Gemeentelijk kenmerk bijlage 1 DigiD:	6400-2024

Bijlage 1 DigiD - Digitaal loket Gemeente Raalte - 1000313

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal loket Gemeente Raalte met aansluitnummer 1000313

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

- Een digitaal loket voor burgers en bedrijven met daarin formulieren
- Een Producten en Diensten Catalogus (PDC)

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- E-suite versie 4.34

De applicatie betreft standaard software en wordt onderhouden door Atos. De infrastructuur waarop de applicatie draait wordt beheerd door SSC Twente in de vorm van fysieke hosting.

Deze applicatie is extern benaderbaar via het volgende internetadres: https://dloket.raalte.nl .

DigiD-aansluiting Digitaal loket Gemeente Raalte bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Atos ontwikkelaar en Dimpact. in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Digitaal loket Gemeente Raalte. 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 Raalte heeft een deel van de DigiD web-omgeving uitbesteed aan Atos ontwikkelaar en Dimpact..
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’s / assurancerapportages van de leverancier(s):

IT-leverancier	
Naam serviceorganisatie:	Dimpact
Referentie/rapportnummer:	2309R.AH114
Afgiftedatum:	29-09-2023
Naam RE-auditor:	3Angles
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage van onze serviceorganisatie 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 202403ERaalte.

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

Gemeentelijk kenmerk bijlage 1 DigiD:	6400-2024

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij IT-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	Niet van toepassing	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet