

GEMEENTE
MIDDEN-DELFLAND

2025 JAARVERSLAG INFORMATIEBEVEILIGING MIDDEN-DELFLAND

Inhoudsopgave

Managementsamenvatting 3
1. Inleiding 5
2. IB-beleid, doelstellingen en ambities 6
2.1. Wat is informatiebeveiliging? 6
2.2. Baseline Informatiebeveiliging Overheid (BIO) 6
2.3. Informatieveiligheid is geborgd in de organisatie 6
2.4. Uitgangpunten en doelen van ons informatiebeveiligingsbeleid 7
2.5. Relatie met privacy 8
3. ENSIA (Eenduidige Normatiek Single Information Audit) 9
3.1. Aanleiding 9
3.2. Uitvoering van ENSIA 2025 10
3.3. Verantwoordingsrapportages zelfevaluatie 2025 11
3.4. Resultaten zelfevaluaties per stelsel 12
3.4.1. Zelfevaluaties BRP en PUN 12
3.4.2. Zelfevaluatie basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO). 13
4. Collegeverklaring ENSIA inzake informatiebeveiliging Suwinet 15
5. Samenvattend beeld en resultaten informatiebeveiliging 2025 16
5.1. Achtergrond 16
5.2. Resultaat meting BIO 17
5.3. Algemene Verordening Gegevensbescherming (AVG) 18
6. Disclaimer 20
7. Realisatie doelstellingen IB-beleid 21
7.1. Controls & beheersmaatregelen IB 22
7.2. Jaarplan Informatiebeveiliging 2026 met verbeterpunten 23
7.3. Nieuwe wet- en regelgeving over informatiebeveiliging 27
8. Incidenten, ontdekte kwetsbaarheden en datalekken 29
8.1. Gemelde incidenten en kwetsbaarheden 29
8.2. Gemelde datalekken 29
9. Meerjarenperspectief 32
9.1. Grootste risico’s voor gemeenten 32
9.2. Dreigingsbeeld 2025 – 2026 33

Managementsamenvatting

Het College van B&W van gemeente Midden-Delfland legt jaarlijks verantwoording af over het informatiebeveiligingsbeleid. Dit jaarverslag Informatiebeveiliging Midden-Delfland 2025 bevat die verantwoording.

Het jaarverslag is gebaseerd op een actuele meting vanuit ons ISMS[1]. Deze meting is uitgevoerd op basis van de 112 normen zoals opgenomen in de Baseline Informatiebeveiliging Overheid (BIO). Hierin zijn ook de resultaten uit de Eenduidige Normatiek Single Information Audit (ENSIA) 2025 opgenomen. Deze meting heeft het karakter van een zelfevaluatie waarbij is nagegaan in hoeverre de gemeente voldoet aan de 112 normen uit de BIO.

De normen uit de BIO zijn vooral vanuit een generiek beeld beoordeeld en niet specifiek toegespitst op applicaties. In het jaarverslag houden we rekening met verbeterpunten die voortkomen uit de meting over de BIO, ENSIA 2025 en de DigiD/Suwinet-audit. De verbeterpunten met de hoogste risico's vormen het informatiebeveiliging jaarplan 2026.

Het College van B&W wordt verzocht het jaarverslag informatiebeveiliging 2024 vast te stellen en de CISO het mandaat te geven het jaarplan met verbeteracties uit te (laten) voeren.

Activiteiten in 2025

In 2025 is op het gebied van informatiebeveiliging het volgende gerealiseerd:

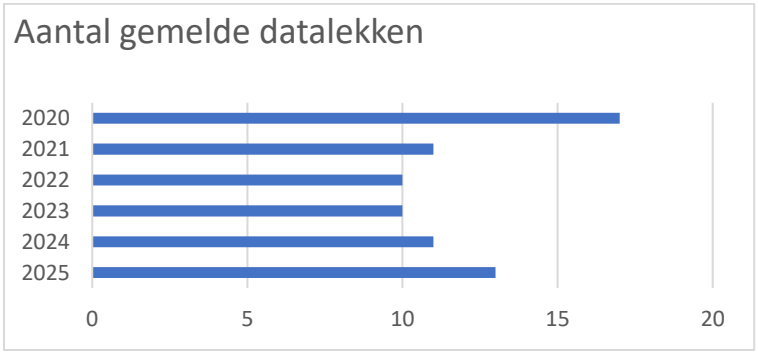
- Het Information Security Management System (ISMS) hebben we met taken verder uitgerold naar andere beheerders van applicaties om de plan-do-check-act cyclus voor informatiebeveiliging op een breder vlak structureel vorm te geven. Dit doen we gefaseerd en gaat in 2026 verder.
- We hebben AI-beleid opgesteld als leidraad voor het gebruik van AI toepassingen.
- We zijn gestart met het actualiseren ons dataclassificatie-overzicht en implementeren labelprocedures in de vakapplicaties, dit loopt door in 2026.
- We verbeterden het beheer van toegangsrechten binnen vakapplicaties, waarbij functioneel applicatiebeheerders een centrale rol krijgen.
- We planden een cybercrisisoefening die gericht is op het vergroten van bewustwording en het testen van beveiligingsmaatregelen. Dit is door vertrek van deelnemende medewerkers doorgeschoven naar 2026.
- We implementeerden een SIEM/SOC-systeem om kwetsbaarheden en beveiligingsincidenten vroegtijdig te signaleren en daarop te reageren.
- We werkten onze bedrijfscontinuïteitsplannen verder uit, met extra aandacht voor noodscenario's voor cruciale processen zoals burgerzaken, dit loopt door in 2026.
- We voerden penetratietesten uit om inzicht te krijgen in de effectiviteit van beveiligingsmaatregelen en om risico's te verkleinen.

Beveiligingsincidenten

In 2025 zijn 244 spam/phishing meldingen, 20 incidenten en 118 geconstateerde kwetsbaarheden gemeld bij de CISO en ISO. Het gaat hierbij ook om ontdekte kwetsbaarheden die met updates van software en zijn opgelost. De kwetsbaarheidsmeldingen kwamen voornamelijk van de Informatie Beveiligingsdienst (IBD) en betroffen geconstateerde kwetsbaarheden in software met daarbij het advies over hoe deze zijn te verhelpen.

[1] ISMS is een Engelse afkorting en staat voor Information Security Management System. In het Nederlands wordt dit aangeduid als een managementsysteem voor informatiebeveiliging.

Datalekken
In 2025 zijn 13 datalekken gemeld bij de privacy officer.



Zelfevaluaties
Gemeenten moeten richting de Rijksoverheid verantwoording afleggen over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI).
Hieronder de resultaten per onderdeel voor 2024:

- De **BRP en reisdocumenten (PUN)** scoren met respectievelijk 95% en 96% score goed op de norm.
- De **BAG** scoort met 100 % ruim voldoende, derhalve worden nog verbeteracties voorgesteld.
- De **BGT** scoort met 100 %goed op de norm.
- De **BRO** scoort met 93 %goed op de norm.
- De gemeente Midden-Delfland is **DigiD** aansluithouder voor de Persoonlijke Internetpagina en webformulieren van ons zaaksysteem (xxllnc zaken). Dit wordt vanaf dit jaar op een andere wijze verantwoord. Over het gebruik van DigiD is door een externe IT-auditor vastgesteld dat op alle onderdelen wordt voldaan aan het gestelde normenkader.
- Over het gebruik van **Suwinet** is door een externe IT-auditor vastgesteld dat op alle onderdelen wordt voldaan aan het gestelde normenkader.

Vooruitblik 2026 op het gebied van de informatiebeveiliging
Activiteiten voor 2026:

- We actualiseren ons Strategisch Informatiebeveiligingsbeleid volgens de nieuwe Cyberbeveiligingswet en BIO 2.0.
- We passen onze processen en informatiebeveiligingsorganisatie aan op aangescherpte regelgeving zoals NIS 2, de Cyberbeveiligingswet en de BIO 2.0.
- We organiseren verplichte trainingen voor bestuurders, zodat zij de risico's van cyberveiligheid beter begrijpen en integreren in regulier risicobeheer.
- We stellen een overzicht samen van wie contact onderhoudt met welke overheidsinstanties en toezichthouders met betrekking tot informatiebeveiliging
- We actualiseren ons dataclassificatie-overzicht en implementeren labelprocedures in de vakapplicaties.
- We plannen een cybercrisisoefening die gericht is op het vergroten van bewustwording en het testen van beveiligingsmaatregelen.
- We werken onze bedrijfscontinuïteitsplannen verder uit, met het in 2025 gestarte noodscenario met uitwijk voor de cruciale processen van burgerzaken.
- We rollen het ISMS breder uit en versterken de controle en verbetering door interne audits.

1. Inleiding

Met de VNG resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. Deze baseline is vanaf 2020 overgegaan in de Baseline Informatiebeveiliging Overheid (BIO) en is nu de kern van de verantwoording over informatieveiligheid aan de gemeenteraad.

Gemeenten verantwoorden zich daarom elk jaar over de kwaliteit van de beveiliging van de informatievoorziening. Sinds 2018 gebeurd dit met de Eenduidige Normatiek Single Information Audit (ENSIA).
Gemeenten voeren nu over 2025 opnieuw een zelfevaluatie informatiebeveiliging uit. Deze is onder meer gericht op beveiligingsnormen van de BIO, AVG, BRP, PUN, BAG, BGT, DigiD en Suwinet. Het College van B&W rapporteert aan de gemeenteraad over de stand van zaken van de informatievoorziening met een jaarverslag.

Dit jaarverslag informatiebeveiliging bevat naast informatie over de informatiebeveiliging in brede zin ook een verwijzing naar de verplichte ‘Collegeverklaring ENSIA’. Deze gaat over twee specifiek geselecteerde beveiligingsnormenkaders (DigiD en Suwinet). Een gecertificeerd IT-auditor heeft de Collegeverklaring getoetst en een assurance-rapport opgeleverd dat nodig is voor de verticale verantwoording.

Met dit achtste jaarverslag over onze informatiebeveiliging geven we uitvoering aan de verantwoordingsplicht naar de gemeenteraad.



2. IB-beleid, doelstellingen en ambities

Met de vaststelling van het integraal informatiebeveiligingsbeleid in 2015 zette de gemeente Midden-Delfland een belangrijke eerste stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente op orde te houden. Het huidige strategisch informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid, die per 2020 de Baseline Informatiebeveiliging Gemeenten opvolgde.

2.1. Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan:
het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor het complete proces van informatievoorziening en de hele levenscyclus van informatiesystemen. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politiek bestuur, medewerkers, burgers en bedrijven en samenwerkingspartners.

2.2. Baseline Informatiebeveiliging Overheid (BIO)

In november 2013 is tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de Vereniging van Nederlandse Gemeenten (VNG) de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' bekrachtigd. Deze Resolutie is opgesteld door de Vereniging van Nederlandse Gemeenten (VNG) in samenwerking met de Informatiebeveiligingsdienst voor gemeenten (IBD) en de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). De resolutie houdt in dat iedere gemeente het informatiebeveiligingsbeleid vaststelt aan de hand van de Baseline Informatiebeveiliging.

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten (BIG) uit 2013, Rijk, Waterschappen en Provincies. Hiermee is één gezamenlijk normenkader ontstaan voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende ISO-normen NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002.

Gericht op risicomanagement
De BIO legt de nadruk op risicomanagement. De rol van bestuurders en lijnmanagers is daarbij explicieter geworden. Om hieraan invulling te geven, is gelijktijdig met de BIO de handreiking '10 bestuurlijke principes voor informatiebeveiliging' van kracht geworden. Deze principes ondersteunen bestuurders bij het nemen van hun verantwoordelijkheid op het gebied van informatieveiligheid.

2.3. Informatieveiligheid is geborgd in de organisatie

Ons doel is om 'in control' te zijn op het gebied van informatiebeveiliging. 'In control' zijn betekent dat we inzicht hebben in welke passende technische en organisatorische maatregelen nodig zijn, welke al zijn getroffen, en dat we actief controleren of deze maatregelen effectief functioneren.

Het belang van informatieveiligheid is voor alle doelgroepen duidelijk
Mensen zijn de sleutel tot informatiebeveiliging. Voor een beveiligingsincident dat uitmondt in een datalek is vaak niet meer nodig dan een klik op een verkeerd linkje, een verkeerd geadresseerde e-mail met gegevens over een burger, een verloren laptop of het uitlenen van een toegangspas. Dit risico kan alleen beheerst worden als dag-in-dag-uit gewerkt wordt aan bewustzijn van medewerkers, medewerkers veilige tools en procedures ter beschikking hebben om hun werk te doen en als bestuurders zelf het goede voorbeeld geven.

