Gemeente REIMERSWAAL
GEMEENTEBLAD
Officiële uitgave van de gemeente Reimerswaal
Nr. 102030
5 maart
2026

Strategisch Gemeentelijk Informatiebeveiligings- en privacy beleid gemeente Reimerswaal 2025-2028

1. Inleiding

Deze beleidsnota beschrijft het Strategisch Gemeentelijk Informatiebeveiligings- en Privacy beleid (IB&P beleid) voor de jaren 2025 tot 2028 en vervangt het in 2021 vastgestelde 'Informatiebeveiligingsbeleid 2021 tot 2024'.

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligings- en Privacy beleid 2025-2028' zet de gemeente een volgende stap om de beveiliging van gegevens en systemen 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 Baseline Informatiebeveiliging Overheid versie 2 (BIO2). Deze herziene versie van de BIO is wettelijk verankerd via de Cyberbeveiligingswet (vertaling NIS2) en verplicht overheidsinstanties te voldoen aan de zorgplicht op het gebied van informatiebeveiliging.

De BIO2 legt de nadruk op risicomanagement. De rol van het college en afdelingshoofden is ten aanzien van risicomanagement explicieter dan voorheen. Om daaraan invulling te geven worden tegelijkertijd met de BIO2 de '10 bestuurlijke principes voor informatiebeveiliging' opgenomen in het informatiebeveiligingsbeleid. Deze principes ondersteunt het college en afdelingshoofden bij de invulling van hun verantwoordelijkheid.

Door de toenemende afhankelijkheid van Clouddiensten zijn in dit beleid ook de aanbevelingen verwerkt van het Centrum Informatiebeveiliging en Privacybescherming (CIP) met betrekking tot deze diensten.

De gemeente Reimerswaal heeft op basis van een stappenplan de voorwaarden en verplichtingen van de Algemene Verordening Gegevensbescherming (AVG) ingevoerd. Op de Privacypagina op de website van de gemeente Reimerswaal is weergegeven op welke wijze de gemeente Reimerswaal omgaat met de privacy van haar inwoners en andere betrokkenen en worden de rechten die betrokkenen hebben nader toegelicht. Dit privacy beleid is als apart beleidsdocument uitgewerkt.

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. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligings- en privacy plan (vastgesteld door de college) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingshoofden, de CISO, de privacy functionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD, de uitkomsten van zelf evaluaties (waaronder ENSIA), DPIA's en de 'Agenda Digitale Veiligheid 2028' van de VNG. Daarin staan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid wordt 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, vertrouwelijkheid en controleerbaarheid van (persoons)gegevens en andere informatie. De informatie moet niet alleen beschikbaar zijn maar ook beschermd worden voor onbevoegd gebruik en niet manipuleerbaar zijn.

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, inwoners, gasten, bezoekers en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)
De gemeente werkt met (persoons)gegevens. 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.

Bij de omgang met persoonsgegevens 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.

1.4 Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy
De gemeente Reimerswaal streeft naar een betrouwbare en toekomstbestendige digitale dienstverlening waarbij de privacy van onze inwoners, bedrijven en organisaties wordt gewaarborgd. Wij zetten ons in om informatiebeveiliging te verankeren in al onze processen, met respect voor onze kernwaarden: betrouwbaar, flexibel, daadkrachtig en eerlijk. Wij zien het beschermen van onze gegevens als een essentieel onderdeel van onze maatschappelijke verantwoordelijkheid en als fundament voor het vertrouwen dat onze inwoners in ons stellen.

Onze ambitie is om in 2025 te starten met risicogericht werken en proactief te anticiperen op kwetsbaarheden en bedreigingen voor informatiebeveiliging. We werken beveiligingsmaatregelen uit conform de Baseline Informatiebeveiliging Overheid versie 2 (BIO2), om de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van gegevens en systemen te gegaranderen. Hiermee willen wij onze verantwoordelijkheid tonen op het gebied van privacybescherming en informatiebeveiliging, waarbij onze digitale processen veilig, transparant en betrouwbaar zijn.

