Bijlage 1 DigiD - Publiekszaken Digitaal Loket - 1001325

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Publiekszaken Digitaal Loket met aansluitnummer 1001325

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

- Digitaal aanvragen van producten en doorgeven van o.a. verhuizingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Iburgerzaken, https://iburgerzaken.weert.nl

Deze applicatie betreft een combinatie van maatwerk en standaard software en wordt onderhouden door gemeente Weert en Pink Roccade Local Government B.V.

Deze applicatie is extern benaderbaar via de volgende internetadressen: https://www.weert.nl en https://www.iburgerzaken.weert.nl.

DigiD-aansluiting Publiekszaken Digitaal Loket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door PinkRoccade Local Government B.V. in de vorm van fysieke hosting SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Publiekszaken 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 PinkRoccade Local Government 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:	PinkRoccade Local Government B.V.
Referentie/rapportnummer:	20211026 DBA-PRLG
Afgiftedatum:	26-10-2021
Naam RE-auditor:	Frank Kossen RE Laurens van Thiel CISA CISSP Drs. M. El Aarbaoui RE (QA)
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 2204R.AH40.

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

Gemeentelijk kenmerk bijlage 1 DigiD: **1616626**

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