Gemeentelijk kenmerk bijlage 1 DigiD:	1616626

Bijlage 1 DigiD - Persoonlijke internet pagina - 1002287

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Persoonlijke internet pagina met aansluitnummer 1002287

Gemeente Weert biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Persoonlijke internet pagina voor authenticatie wordt gebruikt:

- Persoonlijke pagina van de afdeling Werk, Inkomen en Zorgverlening waar cliënten informatie kunnen raadplegen, documenten toevoegen en gegevens doorgeven.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- PIP, https://pip.weert.nl

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door gemeente Weert en Pink Roccade Local Government.

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

DigiD-aansluiting Persoonlijke internet pagina bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Pink Roccade Local Government in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Persoonlijke internet pagina. 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 Pink Roccade Local Government. 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 1	
Naam serviceorganisatie:	Pink Roccade Local Government
Referentie/rapportnummer:	AAS2021-1179
Afgiftedatum:	11-10-2021
Naam RE-auditor:	J.R. Möhle RE
Ondertekend door RE-auditor:	Ja

SaaS-leverancier 2	
Naam serviceorganisatie:	Pink Roccade Local Government
Referentie/rapportnummer:	AAS2021-1178
Afgiftedatum:	30-09-2021
Naam RE-auditor:	J.R. Möhle RE
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).

DigiD-norm		Getoetst bij gemeente	Getoetst bij SaaS-leverancier 1	Getoetst bij SaaS-leverancier 2	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.	Voldoet	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.	n.v.t.	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	n.v.t.	Voldoet	Voldoet	Voldoet