De P&C-cyclus voor informatieveiligheid is ingericht
De P&C-cyclus voor informatieveiligheid is ingericht. De implementatie en borging van informatiebeveiliging is een continu proces. Omgevingsfactoren, en de bijbehorende bedreigingen en kwetsbaarheden, veranderen voortdurend. Daarom is het essentieel dat organisaties periodiek evalueren en bijsturen om de beveiligingsmaatregelen actueel en effectief te houden.

Informatiebeveiligingsplan
Op basis van het informatiebeveiligingsbeleid stellen we jaarlijks een informatiebeveiligingsplan op. Hierin geven we aan op welke wijze de informatiebeveiliging wordt verbeterd en welke tijdsplanning hierbij gehanteerd gaat worden.

2.4. Uitgangpunten en doelen van ons informatiebeveiligingsbeleid

Uitgangspunten informatiebeveiligingsbeleid
De belangrijkste globale uitgangspunten van het informatiebeveiligingsbeleid zijn:

- Het College van B&W is eindverantwoordelijk voor informatiebeveiliging en stelt het informatiebeveiligingsbeleid vast.
- De gemeentesecretaris is verantwoordelijk voor de uitvoering van het Informatiebeveiligingsbeleid.
- De Chief Information Security Officer (hierna CISO) is gepositioneerd in een lijnfunctie.
- De CISO rapporteert jaarlijks over de informatiebeveiliging aan het college van burgemeester en wethouders.
- In het kader van de signaalfunctie rapporteert de CISO in bijzondere gevallen waarbij de veiligheid van de organisatie in het gedrang komt of dreigt te raken rechtstreeks aan de gemeentesecretaris.
- Aan de hand van een GAP-analyse uit ons ISMS en het actuele dreigingsbeeld (van NCSC en IBD) wordt periodiek een top 10 van te nemen maatregelen opgesteld.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de gemeente Midden-Delfland worden bevorderd en geborgd.

Strategische doelen Informatiebeveiligingsbeleid
De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid

De 10 principes voor informatiebeveiliging voor de bestuurder
Een incident binnen de gemeentelijke processen kan directe gevolgen hebben voor onze inwoners, ondernemers en partners. Daarom moet informatiebeveiliging een expliciet aandachtspunt zijn voor bestuurders. De onderstaande tien principes voor informatiebeveiliging vormen een bestuurlijke aanvulling op het normenkader van de BIO. Ze gaan over de waarden en verantwoordelijkheden die bestuurders zichzelf opleggen om grip te houden op informatieveiligheid.

1. *Bestuurders bevorderen een veilige cultuur.*
2. *Informatiebeveiliging is van iedereen.*
3. *Informatiebeveiliging is risicomanagement.*
4. *Risicomanagement is onderdeel van de besluitvorming.*
5. *Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.*
6. *Informatiebeveiliging is een proces.*
7. *Informatiebeveiliging kost geld.*
8. *Onzekerheid calculeren we in.*
9. *Verbetering komt voort uit leren en ervaring.*
10. *Het bestuur controleert en evalueert.*

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement.

2.5. Relatie met privacy

Sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 staat privacy volop in de schijnwerpers. Privacy heeft specifiek betrekking op persoonsgegevens — een begrip dat ruim moet worden geïnterpreteerd. Zo kan bijvoorbeeld een kenteken als persoonsgegeven worden beschouwd als het herleidbaar is tot een individu. Informatiebeveiliging heeft een breder aandachtsgebied. Het richt zich niet alleen op de bescherming van persoonsgegevens, maar ook op zaken als bedrijfscontinuïteit en de beveiliging van andere soorten informatie.
Toch worden privacy en informatiebeveiliging vaak in één adem genoemd, en terecht. Veel beveiligingsmaatregelen dragen direct bij aan het waarborgen van privacy. Omgekeerd versterken privacyvereisten, zoals het afsluiten van verwerkersovereenkomsten, ook de informatiebeveiliging. Binnen gemeente Midden-Delfland worden informatiebeveiliging en privacy daarom in samenhang benaderd.

Afbeelding: relatie informatiebeveiliging met privacy



3. ENSIA (Eenduidige Normatiek Single Information Audit)

3.1. Aanleiding

Sinds 1 juli 2017 is ENSIA (Eénduidige Normatiek Single Information Audit) de verplichte verantwoordingsmethodiek voor gemeenten. Deze is ontwikkeld door BZK (Binnenlandse Zaken en Koninkrijksrelaties), SZW (Sociale Zaken en Werkgelegenheid), IenM (Infrastructuur en Milieu), VNG (Vereniging van Nederlandse Gemeenten) en gemeenten zelf. ENSIA ondersteunt gemeenten bij hun verantwoordelijkheid voor informatieveiligheid.

Jaarlijks wordt verantwoording afgelegd over onder andere DigiD, Suwinet, BRP (Basisregistratie Personen), BAG (Basisregistratie Adressen en Gebouwen), BGT (Basisregistratie Grootschalige Topografie), BRO (Basisregistratie Ondergrond) en PUN (Paspoortuitvoeringsregeling Nederland). Deze verantwoording sluit aan op de P&C-cyclus en is in lijn met de BIO (Baseline Informatiebeveiliging Overheid).

Achtergrond
ENSIA (Eénduidige Normatiek Single Information Audit) helpt gemeenten om transparant en aantoonbaar 'in control' te zijn op het gebied van informatieveiligheid. Gemeenten leggen verantwoording af aan zowel de gemeenteraad als landelijke toezichthouders, zoals BZK (Binnenlandse Zaken en Koninkrijksrelaties), IenW (Infrastructuur en Waterstaat) en SZW (Sociale Zaken en Werkgelegenheid), over onder andere BRP (Basisregistratie Personen), PUN (Paspoortuitvoeringsregeling Nederland), DigiD, BAG (Basisregistratie Adressen en Gebouwen) en Suwinet.

ENSIA bundelt deze verantwoordingslijnen in één werkwijze, gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid). Waar mogelijk zijn toezichtvereisten geïntegreerd in de ENSIA-vragenlijst, die is afgeleid van de BIO.

Hoewel ENSIA bedoeld is om audits te vereenvoudigen, nemen de werkzaamheden jaarlijks toe. Dit komt door uitbreiding van normenkaders, nieuwe wet- en regelgeving, en een groeiend aantal domeinen waarop informatieveiligheid en privacy van toepassing zijn.

ENSIA en de BIO bieden gemeenten de kans om het proces van aantoonbare informatieveiligheid te verbeteren. Door toenemende digitalisering en decentralisatie beheren gemeenten steeds meer (persoons)gegevens. Jaarlijks wordt verantwoording afgelegd over de kwaliteit van informatieveiligheid en de gebruikte systemen.

3.2. Uitvoering van ENSIA 2025

ENSIA ondersteunt zowel het horizontale als het verticale verantwoordingsproces. De ontwikkeling gaat daarbij steeds meer in de richting van horizontale verantwoording. Hieronder is het ENSIA-proces voor het verantwoordingsjaar 2025 grafisch weergegeven. Meer informatie over ENSIA en de werkwijze is terug te vinden op www.ensia.nl.

Afbeelding: grafische weergave ENSIA verantwoordingsproces 2025



ENSIA	Verantwoording over informatiebeveiliging aan gemeenteraad		Verantwoording aan toezichthouders
Zelfevaluatie	• Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO). • Domeinspecifieke vragenlijsten voor diverse stelsels. • Zelfevaluatie afronden en vastleggen in ENSIA.	**1 JUL 2025**	Vragenlijsten: • RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). • BKWI: Informatiebeveiliging Suwinet (BIO). • Logius: Informatiebeveiliging DigiD. • DGRO: Datakwaliteit en -integriteit BAG, BGT en BRO.
Opstellen	• Genereren en opstellen verantwoordingsrapportages. • Audit door gecertificeerde RE-auditor over collegeverklaring Suwinet en DigiD. • Opstellen rapportage ENSIA t.b.v. de gemeenteraad.	**31 DEC 2025**	Producten: • Collegeverklaring over Suwinet en DigiD. • Rapportage BAG, BGT en BRO door college van B&W. • Rapportage BRP en Reisdocumenten (voor eigen gebruik). • Rapportage ENSIA voor de gemeenteraad.
Verantwoorden	• Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W. • Resultaten BRP en Reisdocumenten worden door RvIG geautomatiseerd verwerkt en in de Kwaliteitsmonitor geplaatst.	**30 APR 2026**	Resultaten: • De toezichthouders Logius, DGRO en BKWI krijgen via ENSIA de verantwoordingsrapportages aangeleverd. • RvIG krijgt de informatie via de Kwaliteitsmonitor aangeleverd.
Versturen	• Opstellen paragraaf verantwoording informatiebeveiliging voor de paragraaf Bedrijfsvoering in het jaarverslag. • Gemeenteraad neemt kennis van rapportage ENSIA. • College van B&W behandelt het jaarverslag en biedt deze aan het college aan. • Gemeenteraad stelt het jaarverslag vast. • Het college van B&W stuurt het gemeentelijk jaarverslag aan de provincie.	**15 JUL 2026**	• De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd. • De vastgestelde jaarstukken zijn aan de provincie toegestuurd.

Verklaring van het college van burgemeester en wethouders
Sinds 2020 wordt de zelfevaluatie uitgevoerd aan de hand van vragenlijsten die zijn gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid). Op basis van de uitkomsten van deze zelfevaluatie is een collegeverklaring opgesteld, waarop een audit heeft plaatsgevonden.

De scope van de audit over 2025 is, net als in voorgaande jaren, beperkt tot Suwinet en DigiD. De collegeverklaring, waarin de gemeente de algehele status van informatieveiligheid verantwoordt, wordt 'horizontaal' aangeboden en als bijlage opgenomen in dit jaarverslag. Deze verklaring wordt als integraal rapport toegevoegd aan het jaarverslag informatiebeveiliging (zie ook hoofdstuk 3).

Toelichting werkwijze zelfevaluatie.
Via de online ENSIA-tool zijn zelfevaluatievragenlijsten beschikbaar gesteld aan de gemeentelijke ENSIA-coördinator. Deze vragenlijsten bestrijken het volledige domein van de BIO (Baseline Informatiebeveiliging Overheid), inclusief specifieke normen voor:

- BRP (Basisregistratie Personen)
- PUN (Paspoortuitvoeringsregeling Nederland)
- DigiD (Digitale persoonsidentificatie)
- BAG (Basisregistratie Adressen en Gebouwen)
- BGT (Basisregistratie Grootschalige Topografie)
- BRO (Basisregistratie Ondergrond)
- Suwinet (Structuur uitvoeringsorganisatie Werk en Inkomen)

In de periode van 1 juli tot 31 december 2025 zijn de vragenlijsten ingevuld door de domeinbeheerders en ingediend bij de landelijke toezichthouders.

Voor de basisregistraties BAG, BGT en BRO zijn aanvullende verantwoordingsrapportages als bijlagen toegevoegd.

Verticale verantwoording
'Verticaal' verantwoorden we met de collegeverklaring de specifieke status van auditonderdeel Suwinet richting de betreffende landelijke toezichthouder. In voorgaande jaren betrof dit ook DigiD. DigiD maakt vanaf dit jaar geen onderdeel meer uit van de collegeverklaring. De landelijke toezichthouder Logius heeft de verantwoordingssystematiek aangepast. De beveiliging van DigiD wordt voortaan volledig en rechtstreeks door de externe IT-auditor getoetst volgens een aparte auditmethodiek.
Daarnaast rapporteren we onze zelfevaluatie over de BAG, BGT en BRO naar de verticale toezichthouder (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.)
De rapportagedeadline hiervoor is 30 april 2026.
In paragraaf 3.3 vindt u de conclusies uit de betreffende verantwoordingsrapportages.

3.3. Verantwoordingsrapportages zelfevaluatie 2025

De verantwoordingrapportages over de ingevulde ENSIA-vragenlijsten zijn als bijlagen bijgevoegd voor het college en de raad.

De verantwoording over de BIO bevat de vragen die wettelijk gericht zijn op de specifieke normen (BRP, PUN, Suwinet, en DigiD).

Daarnaast zijn apart de verantwoordingsrapportages over de BAG, BGT en BRO als bijlagen van dit jaarverslag bijgevoegd. Deze bevatten ook de niet BIO gebaseerde vragen, die gericht zijn op de specifieke normenkaders van BAG, BGT en BRO.

