helmond draagt het werken onder architectuur uit als een belangrijke ambitie. Wij vertalen het strategisch beleid naar een thema architectuur voor IB&P, met richtinggevende principes en een toekomstige inrichting van organisatie en informatievoorziening. Wat vanuit deze thema architectuur nodig is voor de realisatie van de ambities komt op een roadmap. Daarmee geeft deze roadmap belangrijke input voor het IBP-programma en IB&P jaarplannen.

De architectuur functie maakt het mogelijk om bewaking (toetsing & handhaving) op de strategische doelstellingen en principes plaats te laten vinden op strategisch, tactisch en operationeel niveau. Door de toepassing van architectuur vindt deze bewaking en sturing plaats gedurende veranderinitiatieven, ontwerpen, realisatie en implementatie. Dit bevordert het succesvol behalen van de beoogde doelen en voorziet in optimaal ontwerp en realisatie vanuit de projecten. Daarnaast is de architectuurfunctie cruciaal voor advies naar de strategievorming en -uitvoering vanuit de afstemming met de bredere bedrijfscontext. De thema architectuur IB&P wordt gebruikt door de CISO als instrument om te sturen en wordt beheerd door een thema architect.

5.3 IB&P Jaarplan & -programma

Het IB&P programma geeft een overzicht hoe in de periode 2026-2029 de speerpunten van dit beleid verder worden opgepakt (hoogover prioritering). In ieder jaarplan wordt dieper ingegaan op de voor dat jaar geprioriteerde projecten: planning, uitvoering, controle en sturing.

Het IB&P jaarplan en IB&P programma staan vooral in het teken van het realiseren van *centrale* IB&P doelstellingen. Dit betreft met name projecten die enkel impact hebben op de IB&P organisatie zelf, bijdragen aan de algehele IB&P strategie van de gemeente, betrekking hebben op organisatie brede maatregelen, meerdere afdelingen overstijgen en een gecoördineerde aanpak vereisen.

Afdelingen hebben hun *eigen* jaarplannen en programma's met daarin IB&P doelstellingen. Dit betreft projecten specifiek gericht op de processen van een organisatieonderdeel of staan in het teken van het implementeren van beleid en/of maatregelen beperkt tot de processen van dat organisatieonderdeel. De IB&P organisatie draagt bij aan deze projecten en ondersteunt deze, maar neemt niet de primaire verantwoordelijkheid van de eerste lijn over. Als onderdeel

van de in te richten PDCA cyclus wordt ook de voortgang van deze projecten gemonitord en besproken.

5.4 Communicatie van dit beleid

Dit beleid wordt gebruikt als kader en basis voor verdere uitwerking en dient bekend te zijn bij iedere medewerker, met oog voor wat hiervan van toepassing is voor de rol van die medewerker. De directie heeft vanuit haar rol de taak dit beleid in te bedden in de afdelingen en op niveau door te communiceren. De eerste lijn vertaalt wat van belang is in verdere communicatie. De tweede lijn kan hierbij ondersteunen door passende kaders te formuleren die de van toepassing zijnde elementen van het beleid effectief vast weten te leggen en door te communiceren op basis van het beoogde publiek. Deze passende kaders worden ook toegepast om het beleid te communiceren met externe stakeholders, waaronder leveranciers, externe toezichthouders, speciale belangengroepen en samenwerkingsverbanden/partners.

6 Bijlagen

6.1 Bijlage A: Afkortingenlijst

Afkorting	Betekenis
AI	Artificial Intelligence (Kunstmatige intelligentie)
AVG	Algemene Verordening Gegevensbescherming
B&W	Burgemeester & Wethouders
BIO	Baseline Informatiebeveiliging Overheid
BOA	Buitengewoon Opsporingsambtenaar
BRP	Basisregistratie personen
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSIR	Cybersecurity Implementatie Richtlijn
DigiD	Digitale Identiteit
DSPO	Decentrale Security en Privacy Officer
FG	Functionaris voor de Gegevensbescherming
GRC	Governance Risk Compliance
IB	Informatiebeveiliging
IB&P	Informatiebeveiliging & Privacy
IBD	Informatiebeveiligingsdienst
ISMS	Information Security Management System
NIS2	2e versie van de Europese Network Information Security richtlijn
PDCA	Plan Do Check Act
PNIK	Paspoorten en Nederlandse Identiteitskaarten
PUN	Paspoort Uitvoeringsregeling Nederland
SPO	Security en Privacy Officer
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
VNG	Vereniging van Nederlandse Gemeenten
Wpg	Wet politiegegevens