GEMEENTE DE BILT

GEMEENTEBLAD

Officiële uitgave van de gemeente De Bilt

Nr. 325055

24 juli

2025

Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente De Bilt 2025 – 2028

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiliging beleid (IB beleid) voor de jaren 2025 tot 2028 en vervangt het in 2021 vastgestelde Gemeentelijk Informatiebeveiligingsbeleid. Deze nota is soms richtinggevend en soms kaderstellend, Het strategische beleid wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid zet de gemeente een volgende stap om de beveiliging van 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 27002:2022 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid 2.0 (BIO 2.0) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid op specifieke onderwerpen zoals fysiek- en logisch toegang, kunstmatige intelligentie, bedrijfcontinuïteit, etc . In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van ambtelijk opdrachtgevers, de CISO, de ISO, de privacy functionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

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 bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

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 taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of 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. Vanuit de AVG hebben wij de plicht om persoonsgegevens zorgvuldig te beveiligen.

2. Strategisch beleid

2.1 Doel

Het doel van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2025 tot 2028' is het voldoen aan relevante wet en regelgeving, richting geven aan de organisatie op het vlak van informatiebeveiliging

en kaders te stellen. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in risicogerichte meerjarenplanning en draagt bij aan de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van onze dienstverlening.
Het beleid op informatiebeveiliging dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid.

2.2 Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het IB beleid zijn de volgende:

2.2.1 De BIO
De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de ambtelijk opdrachtgevers 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 is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. In dit strategisch beleid sorteren we voor richting de BIO 2.0

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

2.2.3 De WPG
De 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

2.2.4 De 10 principes voor informatiebeveiliging
[1]

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

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

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

1) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

2.2.6 Informatie uit incidenten, inbreuken op de beveiliging 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 27001:2022. 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[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing, bewaking en beheer van fysieke processen. Denk aan technologie die nodig is om een brug of sluis te bedienen, verkeersinstallaties, gebouwbeheersysteem, straatverlichting etc. Het beveiligingsbeleid van de gemeente is ook voor de bescherming van OT en beleidsafdelingen die zich met OT bezighouden.[3] Voor de bescherming van OT gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR).[4]

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 op tactisch en operationeel niveau.

2.5 Scope informatiebeveiliging
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 en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten geformuleerd.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college is eindverantwoordelijke voor de informatiebeveiliging. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.
- Alle operationele technologie (OT) die gebruikt wordt binnen de gemeentegebouwen en in de publieke ruimte van de gemeente, en die eigendom is van de gemeente, zoals gebouwbeheersystemen, cameratechnologie, pompen en gemalen.

2.6 Uitgangspunten
Het bestuur, de directie en het MT spelen een cruciale rol bij het uitvoeren van dit strategische IB beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de 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 op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB beleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering

2) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*
3) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
4) https://www.cert-wm.nl/csir

en (persoons)gegevens(verzamelingen). Het IB beleid is in lijn met de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het IB 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.
- Het waarborgen van een veilige werkomgeving

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Elke medewerker heeft een verantwoordelijkheid voor het correct uitvoeren van informatiebeveiligingsrichtlijnen. Management is eindverantwoordelijk voor het correcte uitvoer van informatiebeveiliging. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente hebben een interne eigenaar die de vertrouwelijkheid, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het IB beleid vormt samen met het IB plan het fundament onder een betrouwbare informatievoorziening. In het IB plan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging.
- Informatiebeveiliging 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 beleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 IB governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college stelt als eindverantwoordelijke het strategisch IB beleid vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het Information Security Management System (ISMS) systeem voor informatiebeveiliging.
- Bevindingen uit audits, beveiligingsonderzoeken, worden geregistreerd in het ISMS. Hierin wordt de voortgang bewaakt van de bevindingen
- De directie is verantwoordelijk voor het vragen om informatie bij de ambtelijk opdrachtgevers en ziet erop toe dat adequate maatregelen genomen worden voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.

- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
- De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren aan het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
- De Privacy Officer (PO) fungeert als verbindende schakel tussen beleid en uitvoering op het gebied van privacy. De PO ondersteunt de organisatie bij het naleven van privacywetgeving, adviseert over privacyvraagstukken in projecten en processen en draagt zorg voor de coördinatie van het bewustwordingsprogramma. De PO signaleert knelpunten, initieert verbeteracties en rapporteert hierover periodiek aan de directie.
- De Information Security Officer (ISO) ondersteunt het management en de operationele teams bij de implementatie van informatiebeveiligingsbeleid. De ISO ziet toe dat beleid correct wordt uitgevoerd
- De directie en ambtelijk opdrachtgevers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan de FG.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en of de FG. De onderwerpen die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De ambtelijk opdrachtgevers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging binnen de processen waarvoor zij verantwoordelijk zijn.
- De ambtelijk opdrachtgevers zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De ambtelijk opdrachtgevers zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten 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 basiskennis van de privacywetgeving en weten deze 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.
- Ambtelijk opdrachtgevers 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. Ambtelijk opdrachtgevers voeren risicoanalyses uit op de informatiebeveiliging op basis van de BIO en voeren bij het verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG om deze risicoafwegingen te kunnen maken.
- Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiligingseisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging binnen de organisatie dient actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB plan opgesteld gebaseerd op:
    - Dit IB beleid;
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Andere audit resultaten;
    - het dreigingsbeeld gemeenten van de IBD;
    - Uitkomsten risico-analyses en DPIA's
    - De door de ambtelijk opdrachtgevers 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 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 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 management verantwoordelijk voor het realiseren van informatiebeveiliging binnen de eigen processen. De tweede lijn (CISO, 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 FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA coördinator.

3.1 Aansturing: directieteam

De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een ambtelijk opdrachtgever. De directie zorgt dat de ambtelijk opdrachtgevers zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen rust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de gemeente De Bilt gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: MT/ambtelijk opdrachtgevers

Informatiebeveiliging valt onder de verantwoordelijkheden van het MT en alle ambtelijk opdrachtgevers. 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. Het MT en Ambtelijk opdrachtgevers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

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

3.3 Controle en verantwoording

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

3.3.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig

is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke ambtelijk opdrachtgevers. De ambtelijk opdrachtgevers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college 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.

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

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

Slotbepalingen

1. Dit beleid is vastgesteld op 15 juli 2025.
2. Het Informatiebeveiligingsbeleid gemeente De Bilt van 1 juli 2010 wordt ingetrokken.
3. Dit beleid treedt in werking de dag nadat het is bekendgemaakt.
4. Dit beleid wordt elke twee jaar, gerekend vanaf de inwerkingtreding, geëvalueerd en zo nodig aangepast.

Aldus vastgesteld in de vergadering van het college van burgemeester en wethouders van de gemeente De Bilt van 15 juli 2025.

Het college van burgemeester en wethouders van De Bilt,

de secretaris,
drs. I.M. Schuurman

de burgemeester,
drs. M.C. Haverkamp