De uitwerking van de beveiligingsmaatregelen resulteert in de opzet van een ‘Information Security Management System’. Dit ISMS bestaat uit een samenhangend geheel van beleid, procedures, activiteiten en verantwoordelijkheden die ervoor zorgen dat informatie en informatiesystemen effectief worden beheerd en beschermd.

2. Strategisch beleid
2.1 Doel
Het doel van deze beleidsnota is het presenteren van het ‘Strategisch Gemeentelijk Informatiebeveiligings- en Privacy beleid voor de jaren 2025 tot 2028’. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligings- en privacyplan (IB&P-P).

Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het college, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

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

2.2.1 De BIO2
De BIO2 (Baseline Informatiebeveiliging Overheid versie 2) is het normenkader voor de gehele overheid.

De BIO2 is een doorontwikkeling van de BIO 1.04. In deze nieuwe versie zijn enkele belangrijke veranderingen doorgevoerd:
- Het principe van de basis beveiligingsniveaus (BBN’s) is losgelaten. De BIO2 hanteert een risico gebaseerde aanpak;
- Het inrichten van een Information Security Management System (ISMS) volgens de ISO 27001–norm wordt verplicht gesteld;
- De indeling van de controls/beheersmaatregelen en overheidsmaatregelen sluit aan bij vernieuwde indeling van de ISO 27002.

Voor de afdelingshoofden bekent dit dat zij nu meer dan vroeger moeten werken volgens een risico gebaseerde aanpak. 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, vertrouwelijkheid en controleerbaarheid.

2.2.2 Cyberbeveiligingswet (NIS2-richtlijn)

De Cyberbeveiligingswet bevat een zorgplicht die organisaties verplicht zelf een risicoanalyse uit te voeren. Op basis daarvan nemen zij passende en evenredige maatregelen voor de beveiliging van hun netwerk- en informatiesystemen. Het college moet de maatregelen goedkeuren en toezicht houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen. Dit wordt in het jaarlijks op te stellen jaarplan verder uitgewerkt.

2.2.3 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Reimerswaal is zich hiervan bewust en heeft met aanvullend 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 heeft de gemeente beleid en samenhangende procedures ingeregeld.

2.2.5 De 10 bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes voor informatiebeveiliging zijn een aanvulling op het normenkader BIO2 en gaan over de waarden die het college en de directie zichzelf oplegt. De principes zijn als volgt:

1. Het college bevordert 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 college controleert en evalueert.

De principes gaan vooral over de rol van het college 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 o.a. inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de collegetafel.

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. Uit dit dreigingsbeeld komt duidelijk naar voren dat gemeenten moeten blijven investeren in bewustwording, technologie en samenwerking.

2.2.7 Agenda Digitale Veiligheid 2028 van de VNG

Het doel van deze agenda is om de digitale veiligheid van gemeentelijke dienstverlening én de digitale weerbaarheid van de inwoners en ondernemers te verbeteren. Voor de gemeente Reimerswaal betekent dit: voorbereiden op digitale ontwrichting en streven naar een robuuste informatiebeveiliging.

2.2.8 BIO Thema-uitwerking Clouddiensten van het CIP

Het document 'BIO Thema-uitwerking Clouddiensten' van het Centrum Informatiebeveiliging en privacybescherming (CIP) biedt de gemeente Reimerswaal aanvullende handvatten voor het veilig toepassen van Clouddiensten. Ook hier geldt dat aspecten van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid gewaarborgd moeten zijn in een informatielandschap waar de afhankelijkheid van Clouddiensten toeneemt. Het doel is de risico's bij het gebruik van Clouddiensten te minimaliseren.

2.2.9 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast de hierboven genoemde bronnen 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. Het systeem is verdeeld over twee registers: beveiligingsincidenten en datalekken. Over de afwikkeling van incidenten en datalekken wordt verslag uitgebracht aan de directie. De directie voert regie op de afwikkeling doormiddel van het periodiek overleg binnen de 'Regiegroep Informatieveiligheid Reimerswaal'.

