Bijlage 1 DigiD - Gemeente Eijsden-Margraten iBurgerzaken - 1001593

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Eijsden-Margraten iBurgerzaken met aansluitnummer 1001593

Gemeente Eijsden-Margraten biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting gemeente Eijsden-Margraten iBurgerzaken voor authenticatie wordt gebruikt:

- Het genereren van aanvraagformulieren voor burgerzakenproducten.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door PinkRoccade.

Deze applicatie is extern benaderbaar via het volgende internetadres: www.eijsden-margraten.nl

DigiD-aansluiting gemeente Eijsden-Margraten iBurgerzaken bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door PinkRoccade in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting gemeente Eijsden-Margraten iBurgerzaken. 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 Eijsden-Margraten heeft een deel van de DigiD web-omgeving uitbesteed aan PinkRoccade.
Als gevolg hiervan zijn 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.

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
Referentie/rapportnummer:	TPM 1: 20231012 DBA-PRLG DigiD iBurgerzaken Eijsden-Margraten TPM 2: N.v.t.
Afgiftedatum:	TPM 1: 12-10-2023 TPM 2: N.v.t.
Naam RE-auditor:	[redacted] RE (QA) [redacted] CISA CISSP
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 van At Risk Advies BV met kenmerk 202403E-M.

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

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

Behoort bij ons assurancerapport van 22 maart 2024 met kenmerk 202403^{E}-M.

Maastricht, 22 maart 2024
At Risk Advies BV

[redacted] RE