

Bijlage 1 DigiD – Gemeente Groningen - MijnGKB – 1000913

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Groningen - MijnGKB met aansluitnummer 1000913

Gemeente Groningen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Groningen - MijnGKB voor authenticatie wordt gebruikt:

- Schuldhulpverlening.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Schuldhulpverlening versie 2.19.0 betreft een standaardpakket die wordt onderhouden door Innovadis. De hosting betreft de Platform as a Service (PaaS) van Previder, waarbinnen de applicatie Schuldhulpverlening versie 2.19.0 is geïmplementeerd. Het technische beheer wordt uitgevoerd door Previder, de webserver (Internet Information Service, IIS) wordt beheerd door Innovadis.

Deze applicatie is extern benaderbaar via het volgende internetadres: <https://mijngkb.groningen.nl>.

DigiD-aansluiting MijnGKB bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Innovadis en Previder in de vorm van een Software as a Service (SaaS).

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting MijnGKB. 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 Groningen heeft een deel van de DigiD-webomgeving uitbesteed aan Innovadis en Previder. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisaties. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisaties. 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's / assurancerapportages van de leverancier(s):

| ICT-leverancier | |
|------------------------------|-----------------------------|
| Naam serviceorganisatie: | Previder |
| Referentie/rapportnummer: | AAS2021-1243 |
| Afgiftedatum: | 05-11-2021 |
| Naam RE-auditor: | Accoris Audit Services B.V. |
| Ondertekend door RE-auditor: | J.R. Möhle RE |

| Applicatieleverancier | |
|------------------------------|-----------------------------|
| Naam serviceorganisatie: | Innovadis |
| Referentie/rapportnummer: | AAS2021-1195 |
| Afgiftedatum: | 11-10-2021 |
| Naam RE-auditor: | Accoris Audit Services B.V. |
| Ondertekend door RE-auditor: | J.R. Möhle RE |

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(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 2C-2022-318 Gemeente Groningen.

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

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

Groningen, 28 februari 2022

Burgemeester en wethouders van gemeente Groningen



Burgemeester,
Koen Schuling



Gemeentesecretaris,
Christien Bronda