De normen uit de Algemene Verordening Gegevensbescherming (AVG) zijn in de vragen over de BIO en de specifieke domeinen geïntegreerd.

Samen met de collegeverklaring over Suwinet en DigiD vormt het jaarverslag informatiebeveiliging inclusief de verantwoordingsrapportages BAG, BGT en BRO de horizontale verantwoording aan de gemeenteraad.

Zelfevaluatie BIO
Onderwerpen uit de BIO zijn:
- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig Personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

In de hoofdstukken 4 en 6 wordt uitgebreid ingegaan op de resultaten van 2025 en de op basis van de BIO geïmplementeerde maatregelen.

3.4. Resultaten zelfevaluaties per stelsel

Via de ENSIA systematiek is verantwoording afgelegd aan het Rijk. In de volgende paragrafen wordt per zelfevaluatie een toelichting gegeven. De bijbehorende rapportages zijn als bijlagen opgenomen bij deze rapportage.

3.4.1. Zelfevaluaties BRP en PUN

De Basisregistratie Personen (BRP) is onderdeel van het stelsel van basisregistraties van de Nederlandse overheid. De Nederlandse overheid registreert persoonsgegevens in de BRP. Alle overheidsinstellingen en bestuursorganen (zoals bijvoorbeeld de Belastingdienst) zijn verplicht voor hun taken gebruik te maken van die gegevens. Het gaat daarbij onder andere om naam, geboortedatum, geboorteplaats, verblijfplaats en familierelaties. Met deze gegevens wordt bijvoorbeeld een paspoort en identiteitskaart verstrekt of wordt de hoogte van een studietoelage berekend. Voor het uitgeven van reisdocumenten hebben gemeenten met wetgeving te maken zoals de Paspoortuitvoeringsregeling Nederland 2001 (PUN).

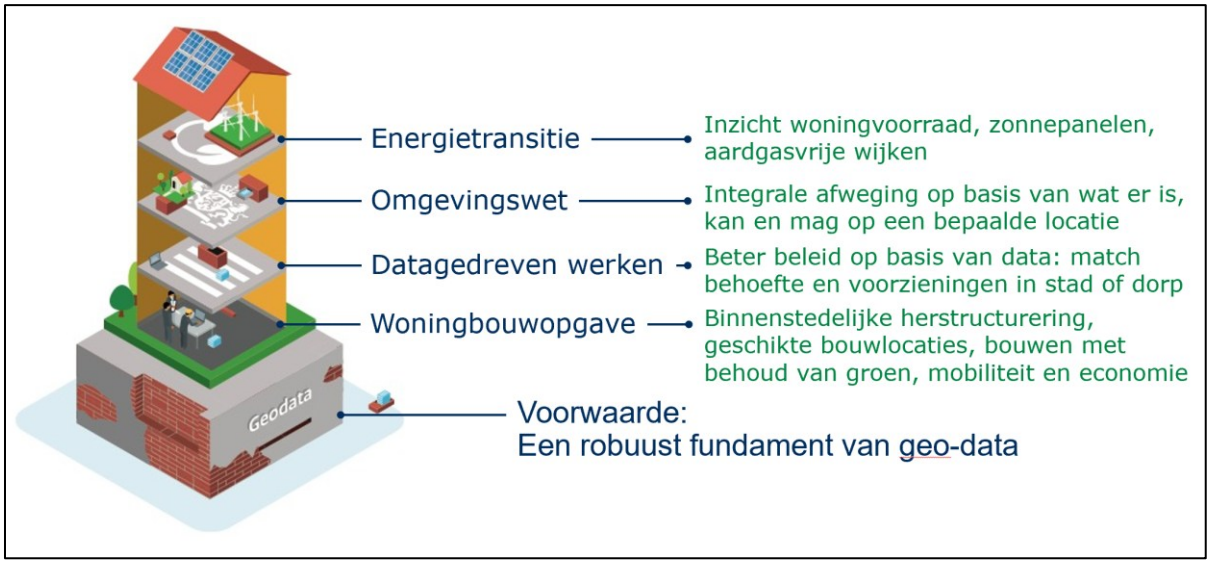
Jaarlijks moeten gemeenten verantwoording afleggen over het gebruik van de BRP en de reisdocumenten. Met de komst van ENSIA is het inhoudelijke deel afgesplitst van het beveiliging technische deel. Het inhoudelijke deel, dat onder andere kijkt naar de kwaliteit van de persoonsgegevens in het BRP en de inrichting van de verwerkingsprocessen, wordt door de vakafdeling uitgevoerd. Het technische deel wordt op basis van de BIO-richtlijnen uitgevraagd. De zelfevaluaties BRP en Reisdocumenten zijn ingediend zodat de externe toezichthouder (het ministerie van Binnenlandse zaken en Koninkrijkszaken) zich hierover een oordeel kan vormen.
Op het inhoudelijke deel van de zelfevaluaties scoort gemeente Midden-Delfland binnen de gestelde normen. De scores van het ENSIA-deel voor de zelfevaluatie BRP en Reisdocumenten treft u hieronder aan.

Resultaat uit zelfevaluatie informatieveiligheid BRP 2025 (ENSIA)			
Thema BRP	**Totaal behaalde punten Midden-Delfland**	**Totaal mogelijk**	**Percentage**
1. Organisatie van de beveiliging	400	400	100 %
2. Toegangsbeveiliging	400	400	100 %
3. Naleving	350	400	87,5 %
Totaal	1.150	1.200	95 %

Resultaat uit zelfevaluatie informatieveiligheid Reisdocumenten 2025 (ENSIA)			
Thema Reisdocumenten	**Totaal behaalde punten Midden-Delfland**	**Totaal mogelijk**	**Percentage**
1. Organisatie van de beveiliging	400	400	100 %
2. Toegangsbeveiliging	400	400	100 %
3. Naleving	360	400	90 %
Totaal	1.160	1.200	96 %

3.4.2. Zelfevaluatie basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO).

In ons land worden geografische basisgegevens jaarlijks meer dan 5 miljard keer gebruikt via de landelijke voorzieningen. Indirect gebruik, via bijvoorbeeld de doorlevering van geo-data door fabrikanten van navigatiesoftware, komt daar nog bovenop.
Het gebruik blijft jaarlijks stijgen en het maatschappelijk belang van deze gegevens, als onderdeel van de geo-informatie infrastructuur, is daarmee groot. Het is daarom cruciaal om de gegevenskwaliteit landelijk op peil te houden.



Afbeelding: nationale geo-informatie infrastructuur (NGII) als basis voor maatschappelijke vraagstukken (bron: BZK)

Wij leggen als bronhouderorganisatie verantwoording af over het beheer van de basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO). Dat doen we intern richting de gemeenteraad en aan het Rijk via het directoraat-generaal Bestuur, Ruimte en Wonen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De hieronder vermelde scores, zijn het resultaat van door ons uitgevoerde zelfevaluaties. Deze evaluaties betreffen de gegevenskwaliteit en de borging van beheerprocessen. Informatiebeveiliging maakt hiervan vooralsnog geen onderdeel uit.

Scores geo-basisregistraties 2025

Basisregistratie	Score	Consequenties score
BAG		We zijn in “Control” en blijven alert op aandachtspunten. De Omgevingswet heeft consequenties voor de registraties in de BAG. Als er niet genoeg gegevens komen bij de aanvragen, kan niet alles op een goede manier in de BAG geregistreerd worden.

< 75% onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BGT		Kwalitatieve BGT → kwalitatief beheer openbare ruimte, adequate voorbereiding plannen en projecten. Essentieel bij de uitvoering van de Omgevingswet Onvoldoende beheercapaciteit BGT → hogere kosten beheer openbare ruimte langere termijn, omdat de ondergrondkaart voor BOR dan niet meer klopt.

< 75% Onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BRO		Als de processen niet op orde zijn, dan worden BRO data niet aangeleverd aan de BRO. Deze gegevens zijn dan niet zichtbaar in het BRO loket en kunnen dan ook niet gebruikt worden voor andere processen.

< 60% Onvoldoende vanaf 60% voldoende

Trend score geo-basisregistraties

Registratie	Score 2018	Score 2019	Score 2020	Score 2021	Score 2022	Score 2023	Score 2024	Score 2025
BAG	90%	95%	95%	92%	92%	92%	94%	**100%**
BGT	70%	60%	60%	72%	100%	100%	98%	**100%**
BRO	N.v.t.	50%	54%	44%	100%	84%	97%	**93%**

De organisatie is “in control” voor wat betreft de basisregistraties BAG, BGT en BRO

Voorgestelde verbetermaatregelen voor 2026
Door de verbetermaatregelen door te voeren zoals hieronder beschreven hopen we bij de volgende verantwoordingsrapportage beter te scoren.

BAG
- We zorgen dat de processen juist blijven werken, zodat alle mutaties tijdig verwerkt kunnen worden.
- Jaarlijks voeren we een mutatiesignalering uit en de resultaten verwerken we in de BGT en de BAG. Voor de WOZ willen we proberen om meer af te gaan stemmen. er is nu al een lijst voor de ontbrekende panden in de WOZ en nu is er sinds dit jaar een lijst met oppervlakte verschillen. Deze lijst wil ik uit gaan zoeken en oplossen. daarna kunnen we aan de slag met het vergelijken en optimaliseren van de bouwjaren.
- Het is een contintu lopen BAG-proces bezig. Zodra er een processtap anders gaat lopen, dan passen we het processenhandboek daaraan aan.

BGT
- De processen met de BAG en de BOR controleren we jaarlijks controleren en apssen we waar nodig aan. Ook in 2026 voeren we een mutatiesignalering zachte topografie uit.
- We volgen wat de kwaliteitseisen zijn van de BGT voor 2026 en geven daar uitvoering aan.
- We zijn in 2021 gestart met het opstellen van een objectenhandboek BGT. Dit handboek wordt geregeld gecontroleerd en aangevuld. We zijn dit jaar bezig geweest met de koppeling tussen de BGT en de BOR. De koppeling van de BGT met de BOR is eind november 2025 daadwerkelijke gerealiseerd .

BRO
- We zorgen dat de processen beter ingebed worden in de organisatie en zorgen dat het proces met de bodemonderzoeken beter gaat lopen.

4. Collegeverklaring ENSIA inzake informatiebeveiliging Suwinet

Het College van Burgemeester en Wethouders geeft in een verklaring aan in hoeverre de beheersmaatregelen voldoen aan de voor de ENSIA verantwoording geselecteerde normen voor Suwinet.

Sinds het huidige verslagjaar is de ENSIA-collegeverklaring uitsluitend gericht op het gebruik van Suwinet. De verantwoording over DigiD maakt geen onderdeel meer uit van de ENSIA-collegeverklaring; hiervoor wordt een separaat verantwoordings- en toetsingsproces gevolgd, conform de geldende landelijke kaders.
Voor zowel Suwinet als DigiD wordt jaarlijks een assuranceverklaring afgegeven door een onafhankelijke IT-auditor, waarmee wordt vastgesteld dat aan de relevante beveiligings- en beheerseisen wordt voldaan.

Bij de ENSIA vragenlijsten is geconstateerd dat inzake Suwinet aan alle normen wordt voldaan. Suwinet, oftewel het Digitaal Klantdossier wordt gebruikt door gemeenten, en diverse andere overheidsinstellingen binnen de sociale sector om gegevens over werkzoekenden en uitkeringsgerechtigden bij te houden en met elkaar te delen.
U treft de collegeverklaring over Suwinet als bijlage van dit jaarverslag aan.



Een gecertificeerd auditor toetst of onze interne beheersingsmaatregelen in opzet, bestaan en werking voldoen aan de normen inzake DigiD en Suwinet. Hierover geeft de auditor een assurance-verklaring af en bekrachtigt de collegeverklaring voor Suwinet. Deze documenten zijn van belang voor de verticale verantwoording aan de departementen.

De auditor heeft geconstateerd dat ook onze interne beheersingsmaatregelen in opzet, bestaan en werking voldoen aan de normen inzake DigiD.

5. Samenvattend beeld en resultaten informatiebeveiliging 2025

5.1. Achtergrond

Dit is het zevende jaarverslagslag is over onze informatiebeveiliging.
Ons gemeentelijk informatiebeveiligingsbeleid is actueel. We hebben ons in 2015 geconformeerd aan het normenkader van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en sinds 2020 de Baseline Informatiebeveiliging Overheid (BIO). In 2023 hebben we ons Strategisch Informatiebeveiligingsbeleid vervangen door een geactualiseerde versie. In 2026 wordt deze vervangen door een op de BIO 2.0 gebaseerd Strategisch informatiebeveiligingsbeleid.



