Gemeente Scherpenzeel

GEMEENTEBLAD

Officiële uitgave van de gemeente Scherpenzeel

Nr. 239525

22 mei 2026

# Strategisch informatiebeveiligings- en privacybeleid

## 1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacybeleid (IB&P beleid). Het vervangt het in 2021 vastgestelde 'Strategisch gemeentebreed Informatiebeveiligingsbeleid 2021' en de in 2018 vastgestelde 'Beleidsregels Privacy gemeente Scherpenzeel 2018'.

### 1.1 Doel

Het IB&P-beleid zorgt voor transparantie en vertrouwen en intern geeft het richting voor verdere invulling op tactisch en operationeel niveau. Het geeft ook invulling aan onze (wettelijke) verplichting voor een gegevensbeschermingsbeleid[1] en een informatiebeveiligingsbeleid[2].

Het IB&P-beleid ondersteunt in het realiseren van de organisatiedoelen en is uitgangspunt voor:

- het passend beheersen van IB&P-risico's voor betrokkenen en de organisatie.
- het verhogen van de (digitale) weerbaarheid.
- het voldoen aan normen en wet- en regelgeving (zie 1.4 en 1.5).

Dit beleid wordt jaarlijks geëvalueerd en indien nodig geactualiseerd.

### 1.2 Opbouw

Het strategisch IB&P-beleid vormt een onlosmakelijk geheel met de kaders op tactisch en operationeel niveau. De opbouw bestaat uit:

A. Strategisch niveau: dit IB&P-beleid.
B. Tactisch niveau: specifieke beleidskaders en normen.
C. Operationeel niveau:
    - plannen met verbeteringen en maatregelen.
    - werkinstructies, procedures en standaarden.

### 1.3 Scope

De scope van het strategische IB&P-beleid is:

- De gemeenteraad, het college van burgemeester en wethouders (hierna college), burgemeester en alle medewerkers (intern, extern, vast en tijdelijk), inwoners, gasten, bezoekers en externe relaties.
- Alle taken en processen binnen de gemeente.
- Systemen die worden gebruikt binnen de gemeente. Hieronder vallen ook de Proces Automatiseringssystemen (PA) die van de gemeente zijn en worden gebruikt binnen de gemeentelijke gebouwen en in de publieke ruimte, zoals gebouwbeheersingssystemen, cameratechnologie, pompen en gemalen.
- Locaties, ruimten en apparatuur die worden gebruikt waar(op) (persoons)gegevens worden verwerkt.
- Opdrachten, contracten of samenwerkingen met (keten)partners.

### 1.4 Wat is informatiebeveiliging?

Informatiebeveiliging is het treffen en onderhouden van maatregelen om de benodigde beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te garanderen.

- Beschikbaarheid: het garanderen van de benodigde beschikbaarheid van processen of gegevens (in een systeem).
- Integriteit: de mate waarin gegevens juist, volledig en actueel moeten zijn.
- Vertrouwelijkheid: de mate waarin gegevens beschermd moeten worden tegen kennisname en mutatie door onbevoegden.

Kaders

Binnen de overheid is afgesproken om aan de Baseline Informatiebeveiliging Overheid (BIO)[3] te voldoen. De BIO is gebaseerd op de ISO 27001 en 27002. De ISO27001 is een norm voor managementsystemen

1) Artikel 24.2 AVG en 4a Wpg
2) Norm 5 Baseline informatiebeveiliging Overheid (BIO)
3) Baseline Informatiebeveiliging Overheid

voor informatiebeveiliging. De ISO27002 is een richtlijn met informatiebeveiligingsmaatregelen als verdieping op de ISO27001.

De Network and Information Security Directive (NIS2-richtlijn) is bedoeld om de informatiebeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. Het is een Europese richtlijn die wordt omgezet naar Nederlandse wetgeving. Deze Cyberbeveiligingswet treedt waarschijnlijk in 2025 in werking. Organisaties die aan deze wet moeten voldoen (essentiële diensten, waaronder overheden) hebben straks een registratieplicht, meldplicht en zorgplicht. Een onafhankelijke toezichthouder gaat toezicht houden op naleving van de NIS2-richtlijn.

De BIO wordt herzien naar BIO 2.0. Hierin wordt de Cyberbeveiligingswet verwerkt.

### 1.5 Wat is privacy?

Iedereen heeft 'recht op de eerbiediging van de persoonlijke levenssfeer'. Dit is een grondrecht[4]. Hieronder valt het huis, briefwisseling, communicatie, innerlijke leven, lichamelijke integriteit, niet te worden bespied of afgeluisterd en het recht op een zorgvuldige behandeling van persoonsgegevens.

