Gemeente Wassenaar

GEMEENTEBLAD

Officiële uitgave van de gemeente Wassenaar

Nr. 252866

29 mei

2026

Strategisch Informatiebeveiligings- en Privacybeleid 2025-2028

Het college van burgemeester en wethouders van de gemeente Wassenaar,

gelet op artikel 4:81, lid 1 van de AWB;

overwegende dat de Basisbeveiliging Informatiebeveiliging Overheid 2 (BIO2) een juridische basis krijgt via de Cyberbeveiligingswet (Cbw) — de Nederlandse implementatiewet van de Europese Network & Information Services 2 (NIS2)-richtlijn. Dit gebeurt door opname van de BIO2 in een ministeriële regeling voor de sector Overheid onder het Cyberbeveiligingsbesluit (Cbb). Tot inwerkingtreding van de Cbw geldt de BIO2 als verplichte zelfregulering (voor Rijk, provincies en waterschappen). Na inwerkingtreding van de Cbw wordt de BIO2 wettelijk verplicht voor overheidsorganisaties, doordat zij via regeling onder het Cbb wordt aangewezen als het normenkader voor cyberbeveiliging.

b e s l u i t :

1) het Strategisch Informatiebeveiligings- en Privacybeleid 2025-2028 met terugwerkende kracht vanaf 1-1-2025 vast te stellen.
2) het huidige, in 2020 vastgestelde 'Informatiebeveiligingsbeleid 2020-2024' en het in 2025 vastgestelde "Privacybeleid Wassenaar" in te trekken.

1 Inleiding

Deze nota beschrijft het strategisch Informatiebeveiligings- en privacybeleid (IB&P-beleid) voor de jaren 2025 tot en met 2028 en vervangt het in 2020 vastgestelde 'Informatiebeveiligingsbeleid 2020-2024' en het in 2025 vastgestelde "Privacybeleid Wassenaar". De vastgestelde Privacyverklaring blijft wel van kracht. Daarnaast wordt met de vaststelling van het Strategisch Informatiebeveiligings- & Privacybeleid 2025-2028 concreet invulling gegeven aan Aanbeveling 4.3 (Informatiebeveiliging) uit de Managementletter 2025 en het Plan van Aanpak dat hierop door de Gemeente Wassenaar is opgesteld.

De strategie voor informatiebeveiliging en privacy is afgeleid van en sluit aan op de Dienstverleningsovereenkomst I&A- en P&A Taken van 8 juni 2021 en de Visie op de informatie-voorziening 2024-2025 (iVisie).
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en procedures en standaarden op operationeel niveau.

Dit strategisch Informatiebeveiligings- en privacybeleid is richtinggevend en kaderstellend voor alle informatiebeveiligings- en privacy activiteiten. De basis voor dit strategisch beleid zijn de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) en het VNG Borgingsproduct AVG. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de Vereniging Nederlandse Gemeenten (VNG) en de beginselen uit de Algemene Verordening Gegevensbescherming (AVG) voor het verwerken van persoonsgegevens.

1.1 Leeswijzer

In hoofdstuk 2 worden de doelen en uitgangspunten van het strategisch beleid uiteengezet. Het strategische beleid wordt vastgesteld door het college. Dit wordt aangevuld met onderwerp-specifieke tactische beleidsregels, die worden vastgesteld door de respectievelijke verantwoordelijke manager, die proceseigenaar is. Beleidsdocumenten zijn relatief gezien vrij statisch.

In het jaarlijks uit te brengen Informatiebeveiligings- en privacyplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Het is onderdeel van het jaarplan I&D proces. Rond maart hebben we een definitief concept. Vervolgens werken we toe naar een integratie met het kadernota-proces. De kadernota is het brondocument voor de begroting van het opvolgende jaar. Dit wordt gedaan op basis van input van de eenheidsmanagers, de CISO, de privacyfunctionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de Informatiebeveiligingsdienst voor gemeenten (IBD) en de uitkomsten van risicoanalyses en Data Protection Impact Analyses (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 verplicht.

Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Risicomanagement

Risicomanagement vormt de kern van informatiebeveiliging binnen de gemeentelijke context. Uitgangspunt voor informatiebeveiliging is het systematisch identificeren, analyseren en behandelen van risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie kunnen aantasten. Voor privacy geldt dat er risicobeoordelingen moeten worden uitgevoerd om de risico's voor rechten en vrijheden van betrokkenen te beoordelen. Het risicomanagement voor informatiebeveiliging is gebaseerd op de normen ISO 27001 en ISO 27005 en voor privacy op het IBD Privacy Normenkader. Deze normen bieden een gestructureerde methode voor risicoanalyse en -behandeling. De methode voor informatiebeveiliging is door de IBD (Informatiebeveiligingsdienst van VNG) uitgewerkt in de Business Model Canvas-aanpak (BMC) en de Proces Risico Model Gemeente-aanpak (PRMG). BMC is een manier om in kaart te brengen hoe het te onderzoeken proces er uitziet en met PRMG worden de risico's in kaart gebracht. Beide zijn vooral ook een mooi communicatiemiddel naar de lijnmanager en bieden daarnaast een gestructureerde en herhaalbare aanpak om procesrisico's te vinden en te beoordelen en om passende maatregelen te bedenken. Dit is noodzakelijk voor het waarborgen van dienstverlening, naleving van wet- en regelgeving, en bescherming van persoonsgegevens. Deze werkwijze hanteren we bij processen waar risico's significant en/of gegevensstromen complex zijn, en per proces of project beoordelen we of volledige toepassing nodig is.

1.3 Aandachtsgebied en diepgang

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 politieke bestuur, alle medewerkers, burgers, gasten, bezoekers, bedrijven/ondernemers, instellingen en externe relaties.

Als gemeente sluiten we aan bij de BIO2 aanpak van de IBD, dat wil zeggen dat we beginnen met de belangrijkste primaire processen (zie bijlage 1) en daarbij volledig aanhaken op de door de IBD en de gemeentelijke werkgroep BIO2 uitgevoerde risicoanalyses en de daarbij voorgestelde maatregelen. We zullen de IBD volgen in de verdere stappen die in gezamenlijkheid uitgewerkt worden. We volgen zo de kracht van het collectief.

1.4 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 en om een efficiënte en effectieve bedrijfsvoering te voeren. 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.

De gemeente sluit aan bij de privacy-aanpak van de IBD en de door de IBD gepubliceerde DPIA's. Ook hier maken we gebruik van de kracht van het collectief. Door de gemeente opgestelde DPIA's zullen gedeeld worden met de IBD.

1.5 Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy

De gemeente gebruikt dagelijks privacygevoelige gegevens van inwoners, ondernemers, organisaties en andere partijen. Deze partijen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze gegevens omgaat. Onvoldoende oog voor risico's, rechtmatigheid en ethiek kan leiden tot grote schade voor politiek, reputatie, financiën en personeel. Ook kunnen inwoners en bedrijven het slachtoffer worden van ons handelen of nalaten. Cybercriminelen, geopolitieke krachten, menselijke fouten, falende technologie en geconcentreerde afhankelijkheid van cloud-leveranciers dwingen ons om voorbereid en weerbaar te zijn.

Medewerkers moeten voldoende ondersteund worden om hun werk goed uit te voeren, waarbij de continuïteit van de gemeentelijke processen geborgd blijft. Privacy en informatieveiligheid gaan niet alleen over ICT, maar ook over de mens in de organisatie en hoe deze met risico's omgaat. Voorbeeldgedrag van medewerkers, eenheidsmanagers en directie speelt hierbij een cruciale rol.

De gemeente moet zich steeds afvragen of de risico's in beeld zijn, de juiste vragen stellen over het gebruik van gegevens en de juiste maatregelen treffen. Dit is een continu proces waarbij privacy en informatiebeveiliging al aan het begin van het proces meegenomen moeten worden. Dit voedt ook de bewustwording voor deze onderwerpen.

Ambitie:

De kritische bedrijfsprocessen en de informatie die daarbinnen worden gebruikt zijn beschikbaar en betrouwbaar (gegevens zijn accuraat en volledig) waarbij vertrouwelijkheid (informatie is alleen toegankelijk voor geautoriseerde personen/systemen) en transparantie richting inwoners wordt gewaarborgd.

