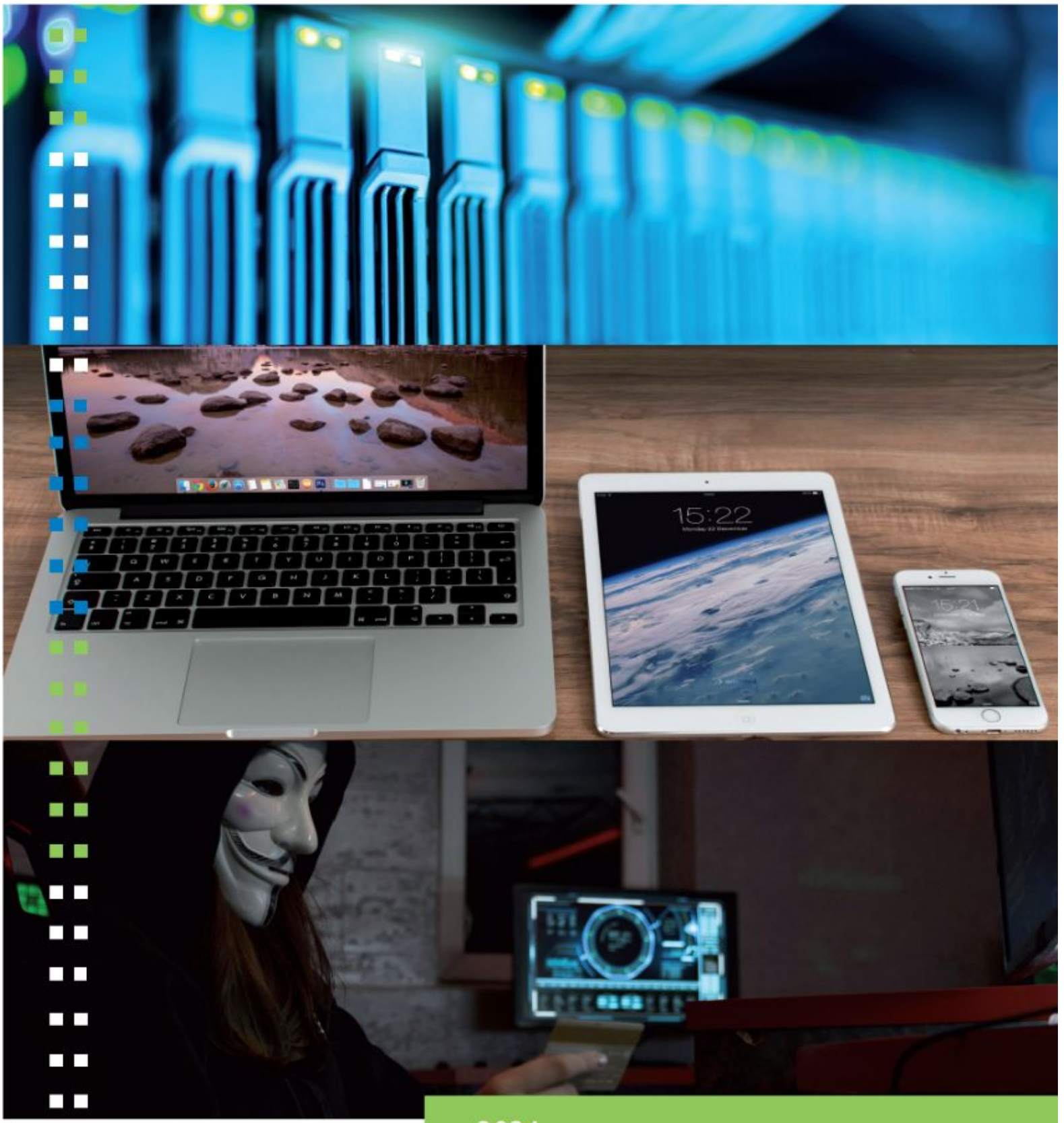


Gemeente Midden-Delfland

2024

Jaarverslag Informatiebeveiliging Midden-Delfland

cittaslow

1. Inhoudsopgave

Managementsamenvatting....3
2. Inleiding....5
3. IB-beleid, doelstellingen en ambities....6
3.1. Wat is informatiebeveiliging?....6
3.2. Baseline Informatiebeveiliging Overheid (BIO)....6
3.3. Informatieveiligheid is geborgd in de organisatie....6
3.4. Uitgangpunten en doelen van ons informatiebeveiligingsbeleid....7
3.5. Relatie met privacy....8
4. ENSIA (Eenduidige Normatiek Single Information Audit)....9
4.1. Aanleiding....9
4.2. Uitvoering van ENSIA 2024....10
4.3. Verantwoordingsrapportages zelfevaluatie 2024....11
4.4. Resultaten zelfevaluaties per stelsel....12
4.4.1. Zelfevaluaties BRP en PUN....12
4.4.2. Zelfevaluatie basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO)....13
5. Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet....15
6. Samenvattend beeld en resultaten informatiebeveiliging 2024....16
6.1. Achtergrond....16
6.2. Resultaat meting BIO....17
6.3. Algemene Verordening Gegevensbescherming (AVG)....18
7. Disclaimer....20
8. Realisatie doelstellingen IB-beleid....21
8.1. Controls & beheersmaatregelen IB....22
8.2. Jaarplan Informatiebeveiliging 2025 met verbeterpunten....23
8.3. Nieuwe wet- en regelgeving over informatiebeveiliging....26
9. Incidenten, ontdekte kwetsbaarheden en datalekken....28
9.1. Gemelde incidenten en kwetsbaarheden....28
9.2. Gemelde datalekken....28
10. Meerjarenperspectief....31
10.1. Grootste risico’s voor gemeenten....31
10.2. Dreigingsbeeld 2025 – 2026....32

Managementsamenvatting

Het College van B&W van gemeente Midden-Delfland legt jaarlijks verantwoording af over het informatiebeveiligingsbeleid. Dit jaarverslag Informatiebeveiliging Midden-Delfland 2024 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) 2024 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 2024 en de DigiD/Suwinet-audit. De verbeterpunten met de hoogste risico's vormen het informatiebeveiliging jaarplan 2025.

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 2024

In 2024 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 is 2025 verder.
- We stemden onze eisen uit de BIO, die gerelateerd zijn aan het ICT beheer door gemeente Westland af met gemeente Westland. Het gaat vooral om de bedieningsprocedures, het monitoren van ons datanetwerkverkeer, hoe zij omgaan met (controle op) logging, het installeren van software en het beheer van technische kwetsbaarheden en meldingen. Het wordt in de praktijk goed uitgevoerd, maar uitgangspunt is om dit ook helder vastgelegd te hebben voor de veranderde systemen die ingericht worden vanuit de projecten rond de verSAASing en de nieuwe Cloudtechnologie.
- In combinatie met voorlichting over privacy zal informatiebeveiliging continu onder de aandacht van de medewerkers worden gebracht. Dit doen we door middel van een e-learning oplossing. Hiermee krijgen we door monitoring meer inzicht in de kennis en vaardigheden van onze medewerkers, waarop we vervolgens gerichter kunnen sturen. Daarnaast zijn er aan teams met gevoelige informatie speciale "social hacktrainingen" gegeven om meer bewustzijn te creëren.
- We hebben het beleid op hybride werken vastgesteld en hebben additionele regels opgesteld over het gebruik van mobiele apparatuur, fysieke beveiliging en communicatieverbindingen.
- We hebben samen met de gemeente Westland een Europese aanbesteding gevoerd voor een de levering en implementatie van een SIEM&SOC-dienstverlening.