Kaders
Een zorgvuldige behandeling van persoonsgegevens is uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG). Dit is Europese wetgeving. In Nederland staan aanvullende voorwaarden in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Het college van B&W heeft buitengewoon opsporingsambtenaren (boa's) in dienst. De boa's hebben zowel toezichts- als opsporingstaken. Binnen de toezichtstaken worden persoonsgegevens verwerkt, waarop de AVG van toepassing is. Binnen de opsporingstaken worden politiegegevens verwerkt. Dit zijn persoonsgegevens die nodig zijn voor voorkoming en opsporing van strafbare feiten. Waar in dit beleid 'persoonsgegevens' staat, worden ook politiegegevens bedoeld.

Op politiegegevens is de Europese Richtlijn gegevensbescherming politie & justitie van toepassing. Deze richtlijn is in Nederland voor boa-organisaties onder meer geïmplementeerd in de volgende wetgeving:
- Wet politiegegevens (Wpg)
- Besluit politiegegevens (Bpg)
- Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpgboa)
- Beleidsregel Buitengewoon opsporingsambtenaar
- Regeling periodieke audit politiegegevens

## 2. IB&P risico's

Met de steeds geavanceerdere technologieën zoals kunstmatige intelligentie en de toename van cyberaanvallen, is het passend beheersen van de IB&P-risico's voor inwoners, medewerkers, ondernemers, andere belanghebbenden en de organisatie van cruciaal belang.

### 2.1 Risico's voor betrokkenen
Het onzorgvuldig omgaan met gegevens en systemen kan enorme gevolgen hebben voor betrokkenen. Denk aan een inbreuk op het grondrecht privacy of slachtoffer worden van digitale criminaliteit. Dit kan de volgende gevolgen hebben:
- Reputatieschade: Het imago van zowel individuen als de gemeente kan worden aangetast.
- Financiële schade: Door bijvoorbeeld afpersing, identiteitsfraude of boetes.
- Emotionele schade: Angst, stress en het gevoel van controleverlies.
- Gevoel van constante surveillance: Bij onrechtmatige tracking of monitoring.
- Uitsluiting en discriminatie: Bijvoorbeeld door algoritmische vooroordelen.
- Onjuiste besluitvorming: Als gevolg van foutieve of onvolledig verwerkte data.

Het niet beschikbaar zijn van systemen, dienstverlening en/of bedrijfsvoering kan de organisatie stil leggen. De gevolgen voor (de veiligheid van) inwoners, medewerkers, ondernemers, andere belanghebbenden, kunnen groot zijn en nog veel groter ten tijde van een crisissituatie.

### 2.2 Risico's voor de organisatie
Het onvoldoende borgen van informatiebeveiliging en privacy kan leiden tot:
- uitval van systemen, dienstverlening en bedrijfsvoering.

4) Artikel 10 grondwet

- incidenten zoals digitale criminaliteit en datalekken.
- personen kunnen schadevergoeding[5] eisen als er schade is omdat de organisatie verwijtbaar in strijd met de privacywetgeving heeft gehandeld.
- onder verscherpt toezicht worden gesteld door de Autoriteit Persoonsgegevens[6] en sancties opgelegd krijgen. De belangrijkste sancties zijn de boete, de last onder dwangsom, het verwerkingsverbod, de berisping en de waarschuwing.

De gevolgen kunnen hoge (herstel)kosten, impact op de capaciteit, reputatieschade en verlies van vertrouwen in de organisatie zijn. Het niet beschikbaar zijn van systemen, dienstverlening en/of bedrijfsvoering heeft impact op inwoners, ondernemers, andere belanghebbenden en medewerkers omdat ze hun werk niet of minder goed kunnen doen.

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[7] onderbouwt de hierboven beschreven risico's. Het geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst.

## 3. Visie en ambitie

### 3.1 Visie

De gemeente Scherpenzeel waarborgt niet alleen de continuïteit van haar bedrijfsvoering en dienstverlening maar beheerst de IB&P-risico's op een passende wijze. Betrokkenen kunnen erop vertrouwen dat de gemeente Scherpenzeel zorgvuldig en veilig met gegevens omgaat.

Dit betekent dat de Gemeente Scherpenzeel de noodzakelijke maatregelen treft om de risico's[8] te beheersen, dat zij hierop monitort en dat zij waar nodig bijstuurt. Het bestuur en management vervult hierin een voorbeeldfunctie en stelt de benodigde middelen en capaciteit beschikbaar.

### 3.2 Ambitie

De gemeente Scherpenzeel streeft ernaar om in 2027 volledig in control te zijn op de naleving de IB&P-kaders[9]. Dat betekent dat we grote stappen zetten in het zorgvuldig en veilig omgaan met gegevens, zodat onze inwoners, medewerkers, ondernemers en andere belanghebbenden kunnen rekenen op veilige en betrouwbare diensten.