Visie:

De gemeente waarborgt de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van informatie binnen alle kritische bedrijfsprocessen. Transparantie richting inwoners staat centraal, waarbij informatiebeveiliging en privacy structureel zijn verankerd. Door proactief risico's te beheersen, bewustwording te stimuleren en te voldoen aan wet- en regelgeving, versterken we het vertrouwen van inwoners en nemen we onze maatschappelijke verantwoordelijkheid serieus.

Missie:

Wij zorgen ervoor dat inwoners en medewerkers kunnen vertrouwen op veilige, beschikbare en betrouwbare informatievoorziening. Door informatiebeveiliging en privacy integraal onderdeel te maken van onze dienstverlening, creëren we een veilige, transparante en zorgvuldige digitale omgeving. We handelen proactief om risico's te beperken, voldoen aan wet- en regelgeving en versterken zo het vertrouwen in onze organisatie.

2 Doelen en uitgangspunten

2.1 Inleiding

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligings- en privacy beleid voor de jaren 2025 tot en met 2028' om daarmee IB&P te borgen binnen de gemeente. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen Informatiebeveiligings- en privacyplan (IB&P-Plan). Het Strategisch Informatiebeveiligings- en privacybeleid geeft richting aan de organisatie en biedt ondersteuning aan het College van B&W, het management en al het overige personeel bij de sturing op de planning, de uitvoering, het beheer van en de controle op informatieveiligheid en privacy.

2.2 Kaders voor dit beleid

De kaders die van belang zijn voor de handhaving en actualisering van het IB&P beleid zijn de volgende:

1. **De BIO2**: is het normenkader voor de overheid en richt zich op risicobeheersing en werkt op basis van risicomanagement. Eenheidsmanagers moeten werken volgens de aanpak van ISO 27001 en continu afwegingen maken over risico's en de beveiliging van informatie.
2. **NIS2 en Cyberbeveiligingswet (in de maak**): 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.
3. **De AVG en het privacy normenkader**: Nieuwe technologische ontwikkelingen en een steeds meer digitaal wordende overheid maken het veilig omgaan met persoonsgegevens meer complex en noodzakelijk. De gemeente wil aangeven hoe zij invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy.
4. **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, dataclassificatie, risico-inschatting, registratie en logging en meld- en documentatieplicht.
5. **De 10 bestuurlijke principes voor informatiebeveiliging**: De principes gaan vooral over de rol van het College van B&W bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen het College van B&W bij het uitvoeren van goed risicomanagement en het nemen van een voorbeeldrol.
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 en helpt bij het actualiseren van beleid en plannen.

7. Informatie uit incidenten, inbreuken op de beveiliging en datalekken: De gemeente heeft een systeem waarin incidenten worden vastgelegd. Deze informatie is waardevol voor het actualiseren van het beleid.
8. **AI**: AI, in welke vorm dan ook, ontwikkelt zich sinds de vorige beleidscyclus in rap tempo. Deze snelle ontwikkeling heeft invloed op de beveiliging van onze data en de privacy van onze inwoners. Het wordt steeds complexer om phishingmails te herkennen, en de snelheid waarmee zich aanvals- en verdedigingstechnieken ontwikkelen, is voor de mens (binnenkort) niet meer bij te houden. Met AI-geletterdheid en transparantie over gebruik van AI (GenAI) geven we inzicht in de kansen en risico's rondom het gebruik van AI-toepassingen.
9. **Integraal Veiligheidsbeleid (IVB)**: Hierin staan de uitgangspunten die gericht zijn op ´eigen huis op orde´, digitale criminaliteit (cybercrime) en bevat ambities die relevant zijn voor dit beleid.
10. **Dienstverleningsovereenkomst (DVL)**: Hierin staan afspraken en uitgangspunten die gericht zijn op de dienstverlening van de eenheid Informatie- en Datamanagement. Een belangrijk uitgangspunt is dat het waarborgen van de integriteit en betrouwbaarheid van data cruciaal is, zodat beslissingen gebaseerd op deze data juist en rechtvaardig zijn.
11. **Visie op de informatievoorziening 2024-2025 (iVisie)**: De iVisie beschrijft het basisniveau van de informatievoorziening. Daarbij gaat het om de continuïteit van de bedrijfsvoering en de kwaliteit van de informatievoorziening voor de dienstverlening. De kaders die in de iVisie zijn vastgelegd gaan over informatieveiligheid, privacy, informatiebeheer en de rechtmatigheid van en in-controle-zijn over de informatievoorziening.