We zijn als gemeente aangesloten bij de Informatiebeveiligingsdienst (IBD).
De IBD is de sectorale CERT / CSIRT (Computer Emergency Response Team en Computer Security Incident Response Team)voor alle Nederlandse gemeenten. Het is onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD draagt namens gemeenten bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD. Voor meer informatie over de IBD, zie hun site https://www.informatiebeveiligingsdienst.nl/

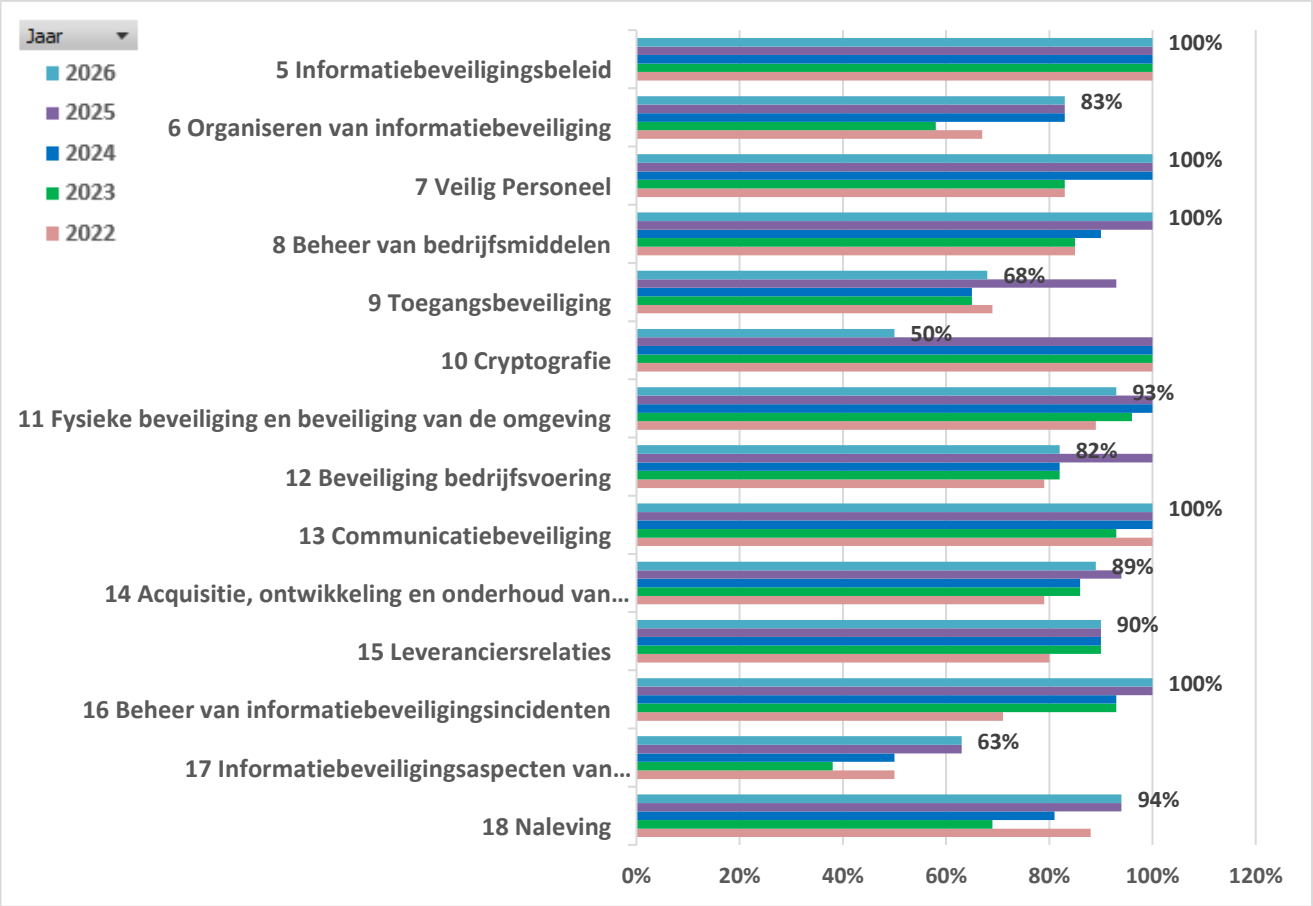
Van GAP-analyse naar planning en prioritering
Om het informatiebeveiligingsbeleid goed te implementeren, werken we op basis van een "GAP-analyse/risicoanalyse". Deze analyses zijn uitgevoerd in directe samenspraak met de betrokken collega's van de vakafdelingen. Hiermee is het "GAP" of "gat" tussen de huidige en de gewenste situatie (volgens de geldende normen) in beeld gebracht. Vanuit deze analyse en het actuele dreigingsbeeld van het NCSC en IBD hebben we een planning en rangschikking van maatregelen gemaakt, om aan de normen met de hoogste prioriteit te voldoen. Deze planning en prioritering is vormgegeven en geactualiseerd in een jaarlijkse top 10 te nemen maatregelen en quick-wins waaraan in 2024 verder is gewerkt. Voortdurend wordt na de genomen maatregelen de top 10 aangevuld met nieuwe actuele, op de gap-analyse gebaseerde, acute dreigingen en de aanbevelingen uit de audit over ENSIA verantwoording.

Om inzicht te verschaffen waar we met onze informatiebeveiliging nu precies staan hebben we met ons ISMS meting uitgevoerd over 2021, 2022, 2023, 2024 en 2025.



5.2. Resultaat meting BIO

Op basis van de resultaten ENSIA 2025 is begin 2026 een meting uitgevoerd op de 112 normen in de BIO. Grafisch ziet het resultaat van meting 5 uit ons ISMS er als volgt uit:



Tabel 1 De in de grafiek getoonde onderdelen betreffen de hoofdstukken uit de BIO (meting uit maart 2026).

Wat valt op?

Over het algemeen zijn er op veel onderdelen stappen gezet om het niveau van onze informatiebeveiliging omhoog te brengen.

In 2025 is ook doorgegaan met het vormgeven van bedrijfscontinuïteitsmanagement. Daarnaast hebben we ons ISMS verder ingericht en uitgerold.

De hoofdstukken 9, 10 en 12 laten een forse daling van de score zien, dit heeft te maken met een strengere toetsing op de uitvoering van de normen over deze aspecten en veranderende technische eisen. In 2026 implementeren we de vereiste maatregelen.

Op de te nemen maatregelen van hoofdstuk 17 van de BIO ofwel informatieveiligheidsaspecten van bedrijfscontinuïteit hebben we een aantal verbeterstappen gezet. Vorige meting zijn we op dit aspect gestegen naar 63% waar we dit jaar ook op uitkomen. We hebben naast het vastgestelde beleid op bedrijfscontinuïteit veel maatregelen ingericht zoals back-up, noodstroomaggregaat etc. Het is allemaal nog niet compleet en in samenhang tot een (crisis) plan gevormd. Het spectrum van bedrijfscontinuïteitsbeheer is veel meer dan dat. Bedrijfscontinuïteitsmanagement (BCM) moet duidelijkheid geven over hoe we onze meest essentiële dienstverlening naar onze burgers kunnen continueren bij uitval van ICT voorzieningen. Hiervoor is in 2023 een BCM beleid voor vastgesteld. Daarbij is ook een noodproces vastgelegd voor het uitkeren van uitkeringen bij uitval van onze systemen. In 2025 zijn we gestart om andere kwetsbare processen noodscenario's op te stellen zoals voor de processen rond burgerzaken en de BAG. Dit krijgt in 2026 vervolg waarbij we kijken

naar een andere totaaloplossing voor zowel fysieke uitwijk als wijziging van de technische uitwijkomgeving voor deze processen.

Verderop in dit jaarverslag gaan we in hoofdstuk 7 nader in op de voorgenomen verbeterpunten en activiteiten die onder de categorie actualisatie/onderhoud vallen voor 2026 voorzien van een toelichting. Deze verbeterpunten gaan we na goedkeuring van dit jaarplan als actiepunten opnemen in het ISMS en van daaruit monitoren.



De vergaande digitalisering en de daarmee gepaard gaande dreigingen zoals bijvoorbeeld ransomware[2] (Hof van Twente) of datalek (Odido) noodzaakt ons als gemeente alert te zijn en aandacht te blijven vragen en geven aan informatieveiligheid. Bewustwording onder het personeel over het digitaal handelen blijft ook in 2026 een continu aandachtspunt.

5.3. Algemene Verordening Gegevensbescherming (AVG)

Sinds 25 mei 2019 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Op 3 juni 2019 heeft het college van de gemeente Midden-Delfland het privacy beleid vastgesteld. Dit beleid bevat de algemene beleidsuitgangspunten over de bescherming van persoonsgegevens door de gemeente Midden-Delfland. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de AVG. De functionaris gegevensbescherming controleert jaarlijks of aanpassingen aan dit beleid nodig zijn.



Ook in 2025 hebben we op basis van de AVG met leveranciers en dienstverleners verwerkersovereenkomsten en dataleveringsovereenkomsten afgesloten. Hierin zijn de verantwoordelijkheden geregeld voor de beveiliging van het gebruik van onze privacygevoelige gegevens. We hebben naast technische maatregelen, ook gewerkt aan bewustzijn bij de medewerkers.

Informatiebeveiliging en privacybescherming hebben een grote 'houding en gedrag'- kant. Vanwege de inwerkingtreding van de AVG zijn door de projectgroep Privacy gemeente-brede bijeenkomsten georganiseerd waarbij vooral is ingegaan op hoe er vertrouwelijk met persoonsgegevens van personen moet worden gegaan. Onze interne beveiligingsorganisatie bestaat uit medewerkers van de verschillende teams die binnen hun team zorgen voor bewustzijn en aanspreekpunt zijn voor informatiebeveiliging voor hun team.
Daarnaast zijn er voor de borging van de AVG en de privacybescherming medewerkers binnen de organisatie aangewezen als privacy-ambassadeur.

Bij het incidenten overzicht informatiebeveiliging in hoofdstuk 8 leest u ook het aantal en soort datalekken over 2025.

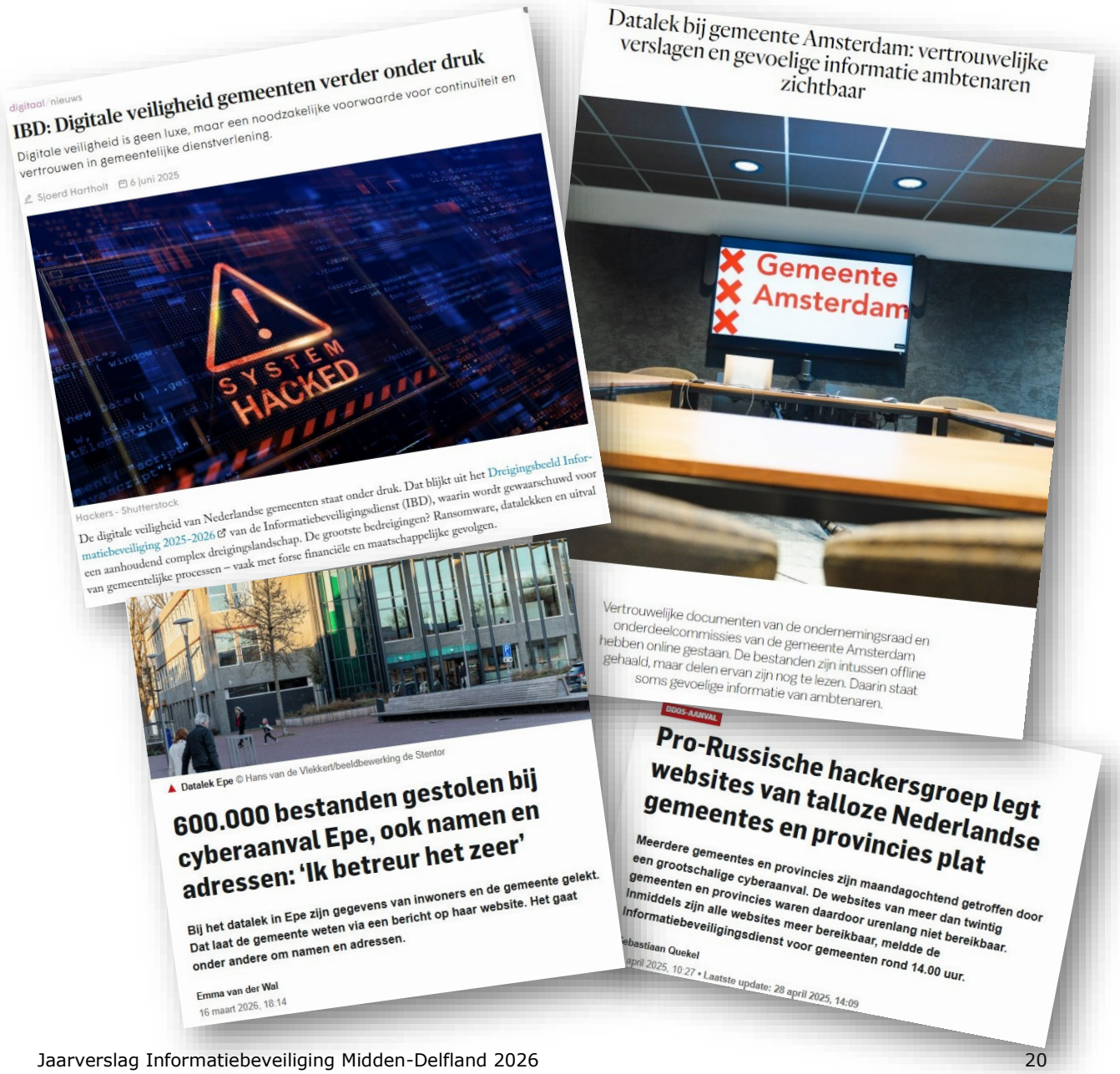
[2] Ransomware ofwel gijzelsoftware is schadelijke software die computers en bestanden gijzelt. Criminelen geven toegang weer vrij als hiervoor losgeld is betaald.

