Bijlage 1 DigiD - Gemeente Amstelveen - Mijn Amstelveen - 1003951

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Amstelveen - Mijn Amstelveen met aansluitnummer 1003951

Gemeente Amstelveen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Amstelveen - Mijn Amstelveen voor authenticatie wordt gebruikt:

- Digitaal loket waar de burger met DigiD kan aanmelden in het Rx.Enterprise portaal. Hier kan de gebruiker naast het indienen van formulieren (meldingen, aanvragen, etc.) ook zijn/haar lopende en afgehandelde aanvragen inzien, met de daarbij beschikbaar gestelde documenten..

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: Rx.Enterprise
- Versie: 2.19.11

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- https://loket.amstelveen.nl/.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Amstelveen - Mijn Amstelveen. 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 Visma Roxit BV.

DigiD-aansluiting Gemeente Amstelveen - Mijn Amstelveen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Visma Roxit BV met beheervorm De infrastructuur waarop de applicatie draait wordt beheerd door Visma Roxit BV.

Gemeente Amstelveen heeft de DigiD web-omgeving uitbesteed aan:

- Visma Roxit BV.
- .

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.

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:	10-12-2025
Controleperiode:	1 juli 2025 t/m 31 december 2025

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

SaaS-leverancier	
Naam SaaS-leverancier:	Visma Roxit BV

SaaS-leverancier	
Referentie/rapportnummer:	TPM: BKBO/250728-01/TPM Sub-TPM: N.v.t.
Oordeelsdatum:	TPM: 18-09-2025 Sub-TPM: N.v.t.
Controleperiode:	TPM: 1 maart 2025 tot en met 31 augustus 2025 Sub-TPM: N.v.t.
Naam RE-auditor	TPM: drs. M.B.H. IJpelaar RE CEH CISA CIPP/e 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 chs/afs/10426.

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

		Aansluithouder	SaaS-leverancier	
DigiD-norm	**Toetsing op**	**Oordeel**	**Oordeel TPM**	**Totaaloordeel**
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*	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	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	Niet van toepassing
U/WA04. Normaliseren uitvoer	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/WA.05 Cryptografie/ Privacybevordering	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
U/PW.02 Garanderen webprotocollen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/PW.03 Configureren webserver	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/PW.05 Toegang tot beheermechanismen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/PW.07 Hardening van platformen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/NW.03 DMZ	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/NW.04 Protectie- en detectiemechanismen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/NW.05 Scheiding beheer- en productieomgeving	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
U/NW.06 Hardening van netwerken	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
C.03 Vulnerability-assessments	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
C.04 Penetratietesten	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
C.06 Signaleringsfuncties	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
C.07 Monitoringfuncties	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
	Werking	Niet van toepassing	Voldoet	Niet van toepassing
C.08 Wijzigingenbeheer	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	*Opzet en bestaan*	Niet van toepassing	Voldoet	Niet van toepassing
	Werking	Niet van toepassing	Voldoet	Niet van toepassing