Bloemendaal

GEMEENTEBLAD

Officiële uitgave van de gemeente Bloemendaal

Nr. 546357

30 december

2024

Strategisch Gemeentelijk Informatiebeveiligings- en privacy beleid gemeente Bloemendaal

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P-beleid) voor de jaren 2025 tot en met 2028. Deze beleidsnota vervangt het in 2020 vastgestelde beleid "Strategie informatiebeveiliging gemeente Heemstede 2020-2024" en het in 2020 vastgestelde beleid "Privacybeleid Gemeente Heemstede". Dit beleid is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit beleid zet de gemeente een volgende stap om de beveiliging van persoons gegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging (in dit hoofdstuk opgenomen bij 1.2.1) zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens (in dit hoofdstuk opgenomen bij 1.3.1).

1.1 Leeswijzer

In hoofdstuk 1 worden de algemene uitgangspunten over informatiebeveiliging en privacy beschreven waar dit strategische beleid op is gebaseerd. In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet, wat zijn de onderliggende wetten en ontwikkelingen en de uitgangspunten voor het beleid. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.1.1 Gebruikte afkortingen

Afkorting	Uitleg		Afkorting	Uitleg
AVG	Algemene Verordening Gegevensbescherming (privacywetgeving)		IBD	InformatieBeveiligingsDienst (onderdeel van de VNG ter ondersteuning voor gemeenten)
BAG	Basisregistratie Adressen en Gebouwen		IB&P	Informatiebeveiliging en Privacy
BGT	Basisregistratie Grootschalige Topografie (kaart met alles wat op het maaivlak zit)		ISO	Information Security Officer (beheerder informatiebeveilging)
BIO	Baseline Informatiebeveilging Overheid (normenstelstel voor informatiebeveiliging)		NEN:ISO	Nederlands Normalisatie Instituut International Standard Organisation
BOA	Bevoegd Opsporings Ambtenaar		OT	Operationele Techniek (machines die gestuurd worden door computers)
BRO	BasisRegistratie Ondergrond (gegevens over geologische en bodemkundige opbouw)		PA	Proces Automatisering
BRP	BasisRegistratie Personen		PO	Privacy Officer (privacy beheerder)
CISO	Chief Information Security Officer (coordinator informatiebeveiliging)		PUN/PNIK	Paspoort Uitvoeringsregeling Nederland Wet op de Nederlandse IndetiteitsKaarten
DPIA	Data Protection Impact Assessment		SUWI	Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
ENSIA	Eenduidige Normatiek Single Information Audit(verplichte jaarlijkse		UAVG	Uitvoeringswet van de AVG

	zelfaudit over voldoen aan de BIO normen)			
FG	Functionaris Gegevensbescherming		Wpg	Wet Politie Gegevens

1.2 Informatiebeveiliging
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente 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 college, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.2.1 De 10 bestuurlijke principes voor informatiebeveiliging
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De gemeente staat achter deze principes. 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.

1.3 Privacy & Gegevensbescherming (AVG)
De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

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

1.3.1 De uitgangspunten voor privacy vanuit de AVG
De gemeente onderschrijft de uitgangspunten voor privacy zoals omschreven in de AVG. Dit zijn de volgende uitgangspunten:
- Persoonsgegevens worden rechtmatig en zorgvuldig verwerkt.
- De betrokkene heeft inzicht in de gegevens die de gemeente verwerkt en (rechtmatig) deelt met derden.
- Persoonsgegevens worden alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen verwerkt.
- Bij het verwerken van persoonsgegevens gaat de gemeente uit van de principes van subsidiariteit en proportionaliteit.
- De gemeente gaat uit van minimale gegevensverwerking.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk.
- Medewerkers van de gemeente hebben een geheimhoudingsplicht voor de verwerkte persoonsgegevens.
- De gemeente zorgt ervoor dat persoonsgegevens met onze samenwerkingspartners op een veilige manier gedeeld kunnen worden en dat hierover duidelijke afspraken worden gemaakt.
- De gemeente honoreert de privacy rechten van betrokkene.

2. Strategisch beleid

2.1 Doel

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.
Dit strategische beleid is hierbij vastgelegd in dit 'Strategisch Informatiebeveiligings- en privacy beleid voor de jaren 2025 tot en met 2028'. Dit beleid wordt specifieker uitgewerkt in tactisch beleid op onderdelen dat afzonderlijk hiervan wordt vastgesteld. In de afzonderlijke tactische stukken wordt wel verwezen naar dit hoger liggende strategische beleid. Daarnaast worden op basis het beleid concrete maatregelen en activiteiten opgenomen in het jaarlijks bij te stellen informatiebeveiligingsplan en privacy plan (IB&PP).