" Als burger ben je verplicht gegevens met de overheid te delen. Natuurlijk ga je er dan vanuit dat de overheid daar zorgvuldig mee omgaat."

Aleid Wolfsen, voorzitter Autoriteit Persoonsgegevens

6. Disclaimer

Beveiligingsincidenten zijn helaas niet te voorkomen; 100% beveiliging is een utopie. De vraag is dan ook niet zozeer of er een beveiligingsincident met een hoge impact zal plaatsvinden, maar wanneer. Beveiligingsincidenten kunnen leiden tot onderbreking van werkzaamheden, reputatieschade en aanzienlijke financiële schade als gevolg van het bestrijden van een incident en het herstellen naar een normale situatie.
De maatregelen die we nemen zijn erop gericht de risico's zoveel mogelijk te minimaliseren tegen aanvaardbare kosten. Daarnaast houden we rekening met de impact op dienstverlening en bedrijfsvoering. Een hele goede maatregel is bijvoorbeeld het uitschakelen van alle internetverbindingen van het gemeentehuis. Een hacker van buiten het kantoor zou dan geen enkele kans meer hebben. Dit is in deze tijd onwerkbaar omdat onze gegevensuitwisseling met inwoners en andere overheden voor een groot gedeelte via het internet lopen.
Naast preventieve maatregelen richten we ons ook op procedures en maatregelen wanneer zich een incident voordoet. Zodat we met onze dienstverlening en bedrijfsvoering zo snel mogelijk weer operationeel zijn.



7. Realisatie doelstellingen IB-beleid

Hieronder geven we aan met welke genomen maatregelen we invulling hebben gegeven aan de in hoofdstuk 2 genoemde strategische doelen.

De strategische doelen van het informatiebeveiligingsbeleid:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

De drie belangrijkste punten, die in grote mate het succes bepalen van de implementatie van de BIO:

Maatregel	Doelstelling
Informatiebeveiligingsbeleid Er is op dit moment een compleet gemeente-breed informatiebeveiligingsbeleid. We hebben de verplichting dit elke 3 jaar te actualiseren. In 2023 is ons het op de BIO gebaseerde informatiebeveiligingsbeleid voor 2023-2026 door het college van burgemeester en wethouders vastgesteld. Naar verwachting actualiseren we dit beleid in 2026 vanwege de Cyberbeveiligingswet en de BIO 2.0 die van kracht worden.	Het managen van de informatiebeveiliging
Informatiebeveiligingsorganisatie (IB-organisatie) Zonder IB-organisatie is het onmogelijk om tot een goede borging van informatiebeveiliging te komen binnen de ambtelijke organisatie. Elk bedrijfsproces bestaat uit verschillende informatiestromen, waarbij ook verschillende (informatie-)systemen gebruikt worden. Voor al deze onderdelen zijn de taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging vastgelegd en toegewezen aan een functie/rol in de organisatie. De leden van de IB-organisatie worden sinds 2017 opgeleid. In 2026 wordt de IB-organisatie geactualiseerde naar de nieuwe Cyberbeveiligingswet en de BIO 2.0.	Het managen van de informatiebeveiliging
ISMS Er is een ISMS (Information Security Management System) geïmplementeerd binnen de gemeente Midden-Delfland. Deze software gebruiken we als ondersteunende tool om alle bedrijfsprocessen in relatie met informatiebeveiliging in kaart te brengen, te monitoren en te borgen binnen de gemeentelijke organisatie. Ook verantwoorden we in het ISMS de stand van zaken per proces en per norm. Het ISMS wordt in 2026 nog verder uitgerold over de IB-organisatie en vakapplicaties.	Het managen van de informatiebeveiliging

Hiermee zijn de randvoorwaarden ingevuld voor een succesvolle verdere implementatie van het IB-beleid.

7.1. Controls & beheersmaatregelen IB

In de BIO staan controls en maatregelen. Het vraagt meerdere jaren om deze maatregelen te implementeren in onze gemeentelijke processen en systemen. Het is daarom nodig om inzicht te krijgen in wat er moet gebeuren met welke prioriteit.
Met een delegatie van applicatie- en procesbeheerders is daarom op basis van de Baseline Informatiebeveiliging Gemeenten (BIG) in 2016 een GAP- en Impactanalyse uitgevoerd op gemeentebrede maar ook systeem specifieke maatregelen. Met de GAP-analyse zoeken we uit waar we staan met genomen maatregelen ten opzichte van de normen en risico's.
Een meting dus over wat we aan maatregelen al 'in huis' hebben, wat is hiervan nog up-to-date en wat moet er nog aan maatregelen georganiseerd worden.
Hierbij is het van belang om alvast na te denken of maatregelen gemeentebreed of systeem specifiek zijn. Deze stap geeft ook al inzicht in hoe het nu geregeld is, dus wie voert feitelijk welke informatiebeveiligingsmaatregelen uit.

Hiermee is er inzicht gekomen in waar we de focus voor het komende jaar qua BIO-implementatie op leggen:

a. De status van belangrijke gemeente-brede maatregelen.
b. Essentiële processen.
c. Kritische systemen.
d. De status van systeem specifieke maatregelen.

Conclusies GAP- en impactanalyse
Uit de eerste (BIG-gebaseerde) GAP-analyse kwamen 155 nog te implementeren maatregelen. Om de juiste prioriteit te krijgen bij deze 155 openstaande maatregelen die de gemeente Midden-Delfland als eerste op moet pakken is naast de GAP-analyse ook een risico- en impactanalyse gemaakt.

Omdat het onmogelijk was om alle maatregelen tegelijk op te pakken, hebben we ons na de risico- en impactanalyse) gericht op een top 10 lijst. De te implementeren maatregelen op deze top 10 lijst pakten we als eerste op. Daarna richten we ons jaarlijks op 10 nieuwe normen en te nemen maatregelen van de BIG, volgens de prioritering uit de impact- en risicoanalyse. Met de inwerkingtreding van de BIO is het aantal maatregelen omlaag gegaan maar wel met de komst van een aantal verplichte maatregelen. Welke maatregelen je moet nemen als organisatie hangt af van de risico's. Deze worden inzichtelijk gemaakt aan de hand van wat de kans is dat zich iets voor doet, wat de impact dit heeft en welke schade er mee gemoeid is.

De BIO Baselinetoets
Na de impactanalyse voor de BIG hebben we een in 2019/2020 de (BIO) baselinetoets uitgevoerd waarmee we een dataclassificatieschema hebben opgesteld. Hiermee bepalen we of een proces, informatiesysteem een bepaald Basis Beveiliging Niveau (BBN) heeft binnen de BIO en welke maatregelen nodig zijn. Er wordt hierbij gekeken naar 3 beveiligingsaspecten van informatie (biv genaamd):

- **b**eschikbaarheid,
- **i**ntegriteit,
- **v**ertrouwelijkheid.

De uitkomsten gebruiken we om te bepalen of er meer maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Deze maatregelen kunnen worden verkregen uit een voor gedefinieerde lijst met maatregelen bovenop de baseline, of door een aanvullende diepgaande risicoanalyse. De normen en (genomen en nog te nemen) maatregelen houden we bij in ons ISMS.

In 2025 is binnen de gemeente actief toegewerkt naar de invoering van de Baseline Informatiebeveiliging Overheid 2.0 (BIO 2.0). De BIO 2.0 is in 2025 landelijk vastgesteld en fungeerde voor gemeenten als richtinggevend normenkader, vooruitlopend op de wettelijke verankering via de Cyberbeveiligingswet.
Gedurende het jaar is ingezet op de voorbereiding van de overgang van BIO 1.04 naar BIO 2.0. Hierbij lag de nadruk op het versterken van het risicogestuurd werken en het verder inrichten van het Information Security Management System (ISMS) conform de uitgangspunten van ISO 27001. De traditionele indeling in vaste beveiligingsniveaus maakte daarbij plaats voor een aanpak waarbij beveiligingsmaatregelen worden afgestemd op actuele en geprioriteerde risico's.
Daarnaast zijn bestaande risicoanalyses en dataclassificaties tegen het licht gehouden om beter inzicht te krijgen in de te beschermen belangen, zoals beschikbaarheid, integriteit en

vertrouwelijkheid van informatie. Deze inzichten vormen een belangrijke basis voor het bepalen van prioriteiten, zowel voor preventieve maatregelen als voor herstel bij eventuele verstoringen. Met deze voorbereidingen heeft de gemeente in 2025 een belangrijke stap gezet om in 2026 aantoonbaar en structureel te kunnen werken conform de BIO 2.0 en de daaruit voortvloeiende wettelijke verplichtingen. 2026 geldt voor gemeenten als overgangsfase naar het werken volgens de BIO 2.0

Er is getoetst wat al is geïmplementeerd en nog actueel is volgens de BIO normen. Met name de generieke beveiligingsmaatregelen die gemeente-breed gelden.

Bij deze generieke beveiligingsmaatregelen gaan we uit van:

- Het gemeentelijk informatiebeveiligingsbeleid, dit is gelijk voor de gehele gemeente
- Het toewijzen van de Chief Information Security Officer (CISO)-functie
- Verantwoordelijkheden van de lijnmanagers (te verankeren in het beleid)
- (ITIL) beheerprocessen en aandacht voor beveiliging
- Personele beveiligingsmaatregelen
- Fysieke toegangsbeveiligingsmaatregelen
- Beveiligingsmaatregelen voor apparatuur en software
- Malware scanning als generieke dienst (dus niet ten behoeve van één informatiesysteem)
- Omgang met (mobiele) gegevensdragers
- Het hebben van een Information Security Management Systeem (ISMS)

7.2. Jaarplan Informatiebeveiliging 2026 met verbeterpunten

De focus voor verbetering richt zich vooral op de hoofdstukken in BIO die volgens de meting of vanwege regelgeving of ontwikkelingen aandacht verdienen. Deze hoofdstukken vindt u in onderstaande tabel terug met de beschrijving van de verbeterpunten voor 2025.

Hoofd-stuk BIO	**Onderwerp**	**Beschrijving verbeterpunten**
5	Informatiebeveiligings-beleid	We actualiseren in 2026 ons Strategisch Informatiebeveiligingsbeleid op basis van de eisen uit de nieuwe Cyberbeveiligingswet en de BIO 2.0
6.1.3	Organiseren van Informatiebeveiliging	Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden. We maken een overzicht wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.
7.2.2	Bewustzijn, opleiding en training	We organiseren voor de gemeentelijke bestuurders een verplicht te volgen training over informatiebeveiliging. Zodra de nieuwe regelgeving ingaat, wordt de gemeente expliciet verantwoordelijk voor de beheersing van cyberrisico's. Dat betekent dat een analyse van cyberrisico's onderdeel moet zijn van het bredere, reguliere risicobeheer, net als financiële, juridische en politieke risico's. De bestuurders hebben hierin een belangrijke rol. Dit brengt met zich mee dat het college van burgemeester en wethouders verplicht is om informatiebeveiligingsmaatregelen goed te keuren en een training te volgen. Deze training stelt de bestuurders in staat om risico's te identificeren, risicobeheersmaatregelen te evalueren en de impact van zowel de risico's als de beheersmaatregelen te beoordelen.