We zorgen voor het planmatig inrichten en borgen van IB&P-maatregelen. Deze maatregelen zijn onderverdeeld naar vijf pijlers en beschreven in de volgende hoofdstukken:

1. Beleid en organisatie
2. Kennis en bewustzijn
3. Privacy-instrumenten
4. Informatiebeveiliging
5. Monitoring

De processen of gegevens (in een systeem) waar de risico's hoog zijn, krijgen prioriteit. De risico's zijn in ieder geval hoog als deze processen of gegevens:

- (deels) niet beschikbaar, integer (juist, volledig, actueel), vertrouwelijk zijn (toegankelijk voor onbevoegden) en de gevolgen voor inwoners, ondernemers, de gemeentelijke organisatie en andere belanghebbenden groot kunnen zijn.
- gevoelige, bijzondere- strafrechtelijke persoonsgegevens of politiegegevens van een grotere groep personen bevatten[10].

Op basis van de 'Plan-Do-Check-Act cyclus' zorgen we dat we blijvend voldoen (in control zijn) aan de IB&P-kaders, door te blijven evalueren en verbeteren.

### 3.3 IB&P-principes en beginselen

Bestuurders en managers hebben een belangrijke rol bij het borgen van IB&P in de organisatie. Als er iets misgaat op het gebied van IB&P, kan dit gevolgen hebben voor inwoners, ondernemers, de gemeentelijke organisatie en andere belanghebbenden.

5) Artikel 82 AVG en 31c Wpg
6) Landelijke toezichthouder persoonsgegevens
7) Producten - Informatiebeveiligingsdienst
8) Zie hoofdstuk 2
9) Zie paragraaf 1.4 en 1.5
10) Artikel 9, 10 AVG, artikel 1 Wpg

Daarom geven bestuurders en managers richting en sturing aan IB&P volgens onderstaande **principes**[11]:
- Bestuurders en managers bevorderen een veilige cultuur.
- Informatiebeveiliging en privacy is van iedereen.
- Informatiebeveiliging en privacy is risicomanagement.
- Risicomanagement is onderdeel van de besluitvorming.
- Informatiebeveiliging en privacy behoeft ook aandacht in (keten)samenwerking.
- Informatiebeveiliging en privacy is een proces.
- Informatiebeveiliging en privacy kosten geld.
- Verbetering komt voort uit leren en ervaring.
- Het bestuur controleert en evalueert.

Daarnaast past elke medewerker de **beginselen**[12] toe:
1. Wij verwerken persoonsgegevens rechtmatig, behoorlijk en transparant.
2. Wij verwerken persoonsgegevens binnen een vooraf welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel.
3. Wij verwerken persoonsgegevens als ze toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor het vooraf bepaalde doel.
4. Wij zorgen dat (persoons)gegevens juist zijn op het moment dat we ze gebruiken.
5. Wij verwijderen (persoons)gegevens zodra ze niet meer nodig zijn.
6. Wij treffen passende maatregelen om (persoons)gegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

## 4. Beleid en organisatie

### 4.1 Beleid

Beleidsdocumenten zorgen voor transparantie en vertrouwen richting betrokkenen en het geeft de organisatie richting om IB&P op een juiste manier toe te passen.

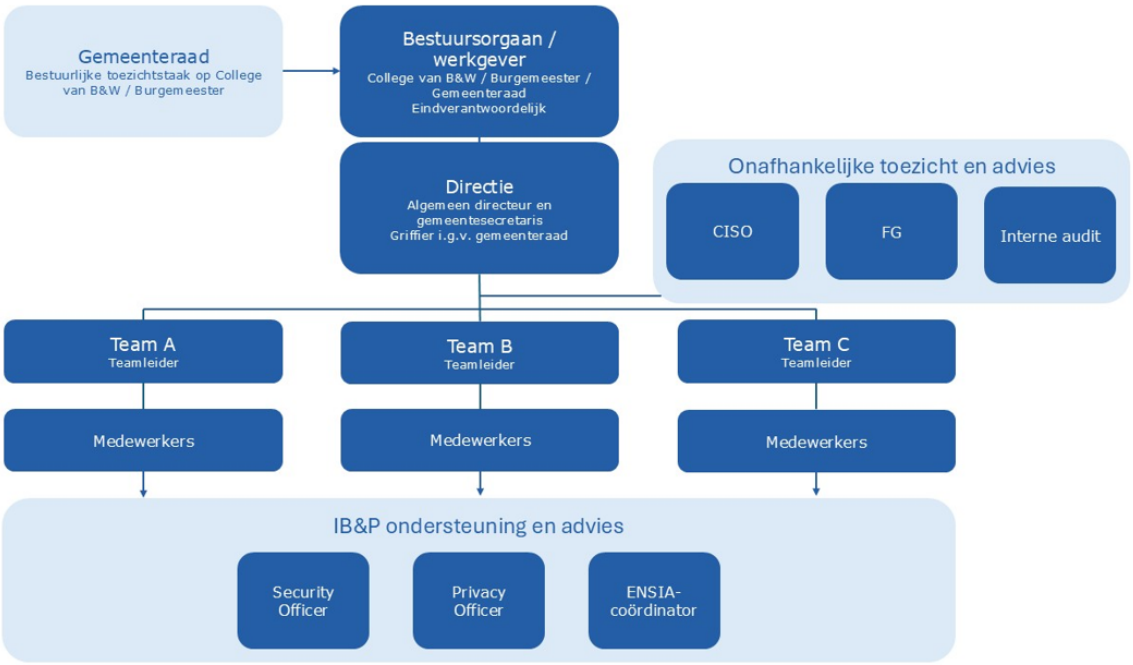
Naast dit strategische IB&P-beleid zorgen we voor:
- vastgestelde specifieke beleidsdocumenten en kaders.
- heldere richtlijnen, werkinstructies, procedures en standaarden op operationeel niveau.
- een vastgesteld IB&P jaarplan op basis waarvan we risico gebaseerd maatregelen implementeren en continueren.
- het periodiek evalueren en indien nodig actualiseren van deze documenten.

