

Bijlage 1 DigiD - Gemeente Doesburg – Inwonerportaal - 1003703

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Doesburg – Inwonerportaal met aansluitnummer 1003703

Gemeente Doesburg biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Doesburg – Inwonerportaal voor authenticatie wordt gebruikt:

- om inwoners in de gelegenheid te stellen, informatie te bekijken over hun dossier binnen het sociaal domein. Zo is het onder andere mogelijk om details over de uitkering te bekijken en specificaties zoals de uitkeringsspecificatie en jaaropgave te downloaden;
- en ook kunnen inwoners wijzigingen in hun situatie doorgeven aan de gemeente.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: Gemeente Doesburg - Inwonerportaal
- Versie: SDMIMR versie 24.5

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- <https://mijninkomen.doesburg.nl>

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Doesburg – Inwonerportaal. 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 Centric Netherlands B.V.

DigiD-aansluiting Gemeente Doesburg – Inwonerportaal bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Centric Netherlands B.V. met beheervorm SaaS.

Gemeente Doesburg heeft de DigiD web-omgeving uitbesteed aan Centric Netherlands B.V.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. 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 van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	12-11-2024
Controleperiode:	01-03-2024 – 30-09-2024

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

SaaS-leverancier	
Naam SaaS-leverancier:	Centric Netherlands B.V.
Referentie/rapportnummer:	TPM: 24X00195119AVN_IWP Sub-TPM: N.v.t.

SaaS-leverancier	
Oordeelsdatum:	TPM: 12-11-2024 Sub-TPM: N.v.t.
Controleperiode:	TPM: 01-03-2024 – 30-09-2024 Sub-TPM: N.v.t.
Naam RE-auditor	TPM: B. Beugelaar Sub-TPM: N.v.t.
Ondertekend door RE-auditor:	TPM: Ja 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 2C-2025-681.

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	Voldoet	Voldoet	Voldoet
U/WA.02 Webapplicatiebeheerproces	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
U/WA.03 Automatische data-invoercontrole	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/WA.04. 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	Voldoet
C.08 Wijzigingenbeheer	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet niet	Voldoet	Voldoet
C.09 Patchmanagement	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet	Voldoet

Verbeterplan werking C.08 Wijzigingenbeheer

Aanleiding

Tijdens de ENSIA verantwoording 2024, die begeleid werd door een extern audit bureau, werd geconstateerd dat we dit jaar niet aan alle ENSIA eisen (Norea normen) hebben voldaan. Het betrof hier een norm uit het onderdeel DigiD Inwonersportaal. In dit verbeterplan geven we een overzicht van het onderdeel dat niet voldeed en de verbeteracties die we in willen gaan zetten.

Het DigiD assessment beperkte zich tot 2023 tot het beoordelen van de opzet en het toetsen van het bestaan van de beheersingsmaatregelen. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in 2022 besloten dat voor een aantal normen de werking zal worden getoetst in 2024. Met het besluit van BZK wordt nu voor 5 normen ook een toets op werking aan toegevoegd. De 5 normen die worden getoetst op opzet, bestaan en werking zijn: U/TV.01; U/WA.02; C.07; C.08 en C.09

De controleperiode is door Logius bepaald op minimaal 6 maanden aaneengesloten voorafgaand aan de audit, waarbij de laatste dag van de controleperiode door Logius wordt gezien/ gehanteerd als de gespecificeerde datum waarop de opzet en het bestaan is getoetst. Voor de ENSIA assessments is de oordeelsdatum 31 december.

De controleperiode voor het DigiD deel van de ENSIA is dan de periode 1 juli (of eerder) tot 31 december van het verantwoordingsjaar. De controleperiode geldt voor de gemeenten en serviceorganisaties (en sub-serviceorganisaties). Een serviceorganisatie zal bij het bepalen van de controleperiode rekening moeten houden met de wensen en afspraken van aansluithouders om aan hun verplichtingen te kunnen voldoen. Hierbij kan de controleperiode vanwege een andere rapportageperiode van die (sub)serviceorganisatie anders zijn dan de laatste 6 maanden voorafgaand aan de oordeelsdatum assurance-rapport van de desbetreffende aansluithouder.

Wat er niet voldeed:

Aantoonbare werking door afdeling Samenleving voldoet niet op norm C.08

Hier voldoen we niet aan de volgende norm:

C.08 Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.

Het was m.b.t. deze norm niet aantoonbaar dat de laatste 6 maanden van 2024 alle ontwikkelingen (release notes) zijn geraadpleegd en beoordeeld op effecten bedrijfscontinuïteit en wensen als opdrachtgever.

Verbeteracties

Wat	Aanpak	Wie	Wanneer
DigiD C.08	In samenwerkingsomgeving afdeling Samenleving wordt een Teams kanaal inrichten. In dit kanaal worden alle zogeheten release notes van de leverancier geplaatst met een activiteiten TAG (@) Na plaatsing worden de release notes beoordeeld door ten minste de functioneel applicatiebeheerders op effect en potentieel gevolg in werkprocessen. Zij plaatsen een korte beschrijving van de beoordeling in het kanaal. De functioneel applicatiebeheerders informeren wanneer van toepassing technisch applicatiebeheerders en actief de belanghebbende gebruiker van de digitale dienstverlening.	Applicatie-beheerders Afdeling Samenleving	April 2025 (en met terugwerkende kracht vanaf 1 jan. 2025)

	De actieve gebruikers in het kanaal plaatsen een signaal dat de instructie gelezen is en/of voorzien de release notes ook van een korte beoordeling. Deze afspraak wordt bij de start opgenomen in het kanaal en met de manager gedeeld en wordt daarmee onderdeel van het DigiD auditproces.		
Organisatie breed	Werkproces invoeren bij alle applicatiebeheerders en over alle afdelingen voor zover dit al niet gedaan wordt.	ENSIA coördinator	April 2025 (en met terugwerkende kracht vanaf 1 jan. 2025)