8.1 / 8.2	Dataclassificatie	In 2026 vervolgen we de actualisatie van ons dataclassificatie-overzicht en stellen we procedures om onze informatie te labelen in de vak-applicaties (dit is wel georganiseerd in ons zaaksysteem).
9	Toegangsbeveiliging	Het gaat dan vooral om het beheer van toegangsrechten in de vakapplicaties zelf. Hier ligt een belangrijke rol voor de functioneel applicatiebeheerders. Dit gaat met de ingezette bredere uitrol van het ISMS in 2026 meer aandacht krijgen.
16 (+ 7,17 en 18)	Beheer van informatiebeveiligings-incidenten	We plannen in de 2e helft van 2026 een cybercrisisoefening in. De oefening is gericht op het creëren of versterken van bewustwording m.b.t. informatiebeveiliging en privacybescherming bij een brede doelgroep: • vakspecialisten informatiebeveiliging en privacybescherming; • bestuurders; • management (op alle niveaus). Daarnaast geeft de oefening inzicht in de werking van bepaalde genomen beveiligingsmaatregelen.
17	Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	We hebben veel maatregelen ingericht zoals back-up, noodstroomaggregaat etc. maar dat is allemaal nog niet compleet en in samenhang tot een (crisis) plan gevormd Het spectrum van bedrijfscontinuïteitsbeheer is ook veel meer dan dat. Bedrijfscontinuïteitsmanagement (BCM) moet duidelijkheid geven over hoe we onze meest essentiële dienstverlening naar onze burgers kunnen continueren bij uitval van ICT voorzieningen. Hiervoor is in 2023 een BCM beleid voor vastgesteld. Daarbij is ook een eerste noodproces vastgelegd voor het uitkeren van uitkeringen bij uitval van onze systemen. In 2024 is gestart om voor andere kwetsbare processen noodscenario's op te stellen zoals voor de processen rond burgerzaken. Dit kreeg in 2025 vervolg waarbij we kijken naar een andere totaaloplossing voor zowel fysieke uitwijk als het snel beschikbaar krijgen van gebruikte systemen dit wordt in 2026 afgerond.
18.2.2	Uitbreiden gebruik ISMS	Het ISMS is ons managementsysteem dat helpt om op een aantoonbare en controleerbare wijze verantwoording af te leggen op het gebied van informatiebeveiliging. Het breder uitrollen van het ISMS onder functioneel applicatiebeheerders op basis van de PDCA-cyclus en de daaruit voortkomende periodieke rapportages is van belang. De verbeterstap is dat organisatie vertrouwd raakt met het ISMS gericht op continu verbeteren van informatiebeveiliging. Dit proces is bij een aantal functioneel applicatiebeheerders al succesvol vorm gegeven en krijgt in 2026 een vervolg.
18.2.2	Beoordeling van technische naleving	We voeren in 2026 wederom pentesten uit op de meest risicovolle onderdelen uit onze technische infrastructuur. Het doel van penetratietesten is het verkrijgen van inzicht in de status en effectiviteit van de beveiligingsmaatregelen. Het resultaat geeft aan wat de aandachtsgebieden zijn en biedt concrete handvatten

		voor adequate maatregelen en investeringen, met als doel de beveiligingsrisico's te reduceren. Het geeft inzicht in de gevonden inbraakmogelijkheden, de genomen maatregelen en de restrisico's en de mogelijkheid hierover aan het management te rapporteren. Een penetratietest gebruiken we eventueel ook als onderdeel van een bewustwordingscampagne om de bewustwording van de medewerkers te verhogen.
18. (en 5.)	Organisatorische aanpassingen op de zelfevaluatie informatiebeveiliging als gevolg van de Cyberbeveiligingswet en de BIO 2.0	De auditlast neemt al sinds 2025 toe op informatiebeveiliging (en privacy) als gevolg van de aangescherpte regelgeving zoals NIS2, de Cyberbeveiligingswet en de BIO2.0. Het ENSIA-proces wordt daar ook op aangepast. Hierdoor wordt er in toenemende mate ook op actieve werking van de genomen beveiligingsmaatregelen worden getoetst. Hiervoor organiseren we in 2026 met de betreffende domeinbeheerders werkbare processen in ons ISMS. Daarnaast actualiseren we in 2026 ons Strategisch Informatiebeveiligingsbeleid op de nieuwe regelgeving en passen we onze beveiligingsorganisatie daarop aan.

Aanbevelingen auditor DigiD en Suwinet
Daarnaast zijn uit de ENSIA audit over DigiD en Suwinet door de auditor aanbevelingen gedaan.

Over Suwinet gaat het om:

- Vanaf verantwoordingsjaar 2026 wordt de toets op werking een verplicht element. Maak aantoonbaar dat gedurende het gehele verantwoordingsjaar:
  - invoerende en controlerende Suwi-taken zijn gescheiden;
  - de gebruikersbeheerder geen security officer Suwinet is;
  - de gebruikersbeheerder en/of de security officer Suwinet geen rol heeft als medewerker met Suwinet inkijk of -inlezen rechten in de uitvoering;
  - het autoriseren van toewijzing van toegang tot Suwinet of Suwinet gerelateerde gegevens gescheiden is van het controleren van deze rechten op het rechtmatig gebruik van Suwinet of Suwinet gerelateerde gegevens, of het controleren van de actualiteit van de gebruikersadministratie
  - Houd gedurende het verantwoordingsjaar een lijst bij van nieuwe medewerkers die toegang krijgen tot Suwinet en houd daarin aantoonbaar bij dat al deze medewerkers maximaal binnen drie maanden na indiensttreding een training (I-) bewustzijn succesvol hebben gevolgd en rapporteer hierover jaarlijks aan het management.
  - Zorg aantoonbaar voor een verbijzonderde interne controle over het verantwoordingsjaar door een onafhankelijke deskundige (dus iemand buiten het administratieve proces zoals bij voorbeeld de security officer Suwinet) op het naleven van de beheersmaatregelen met betrekking tot het registreren en afmelden van gebruikers.
  - Zet de 'Handleiding instroom uitstroom MD' om naar een werkwijze of voorschrift en zorg dat het toekennen/intrekken en controleren van toegangsrechten hierin allemaal duidelijk is opgenomen.
  - Zorg aantoonbaar voor een verbijzonderde interne controle over het verantwoordingsjaar door een onafhankelijke deskundige (dus iemand buiten het administratieve proces zoals bij voorbeeld de security officer Suwinet) op het naleven van de beheersmaatregelen met betrekking tot single sign-on of MFA, het autorisatieproces, het registreren, loggen, analyseren en beoordelen van uitzonderingen op gebruikersactiviteiten en informatiebeveiligingsincidenten.

Over DigiD gaat het om:

- Ondersteun als securityorganisatie de betrokken teams zo veel mogelijk bij het verzamelen van bewijslast gedurende hun eigen proces, zodat men voor de volgende audit alleen maar informatie hoeft aan te leveren die al vastgelegd is.
- Houd er rekening mee dat de controleperiode gedurende de tijd zal toenemen naar uiteindelijk een jaar. Een controleperiode van een jaar is gebruikelijk voor de toetsing op werking.
- Draag zorg voor de verbijzonderde interne controle op het identiteits- en toegangsbeheer en het wijzigingsbeheer van xxllnc Zaken. Deze controles worden ook wel tweedelijnscontroles genoemd en moeten aantoonbaar worden uitgevoerd door een deskundige die buiten het administratieve proces staat zoals een security-officer, een kwaliteitsfunctionaris of intern auditor of CISO. Functioneel beheer mag hier uiteraard wel bij assisteren om de benodigde data voor de controle te verschaffen.
- Ga na of het authenticatieniveau van DigiD dat u voor uw dienst gebruikt nog wel passend is bij de vertrouwelijkheid van de gegevens die worden uitgewisseld. Gebruik hiervoor de https://regelhulpenvoorbedrijven.nl/betrouwbaarheidsniveaus/ Hiermee kan een beredeneerde keuze worden gemaakt voor het juiste betrouwbaarheidsniveau voor digitale diensten.
- De aanwezigheid van uw organisatie op het internet is veel omvangrijker dan alleen de door ons beoordeelde DigiD aansluiting. Ga via https://basisbeveiliging.nl/report na welke mogelijke kwetsbaarheden er op andere URL's van uw organisatie zijn en draag zorg voor het oplossen ervan.

De verwachting is dat de meeste in deze paragraaf vermelde punten binnen het reguliere werk kunnen worden gerealiseerd. Er is alleen goede wil en voldoende medewerking nodig vanuit de organisatie en daarin is alle vertrouwen. We onderkennen immers het belang van informatiebeveiliging steeds meer als randvoorwaarde voor het succes van onze organisatie.

7.3. Nieuwe wet- en regelgeving over informatiebeveiliging

Bovenstaande maatregelen gaan voornamelijk over onze administratieve en dienstverlenende processen. Automatisering en internetkoppelingen zien we echter ook steeds meer in vitale fysieke systemen terugkomen zoals zogenaamde internet-of-things. In onze beweegbare bruggen, verkeerslichten, CCTV systemen en rioolgemalen wordt steeds meer gebruik gemaakt van (industriële) automatisering, ook wel Industrial Control Systems en Supervisory Control And Data Aquisition (ICS/ SCADA) genoemd. Hierop wordt in nieuwe regelgeving op geanticipeerd.

De *Cyberbeveiligingswet (Cbw)* is (samen met de *BIO2.0)* onderdeel van de implementatie van de *Europese Netwerk- en informatiebeveiligingsrichtlijn (NIS2)*. De BIO2.0 dient als normenkader voor de zorgplicht van de overheid op het gebied van informatiebeveiliging en helpt een uniforme en gecoördineerde aanpak van cyberbeveiliging te waarborgen. De normen en verplichtingen worden juridisch verankerd in de Cyberbeveiligingswet.

Toezicht en wetgeving worden strenger

De toezichthouders op informatiebeveiliging worden actiever bij de handhaving van de NIS2-richtlijn en de Cyberbeveiligingswet. De verantwoordelijkheid verschuift hierbij steeds meer naar de gemeenten zelf. Bestuurders worden aansprakelijk gehouden als blijkt dat er onvoldoende toezicht is geweest op informatiebeveiliging. Dit vraagt om een preventieve benadering in plaats van een reactieve.

Zo werkten we in 2025 samen met de gemeente Westland aan het implementeren van technische componenten zoals het SIEM/SOC. Hiermee wordt het mogelijk om systematisch in de gaten houden wat er gebeurt in de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren.
Detectie zorgt voor het vroegtijdig signaleren van afwijkingen en bedreigingen en geeft daarmee ruimte om incidenten te voorkomen voordat ze manifest worden. Detectie zorgt dat kosten als gevolg van incidenten laag blijven en incidenten uiteindelijk zelfs voorkomen kunnen worden, maar ook dat zaken die niet of nooit gezien worden wel aan het licht komen en kunnen worden aangepakt. Detectie en de reactie op meldingen vereist echter tijd van beheerders, die deze tijd vaak niet beschikbaar hebben.



Als de gemeente niet weet wat er gebeurt, dan kan ook niet worden gestuurd op risico's. Gebrek aan inzicht in wat er feitelijk gebeurt is onwenselijk, omdat dit het bestuur belet om adequaat te kunnen sturen op risico's, ernaar te handelen en ervan te leren. Het implementeren van de BIO en de AVG brengt de basis op orde. Daarmee kan informatiebeveiliging en privacybescherming als proces worden ingericht waarmee de focus op detectie en actieve preventie gezien wordt als de logische vervolgstap.

Regionale samenwerking
Sinds 2017 zijn medewerkers (CISO en informatieadviseurs) van Midden-Delfland op regionaal niveau betrokken bij structureel overleg over informatiebeveiliging.
Het doel van het overleg is met name om kennis en ervaringen te delen en waar mogelijk ondersteunen bij informatiebeveiligingsincidenten.



8. Incidenten, ontdekte kwetsbaarheden en datalekken

8.1. Gemelde incidenten en kwetsbaarheden

In 2025 zijn 244 spam/phishing -meldingen, 20 incidenten en 118 geconstateerde kwetsbaarheden gemeld bij de CISO en adviseurs informatiebeveiliging. Het gaat hierbij ook om ontdekte kwetsbaarheden die met updates van software en zijn opgelost. De kwetsbaarheidsmeldingen kwamen voornamelijk van de Informatie Beveiligingsdienst (IBD). Ze betroffen onder andere geconstateerde kwetsbaarheden in software en hardware met daarbij het advies over hoe deze zijn te verhelpen.