### 4.2 Organisatie

De kaders zijn complex en veranderen voortdurend en de risico's zijn hoog. Om de organisatie te adviseren en ondersteunen bij het implementeren van de kaders en het in control blijven, zijn voldoende en kundige medewerkers nodig. Ook is betrokkenheid en sturing van bestuurders en management essentieel.

We zorgen daarom voor een functionerende IB&P-organisatie met duidelijke rollen, taken en verantwoordelijkheden. Onderstaande afbeelding geeft schematisch weer hoe de rollen en verantwoordelijkheden op gebied van IB&P zich tot elkaar verhouden (dit is geen hiërarchisch organogram).

11) We volgen de-10-bestuurlijke-principes-voor 20190109.pdf (vng.nl) van de VNG, aangevuld met privacy.
12) Artikel 5 lid 1 AVG en 3, 4, 4a en b Wpg




* Deze rollen, taken en verantwoordelijkheden zijn uitgewerkt in bijlage 1.

## 5. Kennis en bewustzijn

Medewerkers zijn een belangrijke schakel bij informatiebeveiliging en privacy. We zorgen daarom voor een goed kennisniveau en bewustzijn van IB&P onder medewerkers door:

- het planmatig aanbieden van activiteiten, trainingen, workshops.
- een kennisbank met IB&P-informatie.
- een IB&P-introductie voor nieuwe medewerkers.
- IB&P-richtlijnen waar medewerkers zich aan moeten houden.

Op regelmatige basis wordt het niveau van kennis en bewustzijn gemeten, op basis waarvan het IB&P kennis- en bewustzijnsplan opgesteld of aangescherpt wordt.

## 6. Privacy-instrumenten

In de privacywetgeving zijn een aantal instrumenten verplicht gesteld die bijdragen aan een zorgvuldige behandeling met persoonsgegevens:

### 6.1 Register van verwerkingsactiviteiten[13]

We houden een register van verwerkingsactiviteiten bij met alle verwerkingen van persoonsgegevens door de organisatie. Per verwerking (proces) staat hierin: het doel, de categorieën van betrokkenen, de categorieën persoonsgegevens, derden ontvangers, bewaartermijn en beveiligingsmaatregelen.

### 6.2 DPIA[14]

We voeren planmatig Data Protection Impact Assessments (DPIA) uit voor verwerkingen van persoonsgegevens die een hoog risico betekenen voor de rechten en vrijheden van een persoon. Een DPIA is een uitgebreid onderzoek naar risico's en maatregelen die vooraf moet worden uitgevoerd. Het geeft antwoord op vragen als: mag het, wat is noodzakelijk, met wie deel ik, is het goed beveiligd en bewaren we niet langer dan nodig. Waar nodig zorgen we dat verbeteringen worden getroffen.

### 6.3 Gegevensbescherming door ontwerp en standaard instellingen[15]

Bij veranderingen en vernieuwingen zorgen we voor een projectmatige aanpak, waarbij vanaf de ontwerpfase een zorgvuldige en veilige behandeling van persoonsgegevens wordt meegenomen. Denk

13 )Artikel 30 AVG en 31d Wpg
14 )Artikel 35 AVG en 4c Wpg
15 )Artikel 25 AVG en 4a en b Wpg, ook wel privacy by design en privacy by default.

aan minimaal gebruik van persoonsgegevens en een passende bescherming. Standaardinstellingen zijn zo gekozen dat dit maximaal wordt geborgd.

### 6.4 Privacyafspraken met derden

Als we persoonsgegevens uitwisselen met andere partijen of ze verwerken in opdracht van of in samenwerking met ons persoonsgegevens:

- stellen we eisen op gebied van gegevensbescherming in de inkoopprocedure.
- leggen we afspraken over gegevensbescherming vast in een overeenkomst. Bijvoorbeeld in een:
  - hoofd- en verwerkersovereenkomst als een organisatie een opdrachtnemer en verwerker[16] is. Een verwerker verwerkt persoonsgegevens namens, in opdracht en volgens instructie van onze organisatie als verwerkingsverantwoordelijke[17] uit.
  - convenant of samenwerkingsovereenkomst als we samenwerken met organisaties als (gezamenlijke) verwerkingsverantwoordelijke[18].
  - gegevensleveringsovereenkomst als persoonsgegevens worden uitgewisseld en partijen verder verwerken onder een eigen verwerkingsverantwoordelijkheid. Hierin staan afspraken over een veilige manier van overdragen en moment van overgaan van de verwerkingsverantwoordelijkheid.
- als afspraken in lopende contracten ontbreken, zorgen we dat deze afspraken met terugwerkende kracht worden gemaakt.
- monitoren we dat afspraken op gebied van privacy en gegevensbescherming worden nagekomen.

