

Bijlage 1 DigiD - Gemeente Aalsmeer - eDienst Publiekszaken - 1003779

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken met aansluitnummer 1003779

Gemeente Aalsmeer biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken voor authenticatie wordt gebruikt:

- Met de eDiensten kan er door de burger digitaal gebruik gemaakt worden van een aantal burgerzaken diensten en producten. Via DigiD kan een aanvraag ingediend worden die vervolgens in de applicatie Centric Burgerzaken terecht komt zodat een medewerker de aanvraag correct kan afhandelen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: Centric eDiensten
- Versie: 1.9.5_2024

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- <https://edienstenburgerzaken.aalsmeer.nl/>.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken. 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 Centric Netherlands B.V..

DigiD-aansluiting Gemeente Aalsmeer - eDienst Publiekszaken bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Centric Netherlands B.V. met beheervorm SaaS-dienst. Technisch beheer leverancier, functioneel beheer gemeente; team applicatiebeheer.

Gemeente Aalsmeer heeft de DigiD web-omgeving uitbesteed aan:

- Centric Netherlands B.V..

Als gevolg hiervan is 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.

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:	12-11-2024
Controleperiode:	1 juli 2024 t/m 31 december 2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	Centric Netherlands B.V.
Referentie/rapportnummer:	TPM: 24X00195119AVN_EDB Sub-TPM: N.v.t.
Oordeelsdatum:	TPM: 30-09-2024 Sub-TPM: N.v.t.

SaaS-leverancier	
Controleperiode:	TPM: 1 maart 2024 tot en met 30 september 2024 Sub-TPM: N.v.t.
Naam RE-auditor	TPM: Brigitte Beugelaar RE RA Sub-TPM: N.v.t.
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: N.v.t.

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 Wdn/nda/9874.

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