De verplaatsing van applicaties naar de Cloud gaat de komende jaren toenemen waardoor de kwetsbaarheid van ons eigen ICT-netwerk ook afneemt. Dit betekent dat we ook alert moeten zijn op de beveiliging van onze in de Cloud bij leveranciers opgeslagen informatie.

Meldplicht datalekken
Sinds 2016 geldt de wet Meldplicht datalekken en per 25 mei 2019 is de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) van kracht geworden. Als onze organisatie niet voldoet aan deze wetten, is dat een risico op een bestuurlijke boete van de Autoriteit Persoonsgegevens van maximaal 20 miljoen euro.

8.2. Gemelde datalekken

In 2025 zijn 13 datalekken gemeld bij de privacy officer. In 2020 waren dit er nog 17 in 2021 maar 11 en 10 in 2022, 2023 en 2024. Het lijkt hier om een stabiele lage trend te gaan die aandacht verdient. Van een organisatie met de omvang van de gemeente Midden-Delfland kan verwacht worden dat elk jaar enkele tientallen datalekken plaatsvinden, waar gewerkt wordt worden immers ook fouten gemaakt.

Binnen 72 uur moeten daarvoor in aanmerking komende datalekken bij de Autoriteit Persoonsgegevens (AP) gemeld. Van de bij ons gemelde incidenten is er één door ons als datalek gemeld bij de Autoriteit Persoonsgegevens (AP). Er vindt dan direct verder onderzoek plaats naar de risico’s voor personen waarvan de gegevens zijn gelekt. Dit is ook bepalend of deze personen worden geïnformeerd over dit datalek.
De hieronder beschreven incidenten die niet als datalek bij de AP zijn gemeld betreffen incidenten waarbij gegevens niet buiten de organisatie zijn gekomen of waarbij door snel te handelen het risico op schade voor de persoon in kwestie teniet is gedaan.

Meldings-datum	Omschrijving	Melding aan AP
2-3-2025	Bij een printer in het gemeentehuis is een intakeformulier gevonden met daarop NAW-gegevens, het BSN-nummer en medische gegevens. Het incident is een mogelijk gevolg van een storing bij de printers. Het document is direct na ontdekking veiliggesteld, aangezien de ruimte ook toegangelijk is voor medegebruiker Staatsbosbeheer, collega's en mogelijke bezoekers.	Nee
3-6-2025	Er is een e-mail naar de verkeerde ontvanger gestuurd. In deze e-mail staan persoonsgegevens, namelijk de naam en het e-mailadres van de klant. Direct na het versturen van de e-mail is er een mail verstuurd naar de onbevoegde ontvanger verstuurd met het verzoek om de e-mail te verwijderen. De onbevoegde ontvanger heeft bevestigd de e-mail te verwijderen.	Nee
27-5-2025	Vanuit het Zaakysteem is er door een medewerker naar een ontvanger tweemaal een e-mail verstuurd met als aanhef (achternaam) een ander dan de ontvanger. Aan de medewerker is verzocht om aan de ontvanger een e-mail te sturen met daarin het verzoek om de e-mails die niet voor haar bedoeld waren te verwijderen.	Nee
27-5-2025	Een medewerker van de gemeente liet gedurende 2 uur zijn tas met daarin zijn werklaptop en telefoon in het OV staan. Het risico op een datalek is echter beperkt, aangezien de laptop en telefoon vergrendeld waren.	Nee
28-7-2025	Op donderdag 24 juli 2025 zijn uitkeringsspecificaties van bijstandsgerechtigden per post verstuurd. Naar verwachting zijn de meeste brieven teruggekomen, omdat in het adresveld de combinatie huisnummer en	Nee

	postcode niet herkend werd door PostNL. Het blijkt dat straat + huisnummer van cliënt zijn, terwijl postcode + woonplaats van de bewindvoerder. Omdat het in principe om meer cliënten zou moeten gaan, is het mogelijk dat in andere gevallen de combinatie postcode + huisnummer wel bestaat, alleen bij een verkeerd adres aankomt. Het gaat om minder dan 25 mensen. Op de specificaties staat o.a. naam cliënt, straat + huisnummer, het uitkeringsbedrag, IBAN en BSN. De brieven zijn geretourneerd en niet aangekomen bij de onbevoegde ontvangers. De oorzaak is gevonden in een update van de gebruikte software. Dit is door applicatiebeheer inmiddels hersteld.	
29-7-2025	De gemeente heeft Beslissing op bezwaarschriften omgevingsvergunning AZC gepubliceerd via iBabs. In een bijlage, het advies van de bezwaarschriftencommissie, stonden vanaf pagina 19 tot en met 21 de NAW-gegevens van de bezwaarmakers tegen het AZC. De niet-geanonimiseerde versie van het document is offline gehaald en vervangen voor de geanonimiseerde versie. Daarnaast zijn de betrokkenen geïnformeerd over dit incident. Naar aanleiding van het uitgevoerde onderzoek zijn de volgende maatregelen naar voren gekomen: - Publiceren uitsluitend via het zaaksysteem. Publicatie vanuit e-mail is vanaf heden niet toegestaan. - Verplichte vier-ogencheck op persoonsgegevens vóór publicatie. - In besluitvorming nadrukkelijker afwegen of de transparantie conflicteert met de privacy. - Rolvastheid voor de RIB door het volgen van het reguliere proces met het daarbij benoemde - eigenaarschap en de daarbij horende doorlooptijd (wie levert, wie controleert, wie publiceert; - vervangingsregeling bij afwezigheid). Dit kan effect hebben op de doorlooptijd. – Beperken van bijlagen. De informatie waar mogelijk opnemen in de brief zelf. Alleen bijlagen toevoegen als dit noodzakelijk is	Ja
4-8-2025	Op 19 december 2023 zijn met de beslissing op een Woo-verzoek per abuis persoonsgegevens van een voormalige ambtsdrager van de gemeente meegestuurd. Dit is gemeld op 4 augustus 2025 door de ontvanger van de beslissing van het Woo-verzoek. De ontvanger heeft aangegeven de gegevens niet te hebben verstrekt aan anderen. De voormalige ambtsdrager is geïnformeerd over de situatie. Inmiddels werkt de gemeente met software waarin persoonsgegevens semiautomatisch geanonimiseerd wordt. De medewerker heeft hierbij nog een handmatige eindcontrole.	Nee
4-9-2025	De gemeente maakt gebruik van een DDOS-dienst met cyberbeveiligingssoftware van een derde partij, deze heeft van 12 augustus tot en met 17 augustus 2025 te maken gehad met een datalek. Het gaat daarbij voornamelijk om customer support tickets. Uit verder onderzoek naar het incident is gebleken dat er door onze gemeente geen tickets zijn aangemaakt in bij deze partij. De kans dat er daadwerkelijk persoonsgegevens zijn gelekt, lijkt daardoor niet aannemelijk. Indien er toch persoonsgegevens gelekt zijn, betreffen dit de e-mail en naam van een beperkt aantal medewerkers. Vanuit de betreffende partij zijn de volgende maatregelen aanbevolen en uitgevoerd: - mogelijk accounts aanpassen in de betreffende software - Controleren van de logbronnen die toegang tot het portal en de betreffende software geven. Daarnaast zijn de customer support tickets gecontroleerd op de informatie die deze tickets bevatten en zijn de credential accounts gecontroleerd.	Nee
19-9-2025	Het verslag van het omgevingsoverleg van donderdag 18 september 2025 is per e-mail per abuis naar een onbevoegde ontvanger gestuurd. In dit verslag zijn twee adressen beschreven en de namen van de casushouder en casemanagers (beiden werknemers van de gemeente). Nadat bekend is geworden dat het verslag naar een onbevoegde ontvanger is gestuurd, is deze ontvanger verzocht om de e-mail te verwijderen.	Nee

20-10-2025	De gemeente stuurt brieven naar jubileumechtparen om de betreffende inwoners te feliciteren. In dit geval is de brief naar een verkeerd adres verzonden. De brief is door de onbevoegde ontvanger naar de gemeente geretourneerd.	Nee
20-10-2025	Een medewerker heeft de e-mail van een klant met daarin bankafschriften naar haar oude school e-mailadres verstuurd. Dit e-mailadres is geblokkeerd/verwijderd, maar er kan niet met zekerheid worden vastgesteld in hoeverre er nog e-mails ontvangen kunnen worden door het oude e-mailadres. Aangezien het e-mailadres van de medewerker zelf was, acht ik de kans dat er daadwerkelijk sprake is van een datalek niet aannemelijk. Wel noteer ik dit incident als dusdanig.	Nee
7-11-2025	Een gegevensformulier van een cliënt is als bijlage verzonden aan een andere cliënt. Het gaat om een formulier waarin NAW-gegevens en het BSN-nummer beschreven staat. De onbevoegde ontvanger heeft de medewerker op 6 november telefonisch op de hoogte gesteld van het datalek. Het gegevensformulier is op 13 november geretourneerd.	Nee
24-11-2025	Mail is per abuis verstuurd naar een foutief mailadres. Mailadres waar per abuis informatie naar is toegestuurd betreft die van een medewerker werkzaam binnen het COA. Enige aan de persoon te koppelen gegevens die in de mail vermeld staan is de voornaam van inwoner.	Nee

Met leveranciers en ketenpartners zijn verwerkers- of datalevering-overeenkomsten afgesloten om de beveiliging van privacygevoelige gegevens te borgen. De in deze overeenkomsten opgenomen informatiebeveiligingseisen zorgen ervoor dat de risico's aanzienlijk verkleind zijn.

Landelijk beeld datalekken
Voor het landelijk beeld van datalekken is gebruikgemaakt van de meest recente beschikbare cijfers van de Autoriteit Persoonsgegevens (AP), zoals opgenomen in het *Landelijk beeld meldingen van datalekken 2025*. Deze rapportage heeft betrekking op incidenten die hebben plaatsgevonden in 2024. De landelijke cijfers over 2025 waren ten tijde van het opstellen van dit jaarverslag nog niet beschikbaar.
Uit het landelijke beeld blijkt dat de AP in 2024 bijna 38.000 meldingen van datalekken ontving, een aanzienlijke stijging ten opzichte van het voorgaande jaar (circa 26.000 meldingen). Veel datalekken ontstaan doordat post of e-mail niet bij de juiste persoon terechtkomt. Ook onbedoelde of onrechtmatige inzage in persoonsgegevens vormt een veelvoorkomende oorzaak van datalekken.
Datalekken kunnen risico's opleveren voor de betrokkenen, zoals financiële schade door identiteitsfraude en oplichting. Organisaties zijn op grond van de Algemene verordening gegevensbescherming (AVG) verplicht om een datalek te melden bij de Autoriteit Persoonsgegevens wanneer sprake is van een risico voor de rechten en vrijheden van betrokkenen. De stijgende meldingsaantallen onderstrepen het belang van blijvende aandacht voor zorgvuldige omgang met persoonsgegevens en het treffen van passende organisatorische en technische beveiligingsmaatregelen.

Veel van de datalekken zijn administratieve vergissingen die vlot te herstellen lijken. Cyberaanvallen zoals gijzelsoftware, phishing of diefstal van data via malware worden minder vaak gemeld. Maar één succesvolle hack kan leiden tot de diefstal van tienduizenden klantgegevens, langdurige uitval van bedrijfsprocessen, verlies van gevoelige informatie, imagoschade of juridische aansprakelijkheid.

Bron: Autoriteit persoonsgegevens

9. Meerjarenperspectief

Inwoners, ondernemers en maatschappelijke instellingen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig omgaat met (persoons)gegevens. Betrouwbare informatiebeveiliging is een noodzakelijke voorwaarde voor continuïteit van de dienstverlening en een goed functionerende bedrijfsvoering.

Het gemeentelijk informatiebeveiligingsbeleid is gericht op het treffen en onderhouden van passende technische en organisatorische maatregelen, conform geldende wet- en regelgeving zoals de AVG en de Baseline Informatiebeveiliging Overheid (BIO). De Chief Information Security Officer (CISO) is verantwoordelijk voor coördinatie, toezicht en advisering over informatiebeveiliging en risicomanagement binnen de organisatie.

Jaarlijks worden belangrijke processen en wettelijke registraties – waaronder waardedocumenten, BRP, BAG, BGT, BRO, DigiD en Suwinet – beoordeeld via zelfevaluaties en externe audits. Hiermee wordt inzicht gehouden in het volwassenheidsniveau van de informatiebeveiliging en waar nodig bijgestuurd.