2.3 Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is de BIO2. De BIO2 schrijft voor dat risicomanagement ingericht moet worden volgens de norm NEN-EN-ISO/IEC 27001. De maatregelen worden op basis van good practices bij (lokale) overheden en de norm NEN-EN-ISO/IEC 27002 genomen en zijn aangevuld met de overheidsmaatregelen uit de BIO2. Hierbij wordt gebruik gemaakt van het ondersteuningsaanbod van de IBD.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. OT gaat over het besturen van onder andere gebouwen, verkeer, bruggen en gemalen7. Voor de bescherming van OT gebruikt de gemeente de OT-aanpak van de IBD, die gebaseerd is op de Cybersecurity Implementatie Richtlijn (CSIR)8. Voor het verwerken van zorginformatie gebruikt de gemeente de NEN7510.

2.4 Plaats van het strategisch informatiebeveiligingsbeleid
Het strategisch informatiebeveiligingsbeleid vormt de basis voor tactische beleidsplannen en geeft richting aan de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau. Dit beleid wordt vertaald in aanvullend beleid en richtlijnen. De werkzaamheden worden uitgewerkt in het jaarlijkse Informatiebeveiligings- en privacyplan (IB&P-plan).

2.5 Reikwijdte informatiebeveiliging en privacy
Om invulling te geven aan het I&P beleid 2025-2028 maakt de Gem Wassenaar gebruik van de aanpak die door de IBD wordt voorgestaan die rekening houdt met een realistisch groeipad. De reikwijdte van dit beleid is gebaseerd op alle gemeentelijke processen, informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen voor zover deze passen binnen het door de IBD uitgewerkte ondersteuningsaanbod. Dit beleid dekt aanvullende beveiligingseisen uit wetgeving af, zoals voor de AVG, UAVG, WPG, BRP, PNIK/PUN, DigiD en SUWI. Specifieke en vaak technische beveiligingseisen voor kerntaken worden in aanvullende beleidsdocumenten geformuleerd.

2.6 Herziening
Dit beleid wordt jaarlijks beoordeeld of het nog passend is. Hiervan wordt een verslag gemaakt en dit verslag wordt ieder jaar ingebracht in de behandeling van de begroting in Q2.

2.7 Werkwijze
Het bestuur, de directie en eenheidsmanagers spelen een belangrijke rol bij het uitvoeren van dit beleid. Het management beoordeelt hoe belangrijk de verschillende delen van de informatievoorziening zijn voor de gemeente, welke risico's er zijn en welke risico's te groot zijn. Op basis hiervan stelt de CISO het strategisch beleid op en het bestuur stelt dit beleid vast. Het management zorgt ervoor dat het wordt uitgevoerd. Andere vormen van tactisch beleid worden opgesteld binnen de eenheden die verantwoordelijk zijn voor de uitvoering van het onderwerp.

Het management geeft duidelijke richting aan informatiebeveiliging en privacy en laat zien dat ze dit belangrijk vinden. Dit beleid geldt voor de hele organisatie, alle processen, systemen en gegevens. Het beleid is in lijn met de wet- en regelgeving.

2.8 Communicatie- en bewustwordingsplan
Een gestructureerd communicatie- en bewustwordingsplan is essentieel om te borgen dat het informatiebeveiligingsbeleid niet alleen wordt vastgesteld, maar ook daadwerkelijk wordt begrepen, toegepast en nageleefd binnen de organisatie.

Rollen en verantwoordelijkheden:

- de CISO coördineert de inhoud en actualiteit van de communicatie voor informatiebeveiliging;
- de PO coördineert de inhoud en actualiteit van de communicatie voor privacybescherming;
- de communicatieafdeling verzorgt de vormgeving, verspreiding en aansluiting bij bestaande interne kanalen.

Middelen: gebruik van intranetberichten, nieuwsbrieven, quiz vragen, e-learnings, posters, teamoverleggen en onboarding-modules om medewerkers te informeren en te activeren.