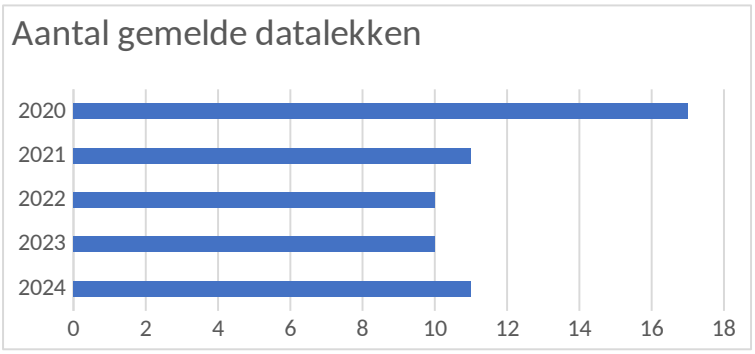
Beveiligingsincidenten

In 2024 zijn 21 spammails, 12 incidenten en 116 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) en betroffen geconstateerde kwetsbaarheden in software met daarbij het advies over hoe deze zijn te verhelpen.

Datalekken

In 2024 zijn 11 datalekken gemeld bij de privacy officer.

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



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 een 100% score goed op de norm.
- De **BAG** scoort met 94% ruim voldoende, derhalve worden nog verbeteracties voorgesteld.
- De **BGT** scoort met 98% goed op de norm.
- De **BRO** scoort met 97% goed op de norm.
- De gemeente Midden-Delfland is **DigiD** aansluithouder voor de Persoonlijke Internetpagina en webformulieren van ons zaaksysteem (xxllnc zaken). Door een externe IT-auditor is vastgesteld dat niet helemaal wordt voldaan aan het vastgestelde normenkader. Het niet aan alle normen voldoen over DigiD ligt bij de leverancier van de cloudapplicatie. Deze heeft inmiddels herstelacties doorgevoerd. Dit is ook bekend bij de landelijke toezichthouder Logius.
- Over het gebruik van **Suwinet** is door een externe IT-auditor vastgesteld dat op alle onderdelen wordt voldaan aan het gestelde normenkader.

Tijdens de audit voor DigiD is naast toetsing op aanwezigheid van genomen maatregelen voor het eerst ook getoetst op de werking over de 2e helft van 2024. De auditor heeft wel aandacht gevraagd voor de uitbreiding van de controleperiode op werking op meer normen, en over het gehele jaar 2025. Hierbij moeten we rekening houden met het aanpassen van interne controle-processen en het creëren van bewijslast.

Vooruitblik 2025 op het gebied van de informatiebeveiliging
Activiteiten voor 2025:

- We actualiseren ons Strategisch Informatiebeveiligingsbeleid volgens de nieuwe Cyberbeveiligingswet en BIO 2.0.
- We stellen AI-beleid op als leidraad voor het gebruik van AI toepassingen.
- We stellen een overzicht samen van wie contact onderhoudt met welke overheidsinstanties en toezichthouders met betrekking tot informatiebeveiliging.
- We organiseren verplichte trainingen voor bestuurders, zodat zij de risico's van cyberveiligheid beter begrijpen en integreren in regulier risicobeheer.
- We actualiseren ons dataclassificatie-overzicht en implementeren labelprocedures in de vakapplicaties.
- We verbeteren het beheer van toegangsrechten binnen vakapplicaties, waarbij functioneel applicatiebeheerders een centrale rol krijgen.
- We plannen een cybercrisisoefening die gericht is op het vergroten van bewustwording en het testen van beveiligingsmaatregelen.
- We implementeren een SIEM/SOC-systeem om kwetsbaarheden en beveiligingsincidenten vroegtijdig te signaleren en daarop te reageren.
- We werken onze bedrijfscontinuïteitsplannen verder uit, met extra aandacht voor noodscenario's voor cruciale processen zoals burgerzaken.
- We voeren penetratietesten uit om inzicht te krijgen in de effectiviteit van beveiligingsmaatregelen en om risico's te verkleinen.
- We rollen het ISMS breder uit en versterken de controle en verbetering door interne audits.
- We passen onze processen en informatiebeveiligingsorganisatie aan op aangescherpte regelgeving zoals NIS 2, de Cyberbeveiligingswet en de BIO 2.0.

2. 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 2024 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 zevende jaarverslag over onze informatiebeveiliging geven we uitvoering aan de verantwoordingsplicht naar de gemeenteraad.



3. 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.

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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 als Chief Information Officer (CIO) 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.

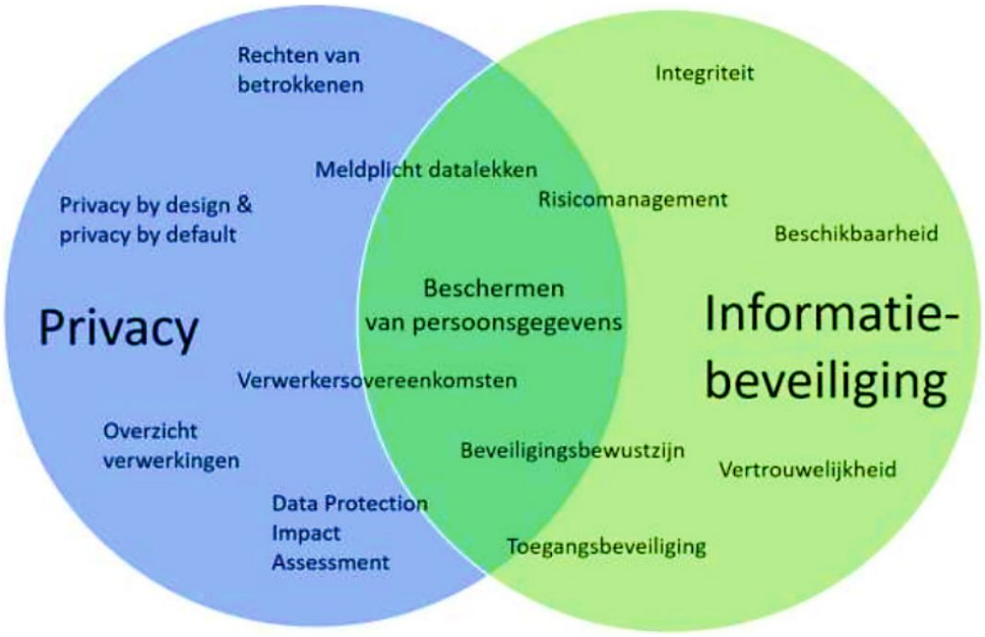
1. *Bestuurders bevorderen een veilige cultuur.*
2. *Informatiebeveiliging is van iedereen.*
3. *Informatiebeveiliging is risicomanagement.*
4. *Risicomanagement is onderdeel van de besluitvorming.*
5. *Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.*
6. *Informatiebeveiliging is een 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.

3.5. 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



4. ENSIA (Eenduidige Normatiek Single Information Audit)

4.1. 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.