### 6.5 Datalekken[19]

Bij een datalek zijn persoonsgegevens onterecht vernietigd of verloren gegaan, veranderd, gedeeld of toegankelijk geweest voor anderen. We registreren datalekken in een intern datalekkenregister, melden ernstige datalekken binnen 72 uur bij de Autoriteit Persoonsgegevens en informeren waar nodig de betrokkenen over het datalek. Er zijn procedures, richtlijnen en formats voor de behandeling van datalekken.

### 6.6 Rechten van betrokkenen[20]

We zorgen dat betrokkenen invulling kunnen geven aan hun rechten om controle te houden op hun persoonsgegevens. Denk aan het recht op informatie, inzage, aanpassing, verwijdering en bezwaar.

In de privacyverklaring en cookieverklaring op onze websites geven we invulling aan onze actieve plicht om personen vooraf in duidelijke en eenvoudige taal te informeren over de verwerking van persoonsgegevens en hun rechten. Verdere invulling aan de informatieplicht wordt per proces bepaald.

Om gebruik te maken van deze rechten kunnen personen een verzoek indienen. Op de website geven we personen duidelijke informatie over hun rechten en hoe ze hier gebruik van kunnen maken. Intern zorgen we voor procedures, richtlijnen en formats voor de behandeling van verzoeken.

## 7. Informatiebeveiliging

### 7.1 Informatiebeveiligingsnorm

Om de benodigde beschikbaarheid, integriteit en vertrouwelijkheid van gegevens, en daarmee de continuïteit van onze dienstverlening en bedrijfsvoering, te garanderen, voldoet de gemeente Scherpenzeel aan de Baseline Informatiebeveiliging Overheid[21]. Binnen de overheid is afgesproken om aan dit normenkader te voldoen. De BIO is gebaseerd op de ISO 27001 en 27002.

In de privacywetgeving is verplicht gesteld dat organisaties zorgen voor passende technische en organisatorische informatiebeveiligingsmaatregelen[22]. Door aan deze beveiligingsnorm te voldoen en de privacy-instrumenten in hoofdstuk 6 toe te passen, geven we hier invulling aan.

Jaarlijks onderzoeken we aantoonbaar in hoeverre we voldoen aan de BIO. Waar nodig treffen we planmatig verbeteringen.

16) Artikel 28 AVG en 6c Wpg
17) Artikel 4.7 en 24 AVG en 1.f Wpg
18) Artikel 26 AVG en 20 Wpg
**19) Artikel 33 en 34 AVG en 33a Wpg**
**20) Artikel 5, 12 t/m 22, 38.4 AVG en 24a tm 28 Wpg**
21) Baseline Informatiebeveiliging Overheid
22) Artikel 32 AVG en 4a Wpg

### 7.2 ICT Dienstverlening
De gemeente Veenendaal verzorgt de ICT voor de gemeente Scherpenzeel. Afspraken over IB&P zijn vastgelegd in een dienstverleningsovereenkomst (DVO) en een verwerkersovereenkomst.

### 7.3 Informatiebeveiliging in overeenkomsten
De beschikbaarheid, integriteit en/of vertrouwelijkheid van gegevens dient te worden gewaarborgd door andere partijen waarmee we samenwerken of die in opdracht van de gemeente diensten leveren. Dit doen we door:

- eisen op het gebied van informatiebeveiliging te stellen in de inkoopprocedure, bijvoorbeeld het voldoen aan normenkaders.
- afspraken over informatiebeveiliging vast te leggen in de overeenkomst, zoals afspraken over:
  - risico- en incidentmanagement
  - passende beveiligingsmaatregelen
  - periodieke penetratietesten op systemen of applicaties
  - continuïteitsmanagement
  - verantwoording door het periodiek overleggen van documentatie en/of certificaten
- ontbrekende afspraken in lopende contracten met terugwerkende kracht te maken.
- de naleving van afspraken te monitoren.

### 7.4 Systemen
Wij voeren op nieuwe systemen met hoge IB&P-risico's[23] een basisbeveiligingstoets uit. Op bestaande systemen wordt deze basisbeveiligingstoets om de drie jaar herhaald. Deze toets brengt in beeld of het systeem voldoet aan het benodigde beveiligingsniveau. Indien nodig zorgen we dat verbeteringen planmatig worden ingevoerd.

