

Bijlage 1 DigiD - Digitaal loket - 1005287

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal loket met aansluitnummer 1005287

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

- Zaaksysteem voor vastlegging alle zaken, inkomende post en communicatie intern/extern met burgers. Tevens voor digitale dienstverlening met webformulieren/aanmelden voor evenementen of het aanvragen van vergunningen..

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: Djuma eLoket
- Versie: 2024.215.001

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- eloket.weert.nl/f/#.

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 versie 3.0" van Logius.

Deze webapplicatie betreft Geheel standaardpakket. De webapplicatie wordt onderhouden door Visma Circle B.V..

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

Gemeente Weert heeft de DigiD web-omgeving uitbesteed aan:

- Visma Circle 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.

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:	Visma Circle B.V.
Referentie/rapportnummer:	TPM: BKBO/240325-01/TPM Sub-TPM: SOC II Type 2 Cloud dienstverlening
Oordeelsdatum:	TPM: 30-08-2024 Sub-TPM: 19-01-2024

SaaS-leverancier	
Controleperiode:	TPM: 01-01-2024 - 30-08-2024 Sub-TPM: 01-01-2023 - 31-07-2024
Naam RE-auditor	TPM: [REDACTED] Sub-TPM: [REDACTED] auditor
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: Ja

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 RK.LT.39086.2165488.

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

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

DigiD-norm	Toetsing op	Aansluithouder	SaaS-leverancier		Totaaloordeel
		Oordeel	Oordeel TPM	Oordeel sub-TPM	
C.08 Wijzigingenbeheer	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet

