Gemeente
Midden-Delfland

# Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Gemeente Midden-Delfland



# Collegeverklaring informatiebeveiliging DigiD en Suwinet 2024

# Gemeente Gemeente Midden-Delfland

## Doel en achtergrond verklaring

De aansluitingen die we als gemeente voor DigiD en Suwinet hebben, vereisen dat voorzieningen moeten zijn beveiligd en (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. De gemeente treft interne beheersingsmaatregelen om veilig gebruik te maken van deze aansluitingen.

Met deze verklaring geven wij, het College van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[1] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet en de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius. De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor/RE.

Deze verklaring is bestemd voor de toezichthouders van DigiD en Suwinet, te weten Logius, en alsmede de stelselhouder: het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en de toezichthouder van Suwinet, te weten het Ministerie van Sociale Zaken en Werkgelegenheid via het Bureau Keteninformatie Werk en Inkomen (BKWI).

## Reikwijdte en diepgang verklaring

De aansluitingen die we als gemeentelijke organisatie voor DigiD en Suwinet hebben, vereisen dat onze voorzieningen moeten zijn beveiligd en dat (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. Hiervoor stellen de stelselhouders een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet interne beheersingsmaatregelen treffen om te voldoen aan deze gestelde normen teneinde gebruik te mogen (blijven) maken van deze aansluitingen.

De zelfevaluatie ENSIA gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2024. Voor DigiD wordt het door Logius vastgestelde Norm ICT-beveiligingsassessments DigiD versie 3.0 gehanteerd. Daarbij zijn normen getoetst op werking.

Voor Suwinet de Verantwoordingsrichtlijn GeVS 2022 (tevens geldend voor het verslagjaar 2024) waarin zijn opgenomen de geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv. Deze Verantwoordingsrichtlijn betreft opzet, bestaan en werking van de interne beheersingsmaatregelen. In het kader van de zelfevaluatie ENSIA zijn geen werkzaamheden uitgevoerd met betrekking tot de werking van deze maatregelen.

Als gevolg van de uitbesteding aan serviceorganisaties door de gemeente is een aantal van de interne beheersingsmaatregelen belegd bij serviceorganisaties. Hiervan hebben wij als gemeente een verantwoording voorzien van een oordeel van een onafhankelijke IT-auditor van de externe dienstverlener ontvangen.

---

1 ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

## Collegeverklaring en samenvattend beeld van de auditbevindingen

### Verklaring / Conclusie

Het college van Burgemeester en Wethouders van de Gemeente Midden-Delfland verklaart dat de gemeentelijke organisatie op 31 december 2024 niet voldoet aan alle geselecteerde normen inzake DigiD en Suwinet.

### Samenvattend beeld

Deze collegeverklaring betreffende de gemeentelijke organisatie en de serviceorganisaties dekt de geslecteerde normen inzake DigiD en Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Bijlage 1 DigiD met kenmerk 655678 CV B1 DigiD 1003883
- Bijlage 2 Suwinet met kenmerk 655678 CV B2 Suwinet

| Onderwerp | Wordt aan alle normen voldaan? | Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord? |
|---|---|---|
| DigiD 1003883 | Nee | Niet van toepassing |
| Suwinet voor SUWI-taken | Ja | Niet van toepassing |
| Suwinet voor niet-SUWI-taken | Ja | Niet van toepassing |

Het niet aan alle normen voldoen over DigiD ligt bij onze SaaS-leverancier, deze heeft inmiddels herstelacties doorgevoerd. Dit is ook bekend bij de landelijke toezichthouder Logius.

**Namens het College van B&W Gemeente Midden-Delfland**

Schipluiden, 15 april 2025

M.A.I. Born
Gemeentesecretaris

F.I. Noordermeer – van Slageren
Burgemeester

**Auditor:**

| | |
|---|---|
| Naam auditfirma: | BKBO b.v. |
| Naam auditor: | drs. M.B.H. IJpelaar RE CEH CISA, directeur |
| Datum: 22 april 2025<br>Vlijmen | [Handtekening of paraaf auditor] |

Signed By: Martinus Benedictus Hermann I
2025-04-22T15:07:31+02:00
ID: 16a6ec0d-c687-4059-9aca-810c7f1c8
Auth: csc

# Bijlage 1 DigiD - Gemeente Midden-Delfland DigiD - 1003883

## Totaaloverzicht getoetste normen ICT-beveiligingsassessment

## DigiD-aansluiting Gemeente Midden-Delfland DigiD met aansluitnummer 1003883

Gemeente Midden-Delfland biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Midden-Delfland DigiD voor authenticatie wordt gebruikt:

- zaaksysteem met de mogelijkheid webformulieren aan te bieden..