2.3 Standaarden informatiebeveiliging
De Baseline Informatiebeveiliging Overheid versie 2 (BIO2) is een normenkader voor informatiebeveiliging dat is gebaseerd op de internationale standaarden ISO 27001 en ISO 27002. De BIO2 is van toepassing op alle overheidslagen in Nederland en zorgt voor een uniforme aanpak van informatiebeveiliging. De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO2.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor besturing van apparaten door middel van Proces Automatisering (PA). Het beveiligings- en privacybeleid van de gemeente is ook van toepassing op de bescherming van Proces Automatisering.

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 operationeel niveau.

Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Gemeentelijk Informatiebeveiligings- en privacyplan'.

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 wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met de 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.

Binnen deze scope vallen de volgende informatie en systemen met bijzondere aandacht:
- 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 eindverantwoordelijk 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 college, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. De directie en afdelingshoofden maken 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 gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB&P beleid van en voor de hele organisatie. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het IB&P beleid is in lijn met het algemene beleid van de 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 (persoons)gegevens.
- Het minimaliseren van risico's van menselijk gedrag.
- Het minimaliseren van risico's bij toepassing van Clouddiensten.
- 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 voorbereiden van de organisatie op digitale ontwrichting.
- Investeren in bewustwording, technologie en samenwerking op het gebied van informatiebeveiliging.
- 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 Reimerswaal 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 en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met het IB&P plan het fundament onder een betrouwbare informatievoorziening en privacy bescherming. In het IB&P jaarplan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. Het plan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in de incidentenregisters 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 informatiebeveiliging en privacy in de uitvoering van gemeentelijke processen vindt risicogestuurd plaats.

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.
- De directie stelt jaarlijks het IB&P plan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Via de 'Regiegroep Informatieveiligheid Reimerswaal' bewaakt en ondersteunt de directie de implementatie van het Informatiebeveiligings- en privacy beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het zaaksysteem.
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en ziet erop toe dat de afdelingshoofden 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 de directie, voorafgaand aan de P&C-gesprekken.
- 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.
- De directie en de afdelingshoofden stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de Functionaris Gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de Functionaris Gegevensbescherming.
- 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 afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingshoofden zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De afdelingshoofden 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.
- Afdelingshoofden 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 inzien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden voeren quickscans informatiebeveiliging uit op basis van de BIO2 en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen het afdelingshoofd en de medewerker.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB&P plan opgesteld onder leiding van de CISO, gebaseerd op:
  - Dit IB&P beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - Andere audit resultaten;
  - Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten van de IBD;
  - Onderwerpen uit Agenda Digitale Veiligheid 2028 van de VNG
  - Onderwerpen uit BIO Thema-uitwerking Clouddiensten van het CIP
  - Uitkomsten risico-analyses en DPIA's
  - De door de afdelingshoofden 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 wordt in overleg en alle redelijkheid financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende ‘Three Lines Model’ (eerder bekend als ‘Three Lines of Defense’). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO, security officers, PO) ondersteunt, adviseert, coördineert en controleert middels steekproeven of het lijnmanagement zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn worden de resultaten uit de tweede lijn en de bijbehorende adviezen in de Regiegroep Informatiebeveiliging Reimerswaal beoordeeld en waar nodig wordt actie genomen. Hier zit ook de ENSIA coördinator (CISO) aan tafel.

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 afdelingshoofd. De directie zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouder 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.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen 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 Reimerswaal gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: afdelingshoofden
Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle afdelingshoofden. 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 minimaal 1 eigenaar hebben; er moet dus iemand verantwoordelijk zijn. Afdelingshoofden rapporteren aan de Regiegroep informatiebeveiliging 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 leidinggevenden overleg.

Taken van de afdelingshoofden 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 uitdragen van het IB&P beleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO en PO 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 Reimerswaal. Het college en directie van de gemeente Reimerswaal zullen werken volgens de 10 bestuurlijke 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.

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan de portefeuillehouder. De directie rapporteert daarnaast over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend of een uitwerking zijn van dit strategische beleid.

3.3.1 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Hiervoor is een ENSIA-coördinator aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingshoofden en

gemeenschappelijke regelingen (indien van toepassing). De afdelingshoofden leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

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 en 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 (ENSIA) vormt de basis voor het opstellen van de collegeverklaring aan de raad.

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

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

Vastgesteld op : 4 december 2025 door het college van de gemeente Reimerswaal