

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate Gemeente Rotterdam voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA¹ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2022.

De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen en eventuele afwijkingen en waar deze belegd zijn, is opgenomen in de bijlagen:

- Bijlage 1 DigiD met kenmerk M2303-3010
- Bijlage 2 Suwinet met kenmerk M2303-3010

Verklaring college

Het college verklaart dat voor DigiD en Suwinet niet aan alle normen wordt voldaan. Wij hebben verbeterplannen opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

¹ ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet) en de Wet Onroerende Zaken (WOZ).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1000161 Mijn Loket	Nee	Ja
DigiD 1001269 Mijn KBR	Ja	Niet van toepassing
DigiD 1002211 Digitaal Loket	Ja	Niet van toepassing
DigiD 1003505 eDiensten Burgerzaken	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Niet van toepassing	Niet van toepassing

Rotterdam, 11 april 2023

College van B&W gemeente Gemeente Rotterdam

V.J.M. Roozen	Gemeentesecretaris	Handtekening:
A. Aboutaleb	Burgemeester	Handtekening:

Naam auditfirma:	Concern Auditing, Gemeente Rotterdam
Naam auditor:	De heer, [REDACTED] RE
Datum	Handtekening:

Bijlage 1 DigiD - Mijn Loket - 1000161

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Mijn Loket met aansluitnummer 1000161

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

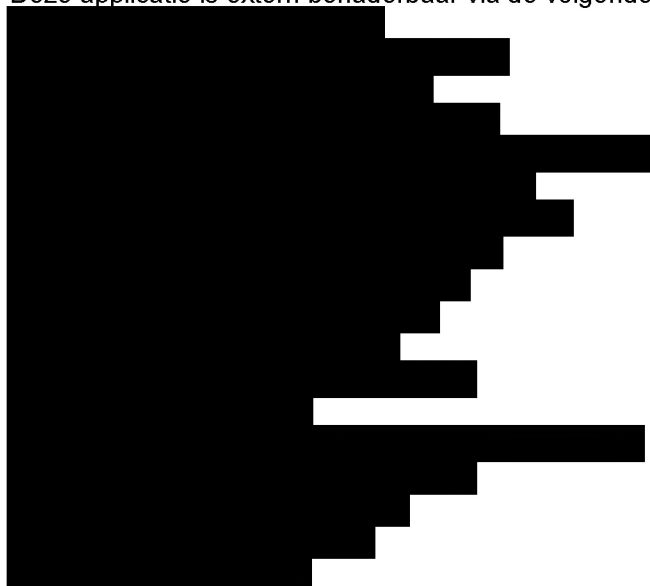
- Het bieden van een platform waar burgers op een centrale plek gemeentelijke diensten en ondersteuning kunnen aanvragen, zoals afspraken bij stadswinkels, gemeentelijke belastingen, vergunningen en subsidies.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Mijnloket

Deze applicatie betreft geheel maatwerk en wordt onderhouden door Gemeente Rotterdam.

Deze applicatie is extern benaderbaar via de volgende internetadressen²:



DigiD-aansluiting Mijn Loket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt deels beheerd door Gemeente Rotterdam en deels beheerd door leverancier Mendix in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Mijn Loket. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Mendix. 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.

ICT-leverancier	
Naam serviceorganisatie:	Mendix
Referentie/rapportnummer:	ITAA/DIGID/MXTGR05122022

² Vertrouwelijke informatie is uit veiligheidsoverwegingen gelakt, en wordt na oplossen bevindingen openbaar gemaakt.