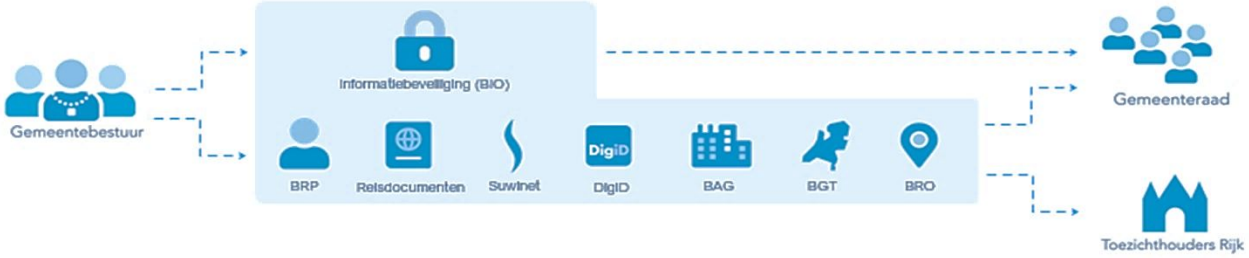
Hoewel ENSIA bedoeld is om audits te vereenvoudigen, nemen de werkzaamheden jaarlijks toe. Dit komt door uitbreiding van normenkaders, nieuwe wet- en regelgeving, en een groeiend aantal domeinen waarop informatieveiligheid en privacy van toepassing zijn.

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..

4.2. Uitvoering van ENSIA 2024

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 2024 grafisch weergegeven. Meer informatie over ENSIA en de werkwijze is terug te vinden op www.ensia.nl.

Afbeelding: grafische weergave ENSIA verantwoordingsproces 2024



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 2024	Vragenlijsten: • RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). • BKWI: Informatiebeveiliging Suwinet (BIO). • Logius: Informatiebeveiliging DigiD. • DGBRW: 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 2024	Producten: • Collegeverklaring over Suwinet en DigiD. • Rapportage BAG, BGT en BRO door college van B&W. • Rapportage BRP en Reisdocumenten. • Rapportage ENSIA voor de gemeenteraad.
Verantwoorden	• Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W. • Uploaden en aanleveren verantwoordingsrapportages via ENSIA (Resultaten BRP en Reisdocumenten verwerken in de uittreksels uit de Kwaliteitsmonitor en daar uploaden).	30 APR 2025	Resultaten: • De toezichthouders Logius en DGBRW en BKWI krijgen via ENSIA de verantwoordingsrapportages aangeleverd. • RvIG krijgt de informatie uit de Uittreksels BRP en Reisdocumenten 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 2025	• 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 2024 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 2024 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 per auditonderdeel (Suwinet en DigiD) richting de betreffende landelijke toezichthouder. 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 2024.
In paragraaf 3.3 vindt u de conclusies uit de betreffende verantwoordingsrapportages.

4.3. Verantwoordingsrapportages zelfevaluatie 2024

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

De verantwoordingsrapportage 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 2024 en de op basis van de BIO geïmplementeerde maatregelen.

4.4. 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.

4.4.1. 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).

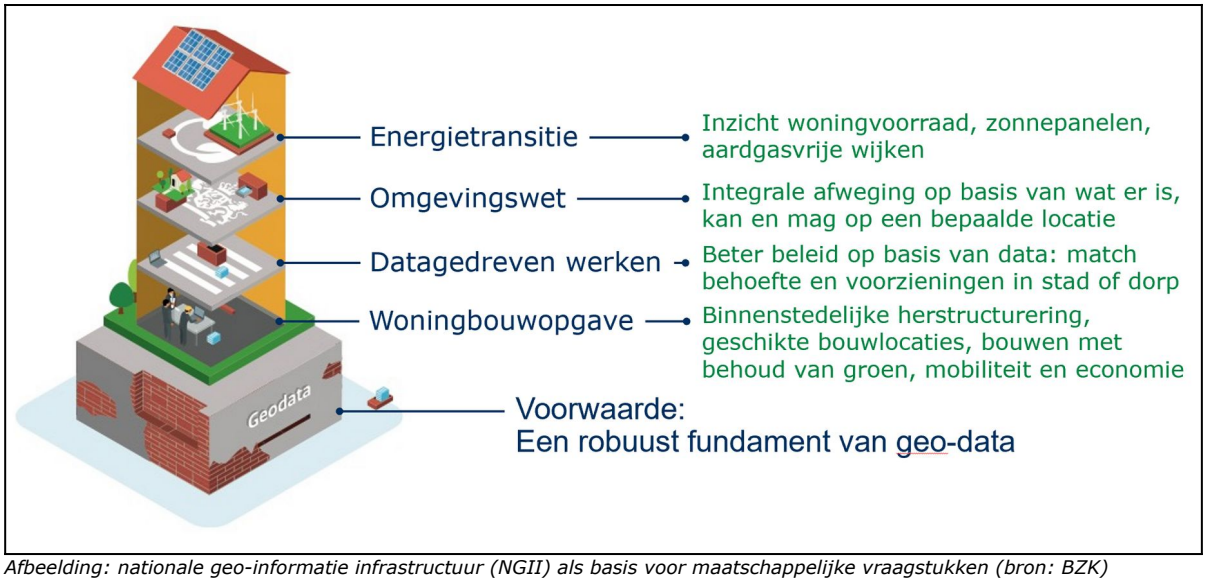
Jaarlijks moeten gemeenten verantwoording afleggen over het gebruik van de BRP en de reisdocumenten. Met de komst van ENSIA is het inhoudelijke deel afgesplitst van het beveiliging technische deel. Het inhoudelijke deel, dat onder andere kijkt naar de kwaliteit van de persoonsgegevens in het BRP en de 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 2024 (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	400	400	100 %
Totaal	1.200	1.200	100%

Resultaat uit zelfevaluatie informatieveiligheid Reisdocumenten 2024 (ENSIA)			
Thema Reisdocumenten	**Totaal behaalde punten Midden-Delfland**	**Totaal mogelijk totaal**	**Percentage**
1. Organisatie van de beveiliging	400	400	100 %
2. Toegangsbeveiliging	400	400	100 %
3. Naleving	400	400	100 %
Totaal	1.200	1.200	100 %

4.4.2. 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)

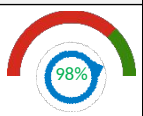
Wij leggen als bronhouderorganisatie verantwoording af over het beheer van de basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO). Dat doen we intern richting de gemeenteraad en aan het Rijk via het directoraat-generaal Bestuur, Ruimte en Wonen van het ministerie 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.

We hebben in 2024 een mutatiesignalering BAG uitgevoerd op basis van de luchtfoto 2024. De resultaten zijn bekeken, gecontroleerd en in de BGT en BAG verwerkt. Daarnaast is het processenhandboek BAG is geactualiseerd en er wordt er volgens dit handboek gewerkt. De processen tussen de BAG en BGT en de BGT en de BOR zijn geactualiseerd en afgestemd met de betrokken afdelingen. Er wordt gewerkt volgens het processenhandboek BGT.
We hebben in 2024 een mutatiesignalering BGT (zachte topografie) uitgevoerd en bekeken. De wijzigingen zijn in februari 2024 gekarteerd in de BGT. Alle kwaliteitseisen BGT zoals genoemd in het jaarplan 2024 zijn gehaald.
In 2024 hebben we ook het objectenhandboek BGT aangevuld.
Voor wat betreft de BRO hebben we de processen zijn beter ingebed in de organisatie.
De sondeergegevens en watermonitoringgegevens zijn nu zichtbaar in onze gemeentelijke GIS-viewer. Hierdoor kunnen de collega's gemakkelijker deze gegevens raadplegen.