De digitalisering van de gemeentelijke dienstverlening neemt verder toe. Ontwikkelingen zoals plaats- en tijdonafhankelijk werken, toenemende afhankelijkheid van leveranciers en de opkomst van toepassingen op basis van kunstmatige intelligentie vergroten zowel kansen als risico’s. Dit vraagt om blijvende aandacht, tijdig anticiperen op nieuwe dreigingen en het structureel beschikbaar stellen van voldoende middelen. Wendbaarheid en weerbaarheid zijn daarbij essentieel.

9.1. Grootste risico’s voor gemeenten

De belangrijkste risico’s op het gebied van informatiebeveiliging en gegevensbescherming hebben een directe impact op de dienstverlening, bedrijfsvoering en het vertrouwen van inwoners.

Uitval van dienstverlening en bedrijfsvoering
Vrijwel alle gemeentelijke processen zijn afhankelijk van digitale systemen. Incidenten zoals ransomware-aanvallen, storingen of problemen bij leveranciers kunnen leiden tot tijdelijke of langdurige uitval van dienstverlening. In ernstige gevallen moeten processen worden stilgelegd, met directe gevolgen voor inwoners en ondernemers.

Vertrouwelijke informatie in verkeerde handen
Gemeenten verwerken grote hoeveelheden privacygevoelige en vertrouwelijke informatie, onder andere op het gebied van zorg, inkomen, veiligheid en gebiedsontwikkeling. Onbevoegde toegang tot deze gegevens kan leiden tot ernstige schade voor betrokkenen, reputatieschade voor de gemeente en mogelijke sancties op grond van de AVG.

Fouten in de dienstverlening
Aantasting van de kwaliteit en integriteit van informatie kan leiden tot onjuiste besluiten, fouten in processen en inefficiënt herstelwerk. Dit risico vraagt nadrukkelijk aandacht, omdat fouten in data direct doorwerken in de kwaliteit van de gemeentelijke dienstverlening en het vertrouwen in de overheid.

9.2. Dreigingsbeeld 2025 – 2026

De gemeentelijke CISO, ISO, PO, FG kunnen, onder verwijzing naar dit dreigingsbeeld management, directie en bestuur adviseren over digitale risico's op zo'n manier dat het de gemeente helpt om snel, efficiënt, effectief en zo foutloos mogelijk haar werk te doen, waarbij maximaal gebruik wordt gemaakt van de mogelijkheden en kansen die moderne technologie ons biedt.

Actueel dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2025–2026

Bron: Informatiebeveiligingsdienst (IBD), VNG

De Informatiebeveiligingsdienst (IBD) constateert dat Nederlandse gemeenten te maken hebben met een structureel en complex digitaal dreigingslandschap. Digitale incidenten raken direct de continuïteit van de gemeentelijke dienstverlening en het vertrouwen van inwoners en ondernemers. Het dreigingsbeeld voor 2025–2026 laat zien dat met name drie typen dreigingen structureel en dominant zijn: ransomware, kwetsbaarheden in software en risico's in ketens en bij leveranciers.

1. Ransomware blijft de grootste dreiging, met ontwrichtende gevolgen

Ransomware is en blijft de nummer één dreiging voor gemeenten. Criminelen maken gebruik van kwetsbaarheden in gemeentelijke systemen of bij leveranciers om toegang te krijgen tot netwerken. Daarbij worden gegevens gestolen, versleuteld en vervolgens ingezet voor afpersing. Steeds vaker dreigen aanvallers met het openbaar maken van privacygevoelige gegevens van inwoners, bedrijven en medewerkers wanneer geen losgeld wordt betaald.

In de periode 2023–2024 waren ruim 150 gemeenten direct of indirect betrokken bij ransomware-incidenten, veelal via de leverancierskete. In meerdere gevallen leidde dit tot langdurige uitval van dienstverlening, hoge herstelkosten en ernstige reputatieschade. De maatschappelijke en financiële impact van dergelijke aanvallen is aanzienlijk en vaak langdurig merkbaar.

2. Toenemend aantal en ernst van kwetsbaarheden in software
Gemeenten zijn in hoge mate afhankelijk van digitale systemen en standaardsoftware. Alle software bevat kwetsbaarheden die door kwaadwillenden kunnen worden misbruikt. De IBD ziet dat niet alleen het aantal kwetsbaarheden toeneemt, maar vooral ook het aantal kwetsbaarheden met een hoge kans op misbruik en grote impact.

Hoewel het oplossen van kwetsbaarheden vaak bestaat uit het tijdig installeren van updates, blijkt dat dit in de praktijk niet altijd eenvoudig is. Gemeenten hebben te maken met complexe applicatielandschappen, beperkte capaciteit en afhankelijkheid van leveranciers. Incidenten laten zien dat uitgestelde of onvolledig uitgevoerde updates kunnen leiden tot grootschalige verstoringen en datalekken.

3. Risico's in ketens en bij leveranciers blijven grotendeels buiten zicht
Gemeenten opereren in uitgebreide netwerken van samenwerkingsverbanden en externe leveranciers. Gemiddeld nemen gemeenten deel aan tientallen samenwerkingsconstructies en wordt een steeds groter deel van de ICT als dienst afgenomen, bijvoorbeeld via SaaS- en cloudoplossingen. Incidenten bij leveranciers hebben daardoor regelmatig directe gevolgen voor meerdere gemeenten tegelijk.

De IBD constateert dat informatiebeveiliging en privacy in samenwerkingsafspraken en contracten nog onvoldoende expliciet en afdwingbaar zijn geregeld. Hoewel gemeenten vertrouwen op externe partijen, is het daadwerkelijke zicht op risico's en de naleving van beveiligingsmaatregelen beperkt. In de afgelopen jaren zijn gemeenten herhaaldelijk geconfronteerd met datalekken en procesverstoringen die zijn ontstaan bij derde partijen, terwijl de impact volledig bij de gemeente terechtkwam.

Bestuurlijke opgave: digitale veiligheid als kerntaak
Het actuele dreigingsbeeld onderstreept dat digitale veiligheid geen operationeel detail is, maar een bestuurlijke kernverantwoordelijkheid. Nieuwe wet- en regelgeving, zoals de aankomende Cyberbeveiligingswet, maakt deze verantwoordelijkheid expliciet. Volgens de IBD vraagt dit om

structurele aandacht voor risicomanagement, investeringen in basismaatregelen, versterkt leveranciersmanagement en intensieve samenwerking tussen gemeenten.

Speerpunten van de Nederlandse Cybersecuritystrategie 2022–2028

Bronnen: Nederlandse Cybersecuritystrategie (NLCS) 2022–2028, NCTV / NCSC

De Nederlandse samenleving is in toenemende mate afhankelijk van digitale systemen. Deze ontwikkeling brengt groeiende risico's met zich mee voor de continuïteit, integriteit en betrouwbaarheid van maatschappelijke en economische processen. Digitale veiligheid en cyberweerbaarheid zijn daarom essentiële randvoorwaarden voor een goed functionerende samenleving.

Met de Nederlandse Cybersecuritystrategie 2022–2028 (NLCS) schetst het kabinet de visie en ambities voor een digitaal weerbaar Nederland. De strategie richt zich op het versterken van een veilig digitaal ecosysteem waarin overheid, bedrijfsleven en maatschappelijke organisaties gezamenlijk verantwoordelijkheid dragen voor cybersecurity. De uitvoering van de strategie wordt gecoördineerd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), met een belangrijke rol voor het Nationaal Cyber Security Centrum (NCSC).

De NLCS kent vier samenhangende pijlers:

1. Digitale weerbaarheid van overheid, bedrijven en maatschappelijke organisaties
De overheid zet in op het verhogen van de digitale weerbaarheid van organisaties door beter zicht te krijgen op cyberdreigingen, risico's en incidenten. Dit gebeurt onder meer door het versterken van detectiecapaciteit, informatie-uitwisseling en samenwerking binnen het Landelijk Dekkend Stelsel van cybersecuritysamenwerkingsverbanden. Organisaties worden gestimuleerd en waar nodig verplicht om proportionele en risicogebaseerde beveiligingsmaatregelen te nemen, passend bij hun rol en maatschappelijke impact.

2. Veilige en innovatieve digitale producten en diensten
Digitale veiligheid moet het fundament vormen waarop nieuwe digitale producten en diensten worden ontworpen en aangeboden. De strategie benadrukt een grotere verantwoordelijkheid voor leveranciers en dienstverleners om gedurende de gehele levenscyclus zorg te dragen voor veilige producten. Europese en nationale wet- en regelgeving, zoals de NIS2-richtlijn en de aankomende Cyberbeveiligingswet, stellen strengere en toetsbare eisen aan overheden, vitale aanbieders en leveranciers van digitale producten en diensten.

3. Tegengaan van digitale dreigingen van staten en criminelen
De Nederlandse overheid investeert in het vergroten van inzicht in digitale dreigingen van statelijke actoren en cybercriminelen. Dit omvat het versterken van analysecapaciteit, opsporing, attributie en respons, evenals internationale samenwerking en diplomatieke inzet. Doel is om digitale dreigingen tijdig te onderkennen, te beperken en waar nodig actief tegen te gaan, ter bescherming van nationale veiligheidsbelangen.

4. Voldoende cybersecurityspecialisten, kennis en digitale weerbaarheid van burgers
Een structureel tekort aan cybersecurityspecialisten vormt een risico voor de digitale weerbaarheid van Nederland. De strategie richt zich daarom op het versterken van de cybersecurity-arbeidsmarkt, het bevorderen van kennis en innovatie, en het vergroten van digitale weerbaarheid bij burgers. Dit gebeurt onder meer via onderwijs, opleidingsprogramma's en bewustwordingsinitiatieven.

Versterking van het nationale cybersecuritystelsel
Als onderdeel van de uitvoering van de strategie wordt het nationale stelsel voor digitale veiligheid versterkt en vereenvoudigd. Het NCSC speelt hierin een centrale rol en ontwikkelt zich, in samenhang met andere publieke taken en op Europese regelgeving, richting één samenhangende nationale cybersecurityautoriteit. Deze autoriteit ondersteunt publieke en private partijen met dreigingsinformatie, handelingsperspectief en, waar wettelijk mogelijk, incidentrespons.

Wake-up call!

Meest getroffen branches in 2025/2026:
Op basis van recente monitors (zoals de Cybersecuritymonitor 2024/2025 en het CSBN 2025) vallen de volgende trends op:

- **Onderwijs:** Deze sector werd in het begin van 2025 het hardst getroffen met een gemiddelde van **4.484 aanvallen** per organisatie per week (een stijging van 73%).

- **ICT-sector:** Ransomware-aanvallen troffen deze branche relatief het vaakst (24% van de gevallen), gevolgd door de handel (20%) en de industrie (13%).

- **Gezondheid en Welzijn:** Volgens de Autoriteit Persoonsgegevens blijft dit de sector met het hoogste aantal gemelde datalekken.

- **Overheid & Telecom:** Het Cybersecuritybeeld Nederland 2025 (CSBN) meldt een toename in incidenten bij overheidsinstanties (zoals het OM) en benadrukt de hoge impact van aanvallen op de telecomsector vanwege de afhankelijkheid van andere sectoren.

Belangrijkste inzichten over gemeenten in 2025:

- **Toename meldingen:** Het jaarverslag van de AP over 2025 meldt een stijging in het aantal klachten en datalekken over de gehele breedte, waarbij de publieke sector een belangrijk doelwit bleef.

- **Interne incidenten:** Op Datalekt.nl zijn specifieke meldingen te vinden, zoals bij de Gemeente Eindhoven in augustus 2025, waarbij een publicatie van een geheime verhuisvergoeding alsnog als datalek werd gemeld (oorzaak: menselijke fout/intern).

- **Privacyboetes:** In februari 2026 werd bekend dat verschillende Nederlandse gemeenten privacyboetes hebben ontvangen naar aanleiding van incidenten in 2025.

Hoewel we er alles aan doen om de risico's zo klein mogelijk te maken zijn incidenten ook voor Midden-Delfland niet uit te sluiten.

“The only system that is truly secure is one that is switched off, cast in concrete, and buried deep underground.”

Gene Spafford (computer scientist)

Gemeente Midden-Delfland
Anna van Raesfeltstraat 37
2636 HX Schipluiden
gemeente@middendelfland.nl
www.middendelfland.nl

Cittaslow Midden-Delfland
Kwaliteit van leven