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: xxllnc zaken
- Versie: 2024.8.6

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- https://mijn.middendelfland.nl/form.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Midden-Delfland DigiD. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD versie 3.0" van Logius.

Deze webapplicatie betreft Geheel standaardpakket. De webapplicatie wordt onderhouden door xxllnc Zaakgericht B.V.

DigiD-aansluiting Gemeente Midden-Delfland DigiD bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door xxllnc Zaakgericht B.V. met beheervorm SaaS.

Gemeente Midden-Delfland heeft de DigiD web-omgeving uitbesteed aan:

- xxllnc Zaken.

*BCBO 25042

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier(s) van de gemeente valt voor de periode:

| Aansluithouder | |
|---|---|
| Oordeelsdatum: | 31-12-2024 |
| Controleperiode: | 01-07-2024 - 31-12-2024 |

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

| SaaS-leverancier | |
|---|---|
| Naam SaaS-leverancier: | xxllnc Zaken |
| Referentie/rapportnummer: | TPM: ITAA/DIGID/MIDD16102024<br>Sub-TPM: N.v.t. |
| Oordeelsdatum: | TPM: 16-10-2024<br>Sub-TPM: N.v.t. |
| Controleperiode: | TPM: 25 februari 2024 tot 26 augustus 2024 |

*BCBO 25042

| SaaS-leverancier | |
|---|---|
| | Sub-TPM: N.v.t. |
| Naam RE-auditor | TPM: Achmed Bouazza RE CISA<br>Sub-TPM: N.v.t. |
| Ondertekend door RE-auditor: | TPM: Ja<br>Sub-TPM: N.v.t. |

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk BKBO/231204-01/V1/AR.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

| | | Aansluithouder | SaaS-leverancier | |
|---|---|---|---|---|
| **DigiD-norm** | **Toetsing op** | **Oordeel** | **Oordeel TPM** | **Totaaloordeel** |
| B.01 Informatiebeveiligingsbeleid | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| B.05 Contractmanagement | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| U/TV.01 Identificatie en authenticatie | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| | *Werking* | Oordeelsonthouding* | Voldoet niet | Voldoet niet |
| U/WA.02 Webapplicatiebeheerproces | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| | *Werking* | Oordeelsonthouding* | Voldoet | Oordeelsonthouding* |
| U/WA.03 Automatische data-invoercontrole | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/WA04. Normaliseren uitvoer | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/WA.05 Cryptografie/ Privacybevordering | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| U/PW.02 Garanderen webprotocollen | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/PW.03 Configureren webserver | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/PW.05 Toegang tot beheermechanismen | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/PW.07 Hardening van platformen | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/NW.03 DMZ | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/NW.04 Protectie- en detectiemechanismen | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/NW.05 Scheiding beheer- en productieomgeving | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| U/NW.06 Hardening van netwerken | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| C.03 Vulnerability-assessments | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| C.04 Penetratietesten | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| C.06 Signaleringsfuncties | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| C.07 Monitoringfuncties | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| | *Werking* | Niet van toepassing | Voldoet niet | Voldoet niet |
| C.08 Wijzigingenbeheer | *Opzet en bestaan* | Voldoet | Voldoet | Voldoet |
| | *Werking* | Voldoet | Voldoet | Voldoet |
| C.09 Patchmanagement | *Opzet en bestaan* | Niet van toepassing | Voldoet | Voldoet |
| | *Werking* | Niet van toepassing | Voldoet | Voldoet |

*Oordeelsonthouding vanwege non occurrence.
Voor beveiligingsrichtlijnen U/TV.01 en U/WA.02 heeft de auditor vastgesteld dat de gemeente Midden-Delfland maatregelen heeft ontworpen en voor een andere deelpopulatie heeft geïmplementeerd (bestaan). Er zijn geen afwijkingen door de auditor geconstateerd. De auditor is van oordeel dat de organisatie in opzet en bestaan voldoet aan deze norm. Vanwege non-occurrence kan de effectieve werking niet worden vastgesteld en daarom geeft de auditor daarover geen oordeel.