# Bijlage 1 DigiD - Gemeente Aalsmeer - eDienst Publiekszaken - 1003779

## Totaaloverzicht getoetste normen ICT-beveiligingsassessment

## DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken met aansluitnummer 1003779

Gemeente Aalsmeer biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken voor authenticatie wordt gebruikt:

- Het aanvragen van verscheidene producten en diensten en het doen van meldingen

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- eDiensten Burgerzaken.

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Centric Netherlands B.V..

Deze applicatie is extern benaderbaar via het volgende internetadres(sen):
https://edienstenburgerzaken.aalsmeer.nl

DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Centric Netherlands B.V. in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken. 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" van Logius.

Gemeente Aalsmeer heeft een deel van de DigiD web-omgeving uitbesteed aan Centric Netherlands B.V..
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.

Een DigiD-aansluiting dient aan het gehele normenkader te 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. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van de leverancier(s):

| SaaS-leverancier | |
|---|---|
| Naam serviceorganisatie: | Centric Netherlands B.V. |
| Referentie/rapportnummer: | TPM 1: 23X00190221AVN-EDB<br>TPM 2: 23X00190221AVN-EDB_v2 |
| Afgiftedatum: | TPM 1: 18-10-2023<br>TPM 2: 17-11-2023 |
| Naam RE-auditor: | B. Beugelaar RE RA, KPMG Accountants N.V. |
| Ondertekend door RE-auditor: | Ja |

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze leverancier(s) het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk wdn/nda/9552.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij leverancier(s).

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