Frequentie: periodieke updates (minimaal elk kwartaal) en gerichte campagnes bij beleidswijzigingen, incidenten of themaweken over informatiebeveiliging en/of privacy.

2.9 Strategische doelen
Dit beleid richt zich op drie hoofddoelen:

1. Risico's beheersen en incidenten voorkomen.
2. De veiligheid van bedrijfsmiddelen en persoonsgegevens waarborgen.
3. Naleving en reactievermogen verbeteren.

We werken risicogestuurd en volgens security- en privacy-by-design, passen PDCA-cyclus toe, en verwachten naleving van alle medewerkers en leveranciers; voortgang meten we met duidelijke KPI's en we herijken bij nieuwe dreigingen of wijzigingen in wet- en regelgeving.

We voorkomen en beperken schade door onder meer de impact van verstoring van onze voorzieningen tijdig in beeld te hebben. Daarom maken we onze collega's, inwoners en organisaties bewuster van (cyber-)risico's en vergroten we de (digitale) weerbaarheid aan de hand van standaarden. Daarnaast hebben we een beeld van het gedrag en de cultuur waarmee we de weerbaarheid kunnen vergroten en ons kunnen voorbereiden op crisissituaties.

Doel 1: Risico's beheersen en incidenten voorkomen

Subdoel 1.1: Identificeren en beoordelen van potentiële risico's in alle processen binnen het Information Security Management Systeem (ISMS) en Privacy Management systeem (PMS).

Subdoel 1.2: Implementeren van risicobeheermaatregelen om geïdentificeerde hoge risico's te mitigeren.

Subdoel 1.3: We werken samen met andere gemeenten en gaan uit van de kracht van het collectief.

Subdoel 1.4: Verlagen van het aantal incidenten door menselijk gedrag door middel van training, bewustwordingscampagnes en door het creëren van een veilige cultuur waarin het doen van meldingen aangemoedigd wordt.

Doel 2: Waarborgen van de veiligheid van bedrijfsmiddelen en persoonsgegevens

Subdoel 2.1: Beveiligen van alle bedrijfsmiddelen en persoonsgegevens die passen binnen de door de organisatie vastgestelde reikwijdte van het ISMS door het toepassen van passende technische en organisatorische maatregelen.

Subdoel 2.2: Implementeren van dataminimalisatieprincipes, zodat alleen noodzakelijke gegevens worden verzameld en bewaard.

Subdoel 2.3: Realiseren van zero incidenten met ongeautoriseerde toegang door verbeterde toegangscontrole en monitoring.

Doel 3: Naleving en reactievermogen verbeteren

Subdoel 3.1: Het opstellen van een effectief incidentresponsplan dat binnen 24 uur na een incident een eerste reactie biedt.

Subdoel 3.2: Zorgen voor continue naleving van het IB&P-beleid, met regelmatige audits en evaluaties die zorgen voor 100% naleving. Dit vertalen we ook door naar onze leveranciers.

Subdoel 3.3: Vergroten van de bewustwording rondom veilig omgaan met persoonsgegevens door middel van AVG-training, bewustwordingsprogramma's rondom dataminimalisatie en grondslagen en door het creëren van een veilige cultuur waarin het doen van meldingen aangemoedigd wordt.

2.10 Belangrijke uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van de eenheidsmanagers. Alle informatiebronnen en -systemen die gebruikt worden hebben een data- en systeemeigenaar die de vertrouwelijkheid, beschikbaarheid, integriteit, privacy-eisen en/of waarde bepaalt van de informatie die ze bevatten.
- Door periodieke controle, organisatiebrede 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 organisatiebreed 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.
- Het College van B&W stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacyeisen volgens de wijze zoals gesteld in dit beleid.
- Het bestuur ziet toe op de uitvoering van het beleid en richt controlemechanismen in om signalen te ontvangen en laat zich hierin bijstaan door de CISO. De gemeenteraad wordt voldoende geïnformeerd zodat ze voldoende kennis heeft om te sturen op dit onderwerp. Risicobeheersing op gebied van informatiebeveiliging en privacy zijn vaste onderdelen van voorstellen aan het bestuur. Er is een IB&P-raadscommissie ingesteld, waarbinnen niet de politieke agenda heerst, maar het in vertrouwen kunnen overleggen over IB&P-onderwerpen.
- Regels en verantwoordelijkheden 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, onbevoegd gebruik, verandering, openbaring, vernietiging, verlies of overdracht. Bij een vermoeden van een inbreuk hierop moet melding worden gemaakt.
- Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels op basis van een risico-inschatting.