2.2 Ontwikkelingen

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

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat het management nu meer dan vroeger moet 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 is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 NIS2 Cybersecuritywet 2025

Medio 2025 moet de Europese NIS2 wetgeving zijn uitgewerkt in Nederlandse wetgeving die de Cybersecuritywet zal gaan heten. In deze wetgeving wordt vooral aandacht besteed aan de meldplicht voor beveiligingsincidenten en de zorgplicht voor een goede informatiebeveiliging. Daarnaast is aandacht voor de verantwoordelijkheid van bestuur en management voor informatiebeveiliging.

2.2.3 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Heemstede is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

2.2.4 De Wpg

De gemeente heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de Wet politiegegevens (Wpg). Hiervoor moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risicoinschatting, registratie en logging, meldplicht en documentatieplicht.

2.2.5 AI Act

Op 1 augustus 2024 is de Europese AI Act in werking getreden. Vanaf februari 2025 worden gefaseerd steeds meer onderdelen van de Act van toepassing. Zeker gezien vanuit Privacy en ook vanuit het oogpunt van mensenrechten moet zorgvuldig worden omgegaan met AI. Dit is een belangrijk aandachtspunt voor de komende jaren.

2.2.6 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

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

2.2.7 Informatie uit incidenten, inbreuken en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2023. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2022 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met normen en

overheidsmaatregelen. Naar verwachting zal medio 2025 de BIO2.0 beschikbaar komen. Vanaf dan geldt de BIO 2.0.
Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsafdelingen die zich met PA bezig houden. Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR).

2.4 Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy op tactisch en daarna operationeel niveau. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven Informatiebeveiligings- en privacy plan.

2.5 Scope informatiebeveiliging en privacy
De scope van deze beleidsnota omvat alle 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.
Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI, DigiD en gemeentelijke basisregistraties). Deze worden in aanvullende tactische beleidsdocumenten geformuleerd.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

Nadere toelichting op de scope van informatie en systemen
- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.
- Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.

2.6 Uitgangspunten
Het bestuur en het management 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 gemeente heeft, de (privacy) risico's die de gemeente 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 IB&P-beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen
De strategische doelen van het IB&P-beleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het 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 toepassen van dataminimalisatie.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Heemstede hebben een interne eigenaar 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.
- 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 gemeente 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 gemeentelijke processen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.3 IB&P-governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch IB&P-beleid vast.
- Het management stelt jaarlijks het IB&P-plan vast.
- Het management is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- Het management ziet erop toe dat de teammanagers en teamleiders adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het management en/of het college van B&W.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals -onder andere- de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
- Het management en de teammanagers en teamleiders stellen informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy naar aanleiding van de rapportage van de CISO en of de FG..
- De teammanagers en teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teammanagers en teamleiders zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De teammanagers en teamleiders zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente 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.
- Teammanagers en teamleiders dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers en teamleiders voeren quickscans informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG uit om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiligings- 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 onder leiding van het Management, gebaseerd op:
  - dit IB&P-beleid;
  - de rapportages van de FG en de CISO;
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - andere eventuele auditresultaten;
  - het dreigingsbeeld gemeenten van de IBD;
  - uitkomsten risicoanalyses en DPIA's
  - de door de afdelingsmanagers 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 (ISO, 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 de FG en de CISO van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA-coördinator.
De opbouw van het lijnmanagement in de gemeente bestaat uit twee tot drie lagen. Verantwoordelijk voor sturen en leidinggeven op strategisch niveau is het managementteam, hierin zitten de gemeentesecretaris, de domeinmanagers en de managers. De tactisch/operationeel leidinggevende laag hieronder bestaat uit teammanagers en teamleiders.

3.1 Aansturing: management

Het management zorgt ervoor dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager of teamleider. Het management zorgt ervoor dat de teammanager of de teamleider zich verantwoordt over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het management zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college 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 college zich ook verantwoorden naar de raad.

Het management stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het management draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacy beleidsonderwerpen en laat zich hierin bijstaan door de CISO, ISO, FG en PO van de gemeente. Het management autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: teammanagers en teamleiders

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle teammanagers en teamleiders. 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. Teammanagers en teamleiders rapporteren aan het managementteam over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het teamoverleg.

Taken van de teammanagers en teamleiders in het kader van informatiebeveiliging en privacybescherming zijn:

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

3.3 Controle en verantwoording

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

3.3.1 ENSIA

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

3.3.2 Jaarlijkse rapportages

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

Verantwoording naar het college
Jaarlijks worden door de FG en de CISO een rapportage opgeleverd over de stand van zaken van voldoen aan alle eisen en normen over respectievelijk de privacy en over informatiebeveiliging. De jaarrapportages worden door het college vastgesteld. Er worden ook halfjaar rapportages opgesteld, deze worden aan het management aangeboden.

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

Verantwoording naar andere instanties

Via de ENSIA verantwoordt de gemeente zich ook aan de stelselhouders voor DIGID/WOZ/BAG/SUWI/BRP. Deze rapportages gaan via de ENSIA systematiek naar de diverse ministeries of uitvoeringsorganisaties.

Vastgesteld op : 10 december 2024 door het college van Bloemendaal