### 7.5 Beveiligingsincidenten
We zorgen dat medewerkers weten wat een beveiligingsincident is en dat zij deze melden bij een vermoeden. We registreren beveiligingsincidenten in een intern register en handelen volgens de vastgestelde specifieke procedure.

### 7.6 Bewaren en vernietigen
Gemeenten hebben een verplichting om gegevens te bewaren conform de Archiefwet. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk[24]. De Wet politiegegevens kent specifieke bewaartermijnen[25].

We zorgen voor het bepalen en toepassen van de bewaar- en vernietigingstermijnen van (persoons)gegevens. We zorgen ook dat medewerkers zich bewust zijn van de eigen verantwoordelijk om onnodige en meervoudige opslag te voorkomen in mailboxen en persoonlijke schijven.

### 7.7 Toegang tot gegevens
Om te zorgen dat medewerkers en derden alleen toegang hebben tot persoonsgegevens die noodzakelijk zijn voor de toegewezen werkzaamheden[26], treffen we de volgende maatregelen:

- Er is een vastgesteld toegangsbeleid met richtlijnen over het verlenen, wijzigen- en beëindigen van toegang tot politiegegevens.
- Voor risicovolle systemen is een autorisatiematrix vastgesteld.
- Medewerkers en derden krijgen alleen toegang tot gegevens conform het toegangsbeleid en de autorisatiematrix.
- Indien medewerkers en derden van functie veranderen of het dienstverband (of opdracht) eindigt, wordt de autorisatie conform het toegangsbeleid en de autorisatiematrix gewijzigd of beëindigd.

### 7.8 Loggen van gegevens
Handelingen (raadplegen, aanpassen en verwijderen) in de risicovolle systemen waarin (persoons)gegevens worden verwerkt, worden gelogd[27]. Het doel is dat herleidbaar is welke gegevens door wie en wanneer zijn geraadpleegd, aangepast of verwijderd. Dit is van belang om te kunnen voldoen aan de rechten van betrokkenen, vragen te beantwoorden of klachten te behandelen.

23) Zie paragraaf 3.2
24) Artikel 5 lid 1e AVG
25) Artikel 14 Wpg
26) Artikel 6 en 6a Wpg
27) Artikel 32a Wpg

## 8. Monitoring en evaluatie

Het is belangrijk dat de organisatie in control is en dat betrokkenen grip hebben op hun persoonsgegevens.

### 8.1 Interne controle en audits

We voeren planmatig en aantoonbaar periodieke IB&P-audits en controles uit. Met deze audits en controles monitoren we in hoeverre de organisatie in control is en betrokkenen grip hebben op hun persoonsgegevens. Indien nodig zorgen we dat verbeteringen planmatig worden ingevoerd.

In ieder geval de volgende interne audits en controles worden uitgevoerd:

- Periodieke controles zoals:
  - Rollen en rechten in risicovolle systemen.
  - Logging van handelingen in risicovolle systemen.
  - Rechtmatige behandeling van persoonsgegevens.
  - IB&P-afspraken in overeenkomsten.

- Zelfevaluatie (ENSIA)
  Wij verantwoorden ons over informatiebeveiliging via Eenduidige Normatiek Single Information Audit (ENSIA)[28] door een jaarlijkse zelfevaluatie, waarin we de informatiebeveiliging beoordelen aan de normen en eisen van:
  - De baseline Informatiebeveiliging Overheid (BIO)
  - De basisregistratie Personen (BRP)
  - De basisregistratie adressen en gebouwen (BAG)
  - De basisregistratie Grootschalige Topografie (BGT)
  - Basisregistratie ondergrond (BRO)
  - De paspoortuitvoeringsregeling Nederland (PUN)
  - Het systeem Suwinet van het ministerie van SZW, waarin UWV, SVB en gemeenten persoonsgegevens uitwisselen.
  - DigiD

- Jaarlijks beoordelen we op basis van het AVG Borgingsdocument in hoeverre de organisatie aan de privacywetgeving voldoet.
- Interne audit Wet politiegegevens

Jaarlijks voeren we de interne WPG-audit uit[29]. De resultaten van deze audit worden in een rapportage vastgelegd en aangeboden aan de verwerkingsverantwoordelijke.

### 8.2 Externe audits

We laten wettelijk verplichte audits uitvoeren door een onafhankelijke externe auditor. Dat zijn in ieder geval:

- Jaarlijks de audits (ENSIA) van DigiD en Suwinet. In een verklaring van het college leggen we verantwoording af over de informatiebeveiliging van Suwinet aan het ministerie van SZW en van DigiD aan Logius als onderdeel van het ministerie van BZK.
- Om de vier jaar de Wet politiegegevens. De rapportage van de externe auditor sturen we naar de Autoriteit Persoonsgegevens en de verwerkingsverantwoordelijke. Indien nodig zorgen we dat verbeteringen planmatig worden ingevoerd.

