Gemeentelijk kenmerk bijlage 4 DigiD:	2043707

Bijlage 4 DigiD - Digitaal loket - 1002411

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal loket met aansluitnummer 1002411

Gemeente Weert biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Digitaal loket voor authenticatie wordt gebruikt:

- Het genereren van aanvraagformulieren en het maken van meldingen openbaar gebied, woningbouw en aanvragen nummeraanduidingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Djuma, https://eloket.weert.nl

Deze applicatie betreft een combinatie van maatwerken en standaard software en wordt onderhouden door gemeente Weert en Visma Circle.

Deze applicatie is extern benaderbaar via de volgende internetadressen: https://www.weert.nl en https://eloket.weert.nl/#/f/[formuliernummer].

DigiD-aansluiting Digitaal loket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Visma Circle in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Digitaal loket. 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 Weert heeft een deel van de DigiD web-omgeving uitbesteed aan .
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):

Applicatieleverancier	
Naam serviceorganisatie:	Visma Circle BV
Referentie/rapportnummer:	BKBO/220524-1/TPM
Afgiftedatum:	23 september 2022
Naam RE-auditor:	[redacted]
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM’s / assurancerapportage(s) 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 2304R.AH26

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

Gemeentelijk kenmerk bijlage 4 DigiD:	2043707

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

*DigiD koppeling Enable-U inmiddels uitgefaseerd, en overgegaan naar de DigiD koppeling van Visma Circle. Hierdoor komt het totaal oordeel op alle normen op “voldoet” te staan.