2.11 Praktische invulling
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

1. Het College van B&W stelt als eindverantwoordelijke het Strategisch Informatie-beveiligings- & Privacybeleid beleid vast.
2. De directie stelt jaarlijks het IB&P plan vast.
3. De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
4. Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden opgevoerd bij de betreffende maatregelen in het managementsysteem voor informatiebeveiliging en privacybescherming door de proceseigenaar.
5. De directie is verantwoordelijk voor het vragen om informatie bij de eenheidsmanagers en ziet erop toe dat zij adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiserings-systemen die onder hun verantwoordelijkheid vallen.
6. 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 in het managementoverleg en daarna aan de verantwoordelijke portefeuillehouder, voorafgaand aan de P&C-gesprekken. De CISO brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
7. 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 de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.

8. De directie en de eenheidsmanagers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan de Functionaris Gegevensbescherming.
9. Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO of de FG. De onderwerpen die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen. Ook worden dan besluiten genomen over overtredingen op of tekortkomingen in de naleving.
10. De verantwoordelijkheid voor de uitvoering en borging van de informatiebeveiliging en privacy ligt in de lijn bij de eenheidsmanagers. (Zie ook de RASCI-tabel.)
11. De eenheidsmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
12. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
13. Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en securityrichtlijnen en weten deze bewust toe te passen in hun dagelijks werk.
14. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
15. Eenheidsmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd door loggingcontrole, zodat zij kunnen vaststellen dat alleen rechthebbenden de juiste persoonsgegevens ingezien en verwerkt hebben.
16. De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Eenheidsmanagers voeren quickscans informatiebeveiliging of dataclassificaties uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's op basis van de AVG om deze risico-afwegingen te kunnen maken.
17. Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.12 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacyeisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd. Voor wat betreft gemeenschappelijke regelingen (GR) kan dat betekenen dat met een vakgenoot bij de GR wordt afgestemd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en gewaarborgd te worden.
- Jaarlijks beoordelen van de actualiteit van dit strategisch beleid op basis van veranderende risico's en veranderende wet- en regelgeving.
- Jaarlijks wordt een IB&P plan opgesteld onder leiding van de CISO en de FG door de lijn, gebaseerd op:
    - dit IB&P beleid;
    - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - de bevindingen uit het toezicht door de FG;
    - andere audit resultaten;
    - het toezichtplan van de FG;
    - 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 moet het bestuur voldoende financiële middelen en uitvoeringscapaciteit ter beschikking stellen. Het is mogelijk dat er dan nog keuzes gemaakt moeten worden wat in het IB&P jaarplan blijft en wat wordt doorgeschoven of geschrapt.

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 zijn de eenheidsmanagers verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO, Information Security Officers (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 rol van ENSIA-coördinator die door de CISO wordt vervuld.

Als bijlage bij dit beleid is opgenomen een voor onze gemeente uitgewerkte versie van de RASCI-tabel (zie bijlage 2).

3.1 College van B&W: Aansturing
Strategische richting: Het College van B&W is verantwoordelijk voor het formuleren en goedkeuren van de strategische doelstellingen van het IB&P-beleid, zoals het voorkomen van incidenten, de bescherming van bedrijfsmiddelen en persoonsgegevens, en de naleving van wet- en regelgeving.

Resources en budget: Toewijzen van de nodige middelen en budget voor de implementatie van het beleid en het bereiken van de doelstellingen. Dit omvat het vrijmaken van middelen voor trainingen, risicobeheer, en technologie-investeringen.

Governance en compliance: Het College van B&W waarborgt de naleving van alle relevante wet- en regelgeving op strategisch niveau, waaronder de AVG, de Wpg, de Cbw, de BIO2 en andere normen. Ze stelt het kader voor compliance vast en zorgt voor de naleving ervan.