Scores geo-basisregistraties 2024 (tijdvak 1 januari 2024 tot en met 31 december 2024):

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		Indien aanlevering van aannemers niet NEN-conform is, dus niet volgens de richtlijn, dan aanpassen c.q. verduidelijken contracten.

< 60% Onvoldoende vanaf 60% voldoende

Trend score geo-basisregistraties

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

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

Voorgestelde verbetermaatregelen voor 2025
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.
- We voeren mutatiesignalering uit met de luchtfoto uit het voorjaar 2025.
- De resultaten van de mutatiesignalering verwerken we in de BGT en de BAG.
- We houden continu zicht op het BAG-proces en passen bij wijzigingen het processenhandboek aan. Op deze manier zorgen we er voor dat de mutaties tijdig verwerkt kunnen worden

BGT
- We voeren mutatiesignalering BGT (zachter topografie) uit met de luchtfoto uit het voorjaar 2025.
- We geven uitvoering geven aan de kwaliteitseisen BGT zoals genoemd in het jaarplan 2025
- We realiseren koppeling met de BOR naar verwachting in het eerste halfjaar van 2025.
- De processen met de BAG en de BOR controleren we en werken we waar nodig bij.
- We controleren het Handboek objectenboek en vullen waar nodig aan.

BRO
- We controleren de processen van de BRO en werken deze waar nodig bij.
- We voeren de 5e tranche, milieukwaliteit in, die op 1 juli 2025 in werking treedt. Hiervoor werken we de processen bij.

5. Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en 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 DigiD en Suwinet.

Bij de ENSIA vragenlijsten is geconstateerd dat bij gemeente Midden-Delfland op 31 december 2024 de onze interne beheersingsmaatregelen in opzet en bestaan voldoen aan alle geselecteerde normen inzake DigID. Door een externe IT-auditor is echter vastgesteld dat op externe beheersingsmaatregelen niet helemaal wordt voldaan aan het gestelde normenkader. Het niet aan alle normen voldoen over DigiD ligt bij de leverancier van de cloudapplicatie. Deze heeft inmiddels herstelacties doorgevoerd. Dit is ook bekend bij de landelijke toezichthouder Logius.



Voor wat betreft de normen inzake Suwinet is geconstateerd dat 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 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. Deze documenten zijn van belang voor de verticale verantwoording aan de departementen.

6. Samenvattend beeld en resultaten informatiebeveiliging 2024

6.1. Achtergrond

Dit is het zevende jaarverslagslag is over onze informatiebeveiliging. Vorig jaar gaven we u een beeld van onze activiteiten en behaalde resultaten vanaf het moment dat we in 2015 gestart zijn met ons informatiebeveiligingsbeleid. In dit verslag beperken wij ons tot de activiteiten en behaalde resultaten van het afgelopen jaar ten opzichte van een meting over 2023.

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. In 2023 hebben we ons Strategisch Informatiebeveiligingsbeleid vervangen door een geactualiseerde versie.

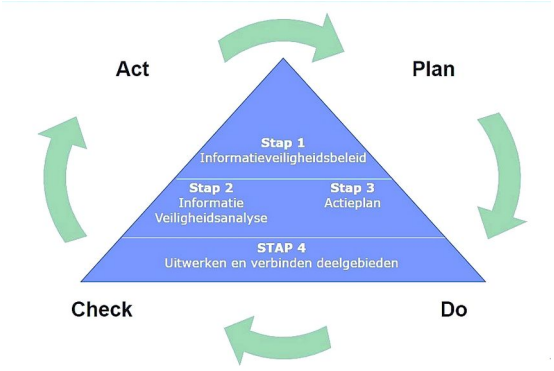
We zijn als gemeente aangesloten bij de Informatiebeveiligingsdienst (IBD).
De IBD is de sectorale CERT / CSIRT (Computer Emergency Response Team en Computer Security Incident Response Team)voor alle Nederlandse gemeenten. Het is onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt 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

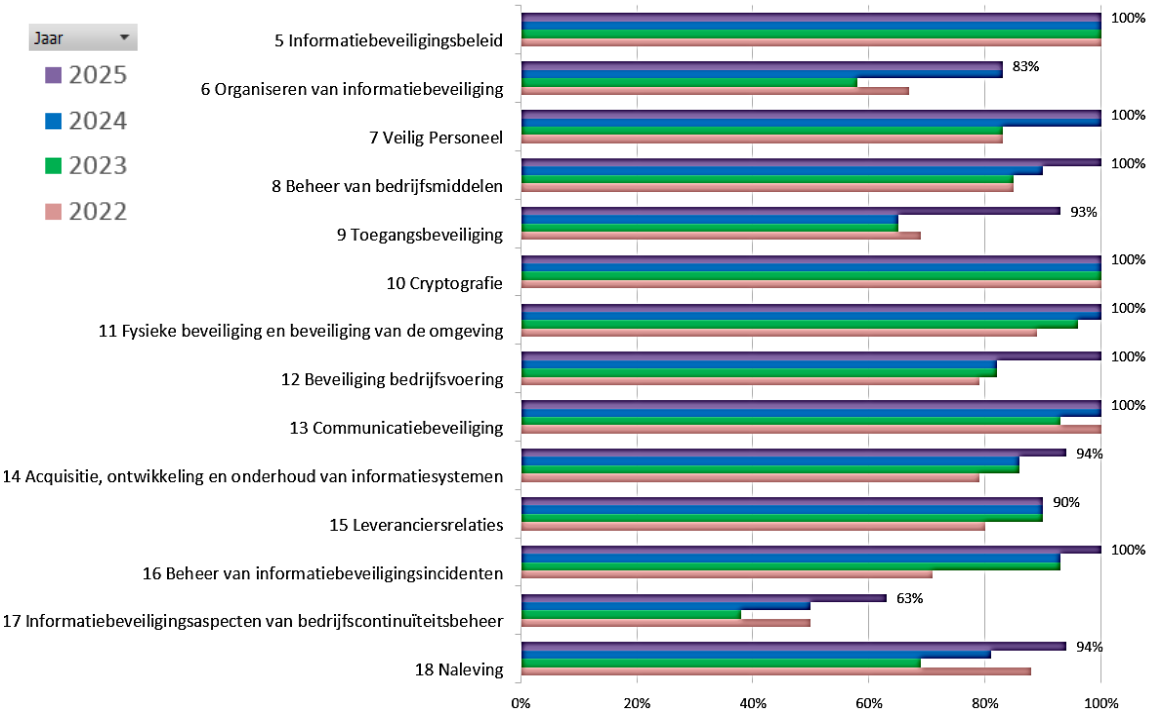
Om het informatiebeveiligingsbeleid goed te implementeren, werken we op basis van een "GAP-analyse/risicoanalyse". Deze analyses zijn uitgevoerd in directe samenspraak met de betrokken collega's van de vakafdelingen. Hiermee is het "GAP" of "gat" tussen de huidige en de gewenste situatie (volgens de 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 en 2024.



6.2. Resultaat meting BIO

Op basis van de resultaten ENSIA 2024 is begin 2025 een meting uitgevoerd op de 112 normen in de BIO. Grafisch ziet het resultaat van meting 4 uit ons ISMS er als volgt uit:



Tabel 1 De in de grafiek getoonde onderdelen betreffen de hoofdstukken uit de BIO (meting uit maart 2025).