### 8.3 Rapporteren

Jaarlijks en indien nodig brengt de directie schriftelijk verslag uit aan het verantwoordelijke bestuursorgaan over de naleving van de IB&P-kaders. Dit rapport omvat de huidige status, voortgang en geplande verbeteringen op het gebied van IB&P. Met deze rapportages brengen we het verantwoordelijke bestuursorgaan in positie om invulling te geven aan hun verantwoordelijkheid en hierop te kunnen sturen.

In de cyclusdocumenten rapporteert het college aan de gemeenteraad over de plannen en naleving van de IB&P-kaders.

28) ENSIA is een verantwoordingsstelsel voor informatieveiligheid en is een initiatief van gemeenten en de ministeries van BZK en SZW.

29) Artikel 33 Wpg en Regeling periodieke audit politiegegevens

Elke teamleider rapporteert aan de directie over de naleving van de IB&P-kaders door het eigen team. De Chief Information Security Officer en functionaris gegevensbescherming brengen jaarlijks verslag uit aan de verantwoordelijke bestuursorganen[30].

## Ondertekening

Het onderhavige Strategisch informatiebeveiligings- en privacybeleid van de gemeente Scherpenzeel wordt vastgesteld ter vervanging van het Strategisch gemeentebreed Informatiebeveiligingsbeleid 2021 en de Beleidsregels Privacy gemeente Scherpenzeel 2018, die hiermee per datum van ondertekening worden ingetrokken.

*Vastgesteld door het college van burgemeester en wethouders van gemeente Scherpenzeel, in de vergadering van het college van burgemeester en wethouders op 11 november 2025:*

*R. 't Hoen*
*Secretaris*

*M.C. Teunissen-Willemsen*
*Burgemeester*

*Vastgesteld door de burgemeester van gemeente Scherpenzeel, in de vergadering van het college van burgemeester en wethouders op 11 november 2025:*

*M.C. Teunissen-Willemsen*
*Burgemeester*

30) Artikel 38.3 AVG, 36.4 Wpg

## Bijlage 1 – Rollen en verantwoordelijkheden IB&P

**Elke medewerker**
Binnen de eigen taken en verantwoordelijkheden draagt elke medewerkers bij aan IB&P. Dit betekent dat elke medewerker:
- zich bewust is van de IB&P-risico's.
- de beginselen in paragraaf 3.3 toepast.
- bekend is met en zich houdt aan dit IB&P-beleid en aanvullende procedures en richtlijnen.

**Bestuursorganen (college, burgemeester en gemeenteraad)**
Betrokkenheid van bestuurders is cruciaal. Het laat zien dat de organisatie IB&P serieus neemt en het een ambitie is om gegevens te beschermen. Elk bestuursorgaan:
- is eindverantwoordelijk voor IB&P[31].
- geeft richting en sturing aan IB&P en volgt hierin dit IB&P-beleid.
- stelt strategische IB&P-kaders vast, zoals dit beleid.
- legt rekenschap af over naleving van de IB&P-kaders aan de CISO en functionaris gegevensbescherming.

Het college en de burgemeester leggen verantwoording af over IB&P in de cyclusdocumenten aan de gemeenteraad vanuit de bestuursrechtelijke toezichtstaak.

**Gemeentesecretaris**
De gemeentesecretaris is tevens de algemeen directeur van de gemeentelijke organisatie. De gemeentesecretaris is verantwoordelijk voor IB&P in de ambtelijke organisatie. De gemeentesecretaris:
- stelt tactische IB&P-kaders vast.
- geeft richting en sturing aan IB&P en volgt hierin dit IB&P-beleid.
- zorgt dat het eigenaarschap, waaronder de IB&P-verantwoordelijkheid, van alle processen en systemen, is belegd bij een teamleider.
- zorgt dat teamleiders zich verantwoorden over IB&P.
- rapporteert over de naleving van IB&P-kaders aan (de verantwoordelijke portefeuillehouders binnen) het college van B&W.
- zorgt dat de privacy officer, security officer, CISO en functionaris gegevensbescherming naar behoren en tijdig worden betrokken bij risicovolle zaken op het gebied van IB&P.

**Teamleiders**
De teamleider is verantwoordelijk voor IB&P binnen het eigen team en de door de directie toegewezen processen en systemen. De teamleider:
- geeft richting en sturing aan IB&P en volgt hierin het IB&P-beleid.
- benoemt de IB&P-doelstellingen in het teamplan.
- zorgt voor het planmatig en risico gebaseerd implementeren en borgen van de maatregelen in dit beleid.
- rapporteert over de naleving van IB&P-kaders aan de directie.
- zorgt dat de privacy officer, security officer, CISO en functionaris gegevensbescherming naar behoren en tijdig worden betrokken bij risicovolle zaken op het gebied van IB&P.