Risicomanagement: Het College van B&W draagt zorg voor het risicomanagementproces op organisatieniveau. Ze zorgen ervoor dat er een goed gedefinieerd risicobeheerproces bestaat en dat de belangrijkste risico's adequaat worden beheerd.

Verantwoordelijkheid voor rapportage: Het College van B&W is verantwoordelijk voor het ontvangen en bespreken van periodieke rapportages met betrekking tot de voortgang van de strategische doelstellingen, inclusief auditresultaten en risicoanalyses.

Beleid en besluitvorming: Het nemen van strategische beslissingen over het beleid en het waarborgen dat het beleid in lijn is met de organisatievisie en doelstellingen en compliant is aan alle regels en wetten.

Acties:

- Goedkeuren van de algemene, strategische beleidslijnen en doelstellingen (dit document). Vaststelling door College van B&W.
- Beheren van het risicoprofiel van de organisatie.
- Evalueren van de rapportages en prestaties van het IB&P-beleid.

3.2 Eenheidsmanagers: Uitvoering
De praktische uitvoering van het Informatiebeveiliging- en Privacybeleid valt onder de verantwoordelijkheden van alle eenheidsmanagers. 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 en dat is dus meestal degene die verantwoordelijk is voor het procesresultaat; er moet dus altijd iemand verantwoordelijk zijn. Eenheidsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de eenheden over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het bedrijfsvoeringsoverleg/managementoverleg.

Implementatie van het beleid: De eenheidsmanagers zijn verantwoordelijk voor de uitvoering van het IB&P-beleid binnen hun eenheden en zorgen ervoor dat de doelstellingen op operationeel niveau behaald worden. Zij werken samen met informatiemanagers, privacyfunctionarissen en beveiligingsprofessionals om risico’s te beoordelen en behandelen.

Zorgdragen voor risicobeheer: Het identificeren van eenheidsspecifieke risico's en het implementeren van de nodige risicobeheersmaatregelen. Dit kan door middel van de uitvoering van risicobeoordelingen en het nemen van passende actie. Ze houden hierbij rekening met factoren zoals prioriteit, beschikbare middelen en de capaciteit om maatregelen effectief uit te voeren.

Opleidingen en bewustwording: Het organiseren en faciliteren van trainingen en bewustwordingscampagnes in afstemming met HR, CISO, PO en FG voor medewerkers binnen hun eenheden, gericht op risico's, beveiliging, en compliance. Dit draagt bij aan de vermindering van menselijke fouten en incidenten.

Verantwoordelijkheid voor toegangscontrole: De eenheidsmanagers zorgen ervoor dat toegangscontrole en de beveiliging van bedrijfsmiddelen en persoonsgegevens effectief worden uitgevoerd. Dit omvat het implementeren van passende toegangsbeperkingen en het monitoren van deze toegang.

Rapportage aan het directieteam: De eenheidsmanagers leveren regelmatige rapportages over de voortgang van de uitvoering van het beleid en de prestaties van hun eenheid. Ze rapporteren incidenten, risico's, en compliance status aan het directieteam (eventueel via de CISO).

Verantwoordelijkheid voor incidentrespons: In geval van een incident binnen hun eenheid zijn zij verantwoordelijk voor de implementatie van het incidentresponsplan en het coördineren van de eerste reactie.

Acties:

- Vertalen van strategische doelen naar operationele plannen binnen de eenheid.
- Leidinggeven aan de uitvoering van beveiligingsmaatregelen en risicobeheerprocessen.
- 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.
- Het laten organiseren van trainingen en bewustwordingscampagnes voor medewerkers en sturen op deelname.
- Rapporteren aan het directieteam over voortgang en incidenten.

3.3 CISO/PO Ondersteuning
De CISO is verantwoordelijk voor de coördinatie van informatiebeveiliging en de PO is verantwoordelijk voor de coördinatie van de privacybescherming.

Zij ondersteunen de bestuurder en moeten gevraagd en ongevraagd advies kunnen geven aan de bestuurder.

- Zij vertalen wetgeving en bedrijfsdoelstellingen naar dit (integraal) Strategisch informatie- en privacy-beleid.
- Zij rapporteren aan het College van B&W hoe het afdelingsmanagement informatiebeveiliging en privacy implementeert en op welke wijze wordt voldaan aan dit beleid en de onderliggende wetgeving, zodat het College van B&W geïnformeerde besluiten kan nemen over de behandeling van informatiebeveiliging- en privacy risico's.