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

Zo is het beleid op het hybride werken (thuiswerken) uitgebreid met nieuwe bruikleen- richtlijnen en overeenkomsten voor het gebruik van mobiele apparatuur. In 2024 is ook doorgegaan met het vormgeven van bedrijfscontinuïteitsmanagement. Daarnaast hebben we het ISMS verder ingericht en uitgerold.-

Hoofdstuk 12 is verbeterd, dat heeft vooral te maken met de verduidelijking van het bij Westland belegde ICT-beheer in zoals beschreven dienstverleningsovereenkomst. We stemmen de eisen uit de BIO die gerelateerd zijn aan het ICT beheer door Westland af met Westland. Het gaat vooral om de bedieningsprocedures, het monitoren van ons datanetwerkverkeer, hoe zij omgaan met (controle op) logging, het installeren van software en het beheer van technische kwetsbaarheden. -

Op de te nemen maatregelen van hoofdstuk 17 van de BIO ofwel informatieveiligheidsaspecten van bedrijfscontinuïteit hebben we een aantal verbeterstappen gezet. Vorig jaar haalden we nog een score van 50% we zijn op dat punt gestegen naar 63%. 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 2024 is gestart mom andere kwetsbare processen noodscenario's op te stellen zoals voor de processen rond burgerzaken. Dit krijgt in 2025 vervolg waarbij we kijken naar een andere totaaloplossing voor zowel fysieke uitwijk als het snel beschikbaar krijgen van gebruikte systemen.

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 2025 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) 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 dan ook een continu aandachtspunt.

6.3. 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 2024 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 2024.

"De bescherming van persoonsgegevens is niet alleen een juridische kwestie,

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

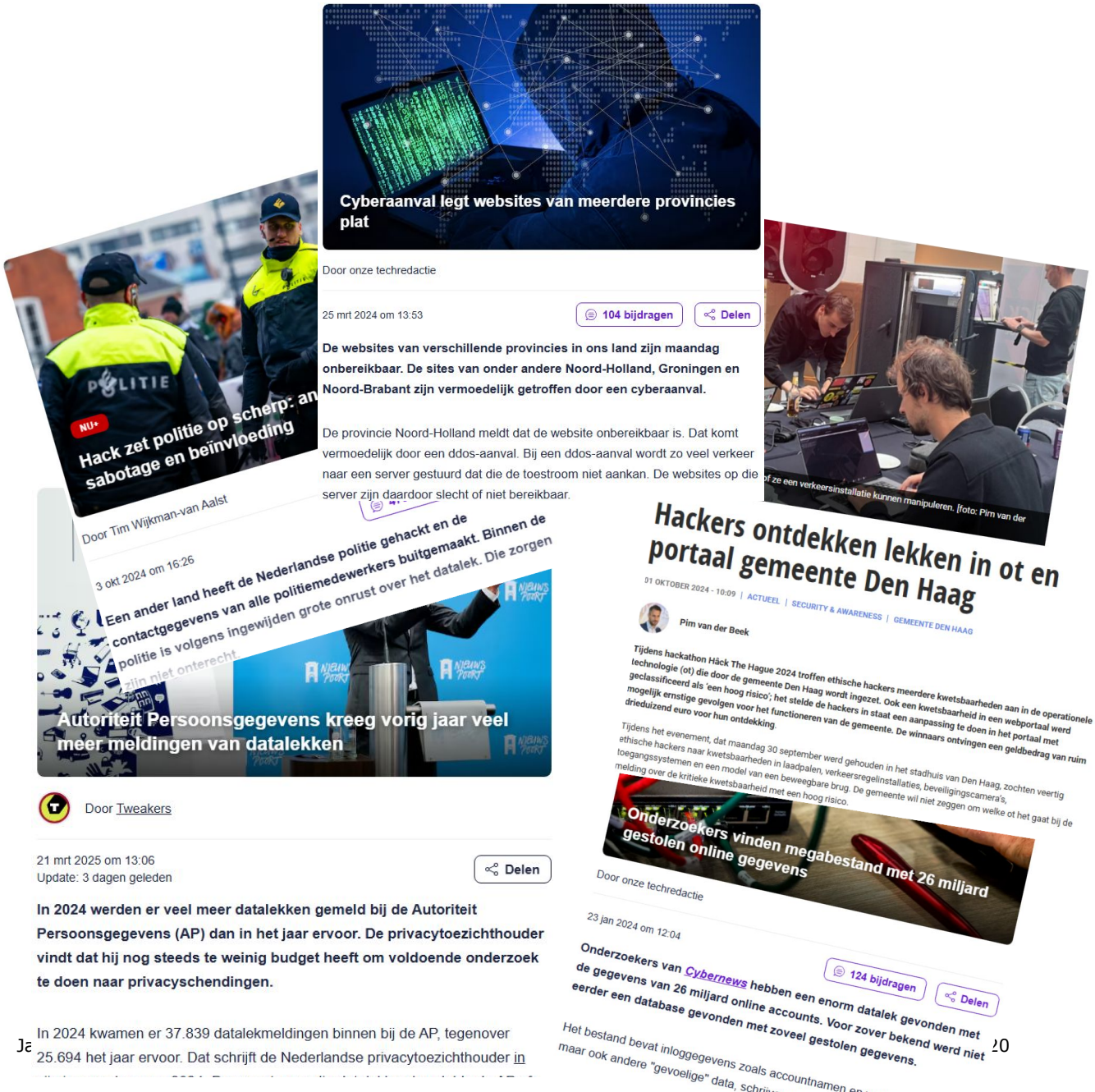
maar ook een morele verantwoordelijkheid."

– Aleid Wolfsen –

voorzitter van de Autoriteit Persoonsgegevens

7. 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.



8. 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. In december 2019 is het op de BIO gebaseerde nieuwe informatiebeveiligingsbeleid 2020-2023 vastgesteld. We hebben de verplichting dit elke 3 jaar te actualiseren. In 2023 is ons nieuwe informatiebeveiligingsbeleid voor 2023-2026 door het college van burgemeester en wethouders vastgesteld. Naar verwachting actualiseren we dit beleid in 2025 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 2025 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 2025 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.

8.1. 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 starten we met de nieuwe op de BIO 2.0 gebaseerde risicoanalyse aanpak volgens het Business Model Canvas (BMC) en het Risk Model Canvas (RMC).
Deze gebruiken we ook bij de risicoanalyse van nieuwe gemeentelijke taken, processen of voor een nieuw informatiesysteem. De uitkomsten van de analyse vormt dan input voor de eventueel te nemen additionele beveiligingsmaatregelen, welke in de definitiefase van het project nader worden uitgewerkt.
Het resultaat van de baselinetoets of risicoanalyses kan duiden op een zwaartepunt in het te beschermen belang, er is bijvoorbeeld een behoefte op Beschikbaarheid, maar niet op Integriteit en Vertrouwelijkheid. In de daarna uit te voeren risicoanalyse dient in dit voorbeeld dan de nadruk te

liggen op verhogen van Beschikbaarheid. Ook geeft de opgeleverde dataclassificatie de volgorde van voor het opnieuw operationeel maken van systemen aan bij uitval.