**Security officer**
De security officer:
- stelt beleidsdocumenten op.
- adviseert over complexe informatiebeveiligingsvraagstukken.
- en de privacy officer werken samen en
  - zorgen voor een vastgesteld IB&P-jaarplan (zie paragraaf 4.1.).
  - coördineren en monitoren de uitvoering van het IB&P-jaarplan en implementeren acties waar nodig zelf.
  - rapporteren over de uitvoering van het IB&P-jaarplan aan de directie, Chief Information Security Officer en functionaris gegevensbescherming.
- adviseert, ondersteunt bij en monitort de IB(&P)-maatregelen in dit beleid.
- draagt actief bij aan IB&P kennis en bewustzijn (zie hoofdstuk 5)
- betrekt de privacy officer, CISO en functionaris gegevensbescherming naar behoren en tijdig bij risicovolle zaken op het gebied van IB&P.

**ENSIA-coördinator**

31) Elk bestuursorgaan is eindverantwoordelijke voor IB&P binnen de eigen taken. Voor persoonsgegevens heet dit in de wet 'verwerkingsverantwoordelijke': artikel 4.7 AVG en 1.f Wpg.

De ENSIA[32]-coordinator:
- coördineert de ENSIA-audit en alle bijbehorende werkzaamheden
- monitort de voortgang en zorgt voor tijdige aanlevering van informatie aan de auditor.
- begeleidt de externe audit.
- bewaakt deadlines.
- zorgt voor aanleveren van de verantwoordingsdocumenten bij de verschillende toezichthouders en ministeries via de ENSIA-tool.
- eerste aanspreekpunt binnen de organisatie en voor de (externe) auditor.
- zet vervolgacties uit op basis van de ENSIA-resultaten.
- zorgt voor de verklaring van het college.

**Privacy officer**
De privacy officer:
- stelt beleidsdocumenten op.
- adviseert over complexe privacyvraagstukken.
- en de security officer werken samen en
  - zorgen voor een vastgesteld IB&P-jaarplan volgens paragraaf 4.1.
  - coördineren en monitoren de uitvoering van het IB&P-jaarplan en implementeert acties waar nodig zelf.
  - rapporteren over de uitvoering van het IB&P-jaarplan aan de directie, CISO en functionaris gegevensbescherming.
- adviseert, ondersteunt bij en monitort de (IB&)P-maatregelen die volgen uit het IB&P-jaarplan.
- draagt actief bij aan IB&P kennis en bewustzijn (zie hoofdstuk 5)
- betrekt de security officer, CISO en functionaris gegevensbescherming naar behoren en tijdig bij risicovolle zaken op het gebied van IB&P.

**IB&P auditor**
De IB&P auditor:
- zorgt voor een vastgesteld auditplan volgens paragraaf 8.3.
- coördineert en monitort de uitvoering van audits en controles volgens het auditplan en voert waar nodig zelf audits en controles uit.
- zorgt dat audits en controles aantoonbaar worden vastgelegd in een rapportage van bevindingen en aan de verantwoordelijke manager worden voorgelegd.
- rapporteert over de uitvoering van het auditplan aan de directie, de Chief Information Security Officer en functionaris gegevensbescherming.
- ondersteunt en coördineert bij de externe audits in paragraaf 8.3.
- betrekt de CISO en functionaris gegevensbescherming naar behoren en tijdig bij risicovolle zaken op het gebied van IB&P.

Deze rol wordt binnen de gemeente Scherpenzeel ingevuld door onderverdeling van audittaken onder CISO, PO en systeem-/applicatiebeheer.

**Chief Information Security Officer (CISO)**
De CISO:
- houdt toezicht op de naleving van de IB(&P)-kaders.
- adviseert over en ontwikkelt IB-beleidsdocumenten.
- brengt verslag uit aan de bestuursorganen over de naleving van de IB(&P)-kaders.
- geeft advies bij beveiligingsincidenten.
- geeft advies op de IB(&P)-jaarplannen/ meerjarenplan.
- onderhoudt contact met (overheids)instanties en toezichthouders ten aanzien van informatiebeveiligingsaangelegenheden.
- draagt actief bij aan IB&P kennis en bewustzijn.

**De functionaris gegevensbescherming:**
De functionaris gegevensbescherming[33]:
- houdt toezicht op de naleving van de (IB&)P-kaders.
- informeert en adviseert over de verplichtingen in de (IB&)P-kaders.
- brengt verslag uit aan de verwerkingsverantwoordelijke over de naleving van de (IB&)P-kaders.
- geeft advies op privacyvraagstukken, uitgevoerde DPIA's en houdt toezicht op het opvolgen van dit advies.

32) Zie paragraaf 8.1 en 8.2
33) Artikel 37, 38, 39 AVG en 36 Wpg

- geeft advies bij (ernstige) datalekken.
- is direct benaderbaar voor betrokkenen over de verwerking van hun persoonsgegevens.
- werkt samen met en is contactpunt voor de Autoriteit Persoonsgegevens.
- draagt actief bij aan IB&P kennis en bewustzijn.