3.4 Controle en Verantwoording: Auditing en Compliance
Audits en evaluaties: De concerncontroller is verantwoordelijk voor het uitvoeren van regelmatige audits om te controleren of het IB&P-beleid effectief wordt uitgevoerd. Ze voeren ook evaluaties uit om te garanderen dat de eenheden voldoen aan de vereisten van het beleid en de wet- en regelgeving.

Monitoren van naleving: De concerncontroller ziet erop toe dat het beleid in alle afdelingen en processen wordt nageleefd. Dit omvat het monitoren van compliance met beveiligingsmaatregelen, gegevensbeschermingsvereisten, en toegangscontrolemaatregelen.

Rapportages en aanbevelingen: De concerncontroller maakt gedetailleerde rapporten van diens bevindingen, inclusief aanbevelingen voor verbetering. Hij/zij rapporteert rechtstreeks aan het directieteam en kan ook betrokken zijn bij de communicatie met externe auditors.

Verantwoordelijkheid voor het incidentbeheer: In geval van ernstige incidenten of een nalevingsprobleem, zorgt de controlefunctie voor het initiëren van een grondig onderzoek en voor het opstellen van verbeterplannen.

Verantwoordelijkheid voor documentatie: Zorgdragen voor de correcte documentatie van alle compliance en controle activiteiten, inclusief incidentrapportages, evaluaties, en auditresultaten.

Acties:

- Uitvoeren van interne audits en compliancebeoordelingen.
- Rapporteren van controleresultaten aan het directieteam en aanbevelingen doen voor verbetering.
- Verifiëren of risicobeheersmaatregelen en controles daadwerkelijk effectief zijn.
- Evalueren van incidenten en het aanbevelen van corrigerende maatregelen.

3.4.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat er een ENSIA-coördinator moet zijn. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke eenheidssmanagers. De eenheidsmanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging en privacybescherming komt als eigen verklaring in het jaarverslag tot uitdrukking onder de kop bedrijfsvoering en is gebaseerd op een extract van de collegeverklaring Informatiebeveiliging en privacy. Deze verklaring noemt men ook wel een 'In Control verklaring' of ICV (Engels: In Control Statement). 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, Cbw, DigiD-audit en Suwi. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen in het komende jaar. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad voor de zogenaamde horizontale verantwoording.

3.4.2 Wpg

De gemeente verwerkt in het kader van haar handhavingstaken politiegegevens als bedoeld in de Wet politiegegevens (Wpg). Op grond van artikel 33 Wpg wordt minimaal eens per drie jaar een onafhankelijke audit uitgevoerd naar de naleving van deze wet en het bijbehorende Besluit politiegegevens.

De audit richt zich op de werking en effectiviteit van de getroffen maatregelen voor beveiliging, rechtmatigheid, logging, bewaartermijnen en toegangsbeheer binnen de processen waarin politiegegevens worden verwerkt. De uitkomsten van de audit worden besproken binnen het college van B&W en vormen input voor het continu verbeteren van de informatiebeveiliging en privacybescherming.

De uitvoering en opvolging van de Wpg-audit worden afgestemd vanuit de interne auditfunctie met de Privacy Officer, zodat bevindingen worden meegenomen in de bredere PDCA-cyclus van het gemeentelijke informatiebeveiligingsbeleid (BIO2). De resultaten en verbetermaatregelen worden verwerkt in het jaarlijkse informatiebeveiligingsplan.

Belangrijke uitgangspunten:

- De Privacy Officer vervult de rol van bevoegde functionaris zoals beschreven in Wpg artikel 6, lid 7.
- Wpg artikel 13-verwerkingen vinden niet plaats binnen onze gemeente.
- In de uitvoering van de Wpg-taken worden geen politiegegevens gedeeld met derde landen.

Aldus vastgesteld in de vergadering van het college van burgemeester en wethouders van de gemeente Wassenaar op dinsdag 12 mei 2026.

drs. A.P.A. Oostermeijer,
gemeentesecretaris

drs. L.A. de Lange,
burgemeester