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)

8.2. Jaarplan Informatiebeveiliging 2025 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 2025 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 2025 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 2025 meer aandacht krijgen.
16 (+ 7,17 en 18)	Beheer van informatiebeveiligings-incidenten	We plannen in de 2e helft van 2025 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.
12.4	Verslaglegging en Monitoring	Samen met de gemeente Westland is de aanbesteding van een SIEM/SOC afgerond de implementatie hiervoor is naar verwachting medio juni 2025 voltooid. SIEM is een systeem dat alle beschikbare informatie binnen de ICT-infrastructuur, dat een relatie heeft met informatie beveiliging, verzamelt en analyseert. Op basis van deze analyses kunnen kwetsbaarheden ontdekt worden en kunnen aanvallen en verdacht gedrag in een vroeg stadium worden gesignaleerd. Het SOC is de dienstverlener met medewerkers die de output van het SIAM kunnen analyseren en op acteren in geval van ontdekte incidenten en/of kwetsbaarheden.
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 krijgt in 2025 vervolg waarbij we kijken naar een andere totaaloplossing voor zowel fysieke uitwijk als het snel beschikbaar krijgen van gebruikte systemen.
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 2025 een vervolg.
18.2.2	Beoordeling van technische naleving	We voeren in 2025 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 sinds 2024 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 2025 met de betreffende domeinbeheerders werkbare processen in ons ISMS. Daarnaast actualiseren we in 2025 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. Daarbij is met name aangegeven dat vanaf verantwoordingsjaar 2025 deze normen op vrijwillige basis kunnen worden getoetst door de auditor en dat dit vanaf verantwoordingjaar 2026 de toets op werking verplicht wordt. We moeten daarbij aantoonbaar zorgen 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). We moeten daarvoor gedurende het jaar controleren op het naleven van de beheersmaatregelen met betrekking tot:

- het toekennen en intrekken van toegangsrechten van gebruikers en beheerders.
- het registreren, loggen, analyseren en beoordelen van uitzonderingen op gebruikersactiviteiten en informatiebeveiligingsincidenten.
- nieuwe medewerkers maximaal binnen drie maanden na indiensttreding een training (I-) bewustzijn succesvol hebben gevolgd en hierover jaarlijks rapporteren aan het management.
- het registreren en afmelden van gebruikers.
- het toepassen van single-sign-on of MFA en het autorisatieproces.

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.

Er zijn verbeterpunten die relatief veel tijd vergen en projectmatig met ondersteuning van expertise moeten worden uitgevoerd. Dit zijn onder andere de SIEM/SOC implementatie, en het realiseren van een bedrijfscontinuïteitsplan met crisisplannen per proces/taakveld.

8.3. 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)* en *BIO2.0* zijn 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.

De BIO2 wordt opgenomen in een Ministeriële Regeling en een Algemene Maatregel van Bestuur, waarna de Rijksinspectie Digitale Infrastructuur (RDI) toezicht houdt op de naleving. Voor waterschappen zal de Inspectie Leefomgeving en Transport het toezicht invullen. De BIO2.0 weerspiegelt internationale beveiligingsnormen en legt meer nadruk op een risicogestuurde benadering. Hierdoor zijn sommige basisbeveiligingsniveaus vervallen en zijn bepaalde overheidsmaatregelen verlicht, terwijl andere verzwaard zijn door de NIS2.

Hoewel de BIO2 nog niet definitief is, roept het ministerie van BZK organisaties op zich voor te bereiden op de komst ervan. Organisaties moeten nu aan de slag om de basisveiligheid op orde te brengen, waarbij bestuurders een verantwoordelijkheid hebben om CISO's te ondersteunen in de transitie naar de BIO2. Een goede eerste stap is het uitvoeren van een gap-analyse en het in kaart brengen van de uitvoeringskosten. De conceptversie van de BIO2 is alvast gedeeld om dit te faciliteren. De BIO 2.0 is in concept gereed en volgt het besluitvormingsproces dat in 2025 wordt afgerond.

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 werken we 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.



9. Incidenten, ontdekte kwetsbaarheden en datalekken

9.1. Gemelde incidenten en kwetsbaarheden

In 2024 zijn 21 spammails, 12 incidenten en 116 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.

9.2. Gemelde datalekken

In 2024 zijn 10 datalekken gemeld bij de privacy officer. In 2020 waren dit er nog 17 in 2021 maar 11 en 10 in 2022 en 2023. Het lijkt hier om een neerwaartse 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.

Van de bij ons gemelde incidenten is er één door ons als gemeente en één door een externe partij als datalek gemeld bij de Autoriteit Persoonsgegevens (AP). Binnen 72 uur worden daarvoor in aanmerking komende datalekken bij de Autoriteit Persoonsgegevens (AP) gemeld. 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
26-1-2024	Melder heeft aangegeven dat zij de CV van de sollicitant heeft doorgestuurd aan een onbevoegde ontvanger. In deze CV staan verschillende persoonsgegevens vermeld. De melder heeft direct contact gehad met degene wiens persoonsgegevens het betreffen. Hij heeft de melder bedankt voor de transparantie. Verder gaf hij aan dat het geen probleem is. Aan de onbevoegde ontvanger is per e-mail gevraagd om de mail te verwijderen en daarvan een bevestiging te sturen. Deze bevestiging is ook ontvangen.	Nee
21-2-2024	Er is een afschrift van de huwelijksakte naar het oude adres van de betrokkene gestuurd. In dit afschrift staan persoonsgegevens vermeldt. Er is een (aangetekende) brief gestuurd naar het oude adres van de betrokkene met daarin het verzoek om het huwelijksafschrift te retourneren naar de gemeente óf, indien het huwelijksafschrift is vernietigd, dit te laten weten.	Nee
9-4-2014	Op het intranet van de gemeente staan verschillende werkgroepen. Deze werkgroepen zijn normaliter alleen toegankelijk voor de leden van een team. In een werkgroep worden bijvoorbeeld werkprocessen gedeeld. In deze casus is per abuis een werkproces gedeeld met daarin de persoonsgegevens van een cliënt. Alhoewel dit überhaupt niet de bedoeling is, stond deze groep ook nog tijdelijk (inmiddels niet meer) op openbaar binnen de gemeentelijke organisatie. De gegevens uit het werkproces zijn op verzoek direct weggehaald. Bovendien is	Nee

	de groep weer op besloten gezet.	
15-4-2024	Doordat een paar documenten met persoonsgegevens tijdelijk zijn achtergelaten bij de printer, konden onbevoegden deze inzien. De documenten zijn weggehaald.	Nee
17-4-2024	Er zijn een aantal brieven voor cliënten met daarbij een link naar een enquête naar verkeerde adressen gestuurd. Organisatorisch zijn maatregelen genomen om dit in de toekomst te voorkomen.	Nee
4-6-2024	Een medewerker heeft een printopdracht gegeven voor bankafschriften zoals ontvangen van een inwoner. Deze zijn onverhoopt en zonder directe kennisname daarvan naar een printer gestuurd staande op de benedenverdieping (waar ook Staatsbosbeheer haar printer heeft staan). Twee uur na de printopdracht heeft een medewerker (van Midden-Delfland) de stukken in de printer zien liggen en deze meegenomen op grond van een vermoeden van een datalek. Het gaat om bankafschriften die niet geanonimiseerd zijn en over een periode van drie maanden inzage geven in financiële gegevens.	Nee
8-8-2024	Een medewerker heeft een brief gestuurd naar een inwoner over het besluit op haar aanvraag. Voorafgaand aan het verzenden van de brief is het BRP niet geüpdatet. Hierdoor is de brief naar het oude adres van inwoonster gestuurd. in de werkinstructie wordt opgenomen dat voorafgaand het sturen van een brief na wordt gegaan of het BRP-adres up to date is.	Nee
1-10-2024	Er zijn documenten openbaar geplaatst via iBabs op de website die niet correct geanonimiseerd waren. De zwart gelakte persoonsgegevens konden door een aantal handelingen weer zichtbar gemaakt worden. De betrokkenen zijn per brief geïnformeerd. Direct na ontdekking van het datalek zijn de stukken offline gehaald. Vervolgens zijn de documenten op de juiste manier geanonimiseerd en weer online gezet.	Ja
31-10-2024	Een softwaredienstverlener in de cloud, een verwerker van onze gegevens, was getroffen door een cyberaanval met ransomware. Hierdoor zijn er vermoedelijk verouderde contactgegevens van ambtenaren buitgemaakt. Meteen nadat de verwerker op de hoogte is gesteld van de ongeoorloofde toegang, is er aan een gespecialiseerd cybersecuritybedrijf de opdracht gegeven om onderzoek te verrichten. Door de verwerker zijn zichtbare en onzichtbare additionele beveiligingsmaatregelen genomen om dit in de toekomst te voorkomen.	Ja, door verwerker
28-11-2024	Een mail met een bankafschrift naar per abuis binnengemeentelijk naar Team Financiën gestuurd. Dit had niet gemoeten, er staan persoonsgegevens in. Per e-mail is verzocht om de e-mail met de bankafschrift te verwijden. Later is bevestigd dat dit ook daadwerkelijk gebeurd is.	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 melding van datalekken 2024
De Autoriteit Persoonsgegevens (AP) ontving in 2024 bijna 38.000 meldingen van datalekken, een aanzienlijke stijging ten opzichte van het jaar ervoor (bijna 26.000). Veel datalekken ontstaan doordat post of mail niet bij de juiste persoon terechtkomt. Ook onbedoelde of onrechtmatige inzage van persoonsgegevens blijkt een veelvoorkomende bron van datalekken. Dit kan een risico opleveren voor de mensen om wiens gegevens het gaat. Mensen kunnen financieel getroffen worden, bijvoorbeeld door identiteitsfraude en oplichting. Organisaties zijn op grond van de AVG verplicht om in voorgeschreven situaties een datalek te melden bij de AP.

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

10. Meerjarenperspectief

Inwoners, ondernemingen en instellingen moeten erop kunnen vertrouwen dat we zorgvuldig omgaan met (persoons)gegevens. Het is daarom van groot belang dat gegevens alleen onder strikte voorwaarden gebruikt worden en goed beveiligd zijn tegen onbevoegd gebruik. Ons meerjaarlijks informatiebeveiligingsbeleid kent passende technische en organisatorische maatregelen om informatie te beschermen. Ook waarborgt het beleid dat de gemeente voldoet aan de relevante wet- en regelgeving. De beveiligingsfunctionaris (CISO) zorgt voor de coördinatie en het toezicht op de naleving van beveiligingsmaatregelen en -procedures, voor elk onderdeel van het informatiebeveiligingsbeleid. Jaarlijks toetsen we door middel van zelfevaluatie en externe audits de maatregelen voor de waardedocumenten, BRP, BAG, BGT, BRO, DigiD en Suwinet.

We houden rekening met ontwikkelingen en nieuwe opkomende bedreigingen.
Dat vraagt om tijdig anticiperen en middelen beschikbaar stellen om maatregelen te nemen.

We hebben afgelopen jaren te maken gehad met nieuwe trends en ontwikkelingen, dit zal ook de komende jaren niet anders zijn. Zo heeft de Coronacrisis gezorgd voor de toename en normaliseren van digitaal plaats en tijd onafhankelijk werken.
Diverse ontwikkelingen in de nabije toekomst maar ook die de afgelopen periode al zijn ingezet zoals AI mogen niet onderbelicht blijven. We moeten daarbij steeds wendbaarder zijn en weerbaar blijven.

In feite zijn de hieronder uitgewerkte punten onder te brengen in een aantal dreigingen. Deze moeten gezien worden als reminders waar nu en de komende jaren rekening mee moet worden gehouden.

De gemeentelijke informatievoorziening is kwetsbaar. We onderscheiden hieronder[3] een aantal categorieën van dreigingen in volgorde van belangrijkheid.

10.1. Grootste risico's voor gemeenten

Wat zijn op dit moment de grootste risico's op het gebied van de informatiebeveiliging en gegevensbescherming?

Uitval van dienstverlening en bedrijfsvoering
Als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering. Nagenoeg ieder proces, van uitgifte van paspoorten tot het betalen van uitkeringen, wordt uitgevoerd of ondersteund door digitale informatie- en communicatievoorzieningen. In het ergste geval moeten gemeenten dienstverleningsprocessen stilleggen.

Vertrouwelijke informatie in verkeerde handen
In principe is overheidsinformatie openbaar. Tenzij deze informatie privacygevoelig is, schade kan toebrengen aan de overheid of commercieel voor- of nadelig kan zijn voor derden. Gemeenten verwerken voor hun wettelijke taken veel vertrouwelijke informatie. Denk aan gegevens over werk en inkomen, zorg, veiligheid of commercieel interessante informatie over gebiedsontwikkeling, aanbestedingen en bedrijfsgevoelige informatie. Onterechte toegang tot deze informatie kan uiterst nadelig uitvallen voor inwoners en ondernemers. Een datalek of een overtreding van de AVG kan leiden tot hoge boetes.

Fouten in de dienstverlening
Informatiebeveiligingsincidenten kunnen leiden tot fouten in de dienstverlening. Kwaliteit en integriteit van data worden in het algemeen niet direct gezien als doel van informatiebeveiliging. Toch dient dit risico nadrukkelijk op het netvlies te staan van de directie. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

[3] Bron: IBD, tweejaarlijks dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023/2024

10.2. Dreigingsbeeld 2025 – 2026

De IBD werkt momenteel aan het Dreigingsbeeld Informatiebeveiliging voor de komende twee jaar. 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 2023-2024

De IBD ziet dat in het bijzonder drie soorten dreigingen opvallen:

Meer ransomware met destructievere gevolgen

De dreiging van ransomware-aanvallen neemt toe. Aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger: het wordt merkbaar. Het fenomeen ransomware (gijzelsoftware) komt al jaren voor. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken. De IBD ontving de afgelopen jaren steeds meer meldingen van situaties waar gemeentelijke proces- sen langdurig(er) verstoord zijn als gevolg van destructieve gijzelsoftware. Criminelen aarzelen niet om privacygevoelige gegevens van inwoners, bedrijven en medewerkers online te publiceren.

Steeds meer en ernstiger kwetsbaarheden in software

Alle hard- en software bevat kwetsbaarheden en fouten. Deze zouden kunnen worden misbruikt door kwaadwillenden. Het is daarom zaak om kwetsbaarheden tijdig te verhelpen.
In 2021 heeft de IBD 1841 kwetsbaarheden gesignaleerd. De ene kwetsbaarheid is de andere niet en daarom wordt per geval een risicoschatting gemaakt op basis van kans en impact. Gevallen met een hoge kans op misbruik en ernstige gevolgen komen in de afgelopen jaren relatief steeds vaker voor. Vaak is het verhelpen van een kwetsbaarheid een kwestie van updaten, maar soms is het complexer en moeten systemen ingrijpend gewijzigd worden.

Gevaren in ketens uit het zicht

Een gemeente neemt deel in gemiddeld 30 samenwerkingsverbanden en maakt gebruik van diensten van derden zoals softwareleveranciers. Omdat men bij uitbesteding vooral stuurt op de kwaliteit van de uiteindelijke dienstverlening en informatiebeveiliging en privacy gezien worden als operationele details, is daar weinig aandacht voor in de samenwerkingsafspraken. Politiek gezien is uitbesteding en/of samenwerking bedoeld om zaken tegen lagere kosten op een hoger kwaliteitsniveau te krijgen.
Informatiebeveiliging is in die zin een kostenpost. Als er al concrete afspraken zijn over informatiebeveiliging en privacy dan staat controle op de naleving beperkt op de agenda. Gemeenten vertrouwen erop dat bij een samenwerkingsverband dergelijke zaken 'gewoon geregeld zijn'. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico's als taken zijn uitbesteed. Gemeenten zijn in de afgelopen twee jaar regelmatig geconfronteerd met incidenten die ontstaan zijn bij derden waarbij de gevolgen in de eigen gemeente merkbaar waren.

Speerpunten Nederlandse Cybersecuritystrategie 2023 – 2028
(Bron: Nationaal Cyber Security Centrum (NCSC))
De Nederlandse samenleving wordt in hoog tempo steeds meer afhankelijk van digitale systemen. Hierdoor groeien de risico's en is digitale veiligheid, cyberweerbaarheid, steeds belangrijker. De Nederlandse Cybersecuritystrategie richt zich op het ontwikkelen van een veilig en digitaal ecosysteem, met vijf speerpunten:

- **Beter zicht op de dreiging**. Het kabinet investeert in mensen en systemen die scherper zicht geven op de herkomst van dreigingen en tegen wie ze gericht zijn.
- **Meer cybersecurityspecialisten**. We nemen verschillende acties om meer ICT-specialisten op de arbeidsmarkt te krijgen.
- **Overheid en sectoren nemen verantwoordelijkheid**. De verantwoordelijkheid voor veiligheid wordt deels verplaatst van eindgebruikers naar de overheid en specifieke sectoren. De meest volwassen en bepalende organisaties dragen de zwaarste verantwoordelijkheden. Voor de gehele overheid zelf zullen stevige wettelijke eisen voor veiligheid en toezicht op naleving erop worden ingericht.
- **Beter toezicht en de noodzakelijke wet- en regelgeving**. Herschikking van verantwoordelijkheden vergt uitbreiding van wettelijke regels en toezicht. Veiligheid moet het fundament worden waarop nieuwe systemen worden ontworpen. Er komen nieuwe regels waar (rijks)overheden, vitale aanbieders, en leveranciers van digitale producten en diensten aan moeten voldoen.
- **Heldere informatie via een nationale cyberautoriteit**. Er komt een centrale cyberautoriteit in Nederland: het nationale Cyber Security Incident Response Team. Deze nieuwe organisatie zal in samenwerking met publieke en private partners, vitale en niet-vitale organisaties, overheden en burgers voorzien van informatie over (dreigende) cyberincidenten om hen in staat te stellen zich te beveiligen.

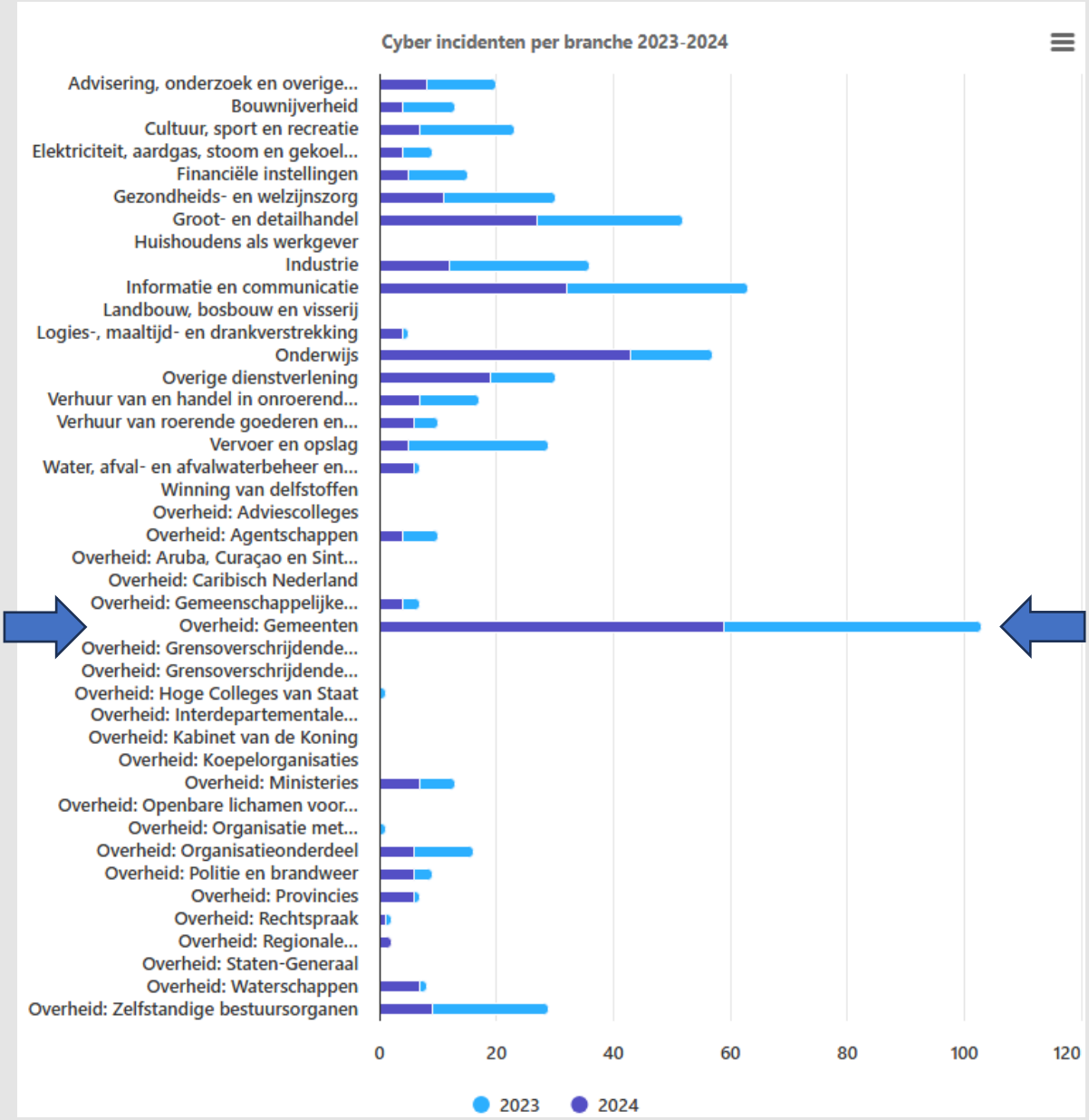
Wake-up call:

Top 5 branches met de meeste incidenten

De overheid, met name gemeenten, blijft de meest getroffen branche (57 incidenten in 2024 tegenover 44 in 2023). Het onderwijs kende een schrikbarende toename, van 13 naar 43 incidenten. Andere opvallende veranderingen zijn een daling in de industrie (van 23 naar 12 incidenten) en vervoer en opslag (van 21 naar 7 incidenten).

Onderstaande grafiek toont een overzicht van het aantal gemelde cyberincidenten per branche in 2023 en 2024. Hierdoor worden trends en verschillen snel duidelijk.

(Bron: DataLekt.nl)



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.

"An ounce of prevention is worth a pound of cure."

– **Benjamin Franklin -**