ICT-leverancier	
Afgiftedatum:	05 december 2022
Naam auditfirma:	Mazars N.V.
Ondertekend door RE-auditor:	RE RI en RE AA

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 2301241.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij ICT-leverancier	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid		Voldoet	
B.05	Contractmanagement		Voldoet	
U/TV.01	Identificatie en authenticatie		Voldoet	
U/WA.02	Webapplicatiebeheerproces		Voldoet	
U/WA.03	Automatische data-invoercontrole		Niet van toepassing	
U/WA.04	Normaliseren uitvoer		Niet van toepassing	
U/WA.05	Cryptografie/ Privacybevordering		Voldoet	
U/PW.02	Garanderen webprotocollen		Niet van toepassing	
U/PW.03	Configureren webserver ³		Niet van toepassing	
U/PW.05	Toegang tot beheermechanismen		Voldoet	
U/PW.07	Hardening van platformen		Voldoet	
U/NW.03	DMZ		Voldoet	
U/NW.04	Protectie- en detectiemechanismen		Voldoet	
U/NW.05	Scheiding beheer- en productieomgeving		Voldoet	
U/NW.06	Hardening van netwerken		Voldoet	
C.03	Vulnerability-assessments		Voldoet	
C.04	Penetratietesten		Voldoet	
C.06	Signaleringsfuncties		Voldoet	
C.07	Monitoringfuncties		Voldoet	
C.08	Wijzigingenbeheer		Voldoet	
C.09	Patchmanagement		Voldoet	

³ T.a.v. norm U/PW.03 merken we op dat één (1) specifiek onderdeel van de gewenste configuratie-items niet op de juiste wijze is geconfigureerd, waarbij naar het oordeel van de auditor de kwetsbaarheden afdoende zijn beperkt en een verbeterplan is opgesteld waarbij de auditor er kennis van heeft genomen, dat de kwetsbaarheid voor 1 mei 2024 geheel is opgelost. Alle andere configuratie-items zijn wel correct geconfigureerd. Voor nadere informatie kan Logius zich wenden tot de auditor.

Bijlage 2 DigiD - Mijn KBR - 1001269

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Mijn KBR met aansluitnummer 1001269

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

Een platform waar burgers op een centrale plek gemeentelijke diensten en ondersteuning kan aanvragen voor schuldhulpverlening.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Schulddienstverlening

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Innovadis en Previder in de vorm van SaaS.

Deze applicatie is extern benaderbaar via het volgende internetadres:

[REDACTED]

DigiD-aansluiting Mijn KBR bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Innovadis en Previder. Innovadis biedt de applicatie aan in de vorm van SaaS.

Leverancier Previder biedt ten aanzien van deze applicatie het platform, hysysteembeheer, managed firewall en servicemanagement aan.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Mijn KBR. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Innovadis en Previder.

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):

IT-leverancier	
Naam serviceorganisatie:	Innovadis en Previder
Referentie/rapportnummer:	TPM 1: Innovadis: AAS2022-1425 TPM 2: Previder: AAS2022-1499
Afgiftedatum:	TPM 1: 27-10-2022 TPM 2: 27-10-2022
Naam RE-auditor:	Innovadis: [REDACTED] RE Van Previder: [REDACTED]
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze serviceorganisatie(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 2301241.

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

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij IT-leverancier 1	Getoetst bij IT-leverancier 2	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
U/NW.03	DMZ	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Niet van toepassing	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet	Voldoet

Bijlage 3 DigiD - Digitaal Loket - 1002211

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket met aansluitnummer 1002211

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

- Een digitaal loket voor burgers en bedrijven met daarin formulieren EN
- Een producten en diensten catalogus (PDC)

Deze functionaliteit wordt geboden door de volgende webapplicatie: e-suite.

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Atos. De infrastructuur waarop de webapplicatie draait wordt beheerd door SSC Twente in de vorm van fysieke hosting.

Deze applicatie is extern benaderbaar via het volgende internetadres: [REDACTED]

DigiD-aansluiting Digitaal Loket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door SSC Twente in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Digitaal Loket. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan 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 / assurancerapportage van de leverancier(s):

IT-leverancier	
Naam serviceorganisatie:	Dimpact
Referentie/rapportnummer:	TPM 1: 2210R.AH130
Afgiftedatum:	TPM 1: 08-03-2023
Naam RE-auditor:	3Angels B.V. [REDACTED] RE RA
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze serviceorganisatie(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 2301241.

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

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

Bijlage 4 DigiD - eDiensten Burgerzaken - 1003505

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting eDiensten Burgerzaken met aansluitnummer 1003505

Gemeente Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting eDiensten Burgerzaken voor authenticatie wordt gebruikt:

- Het in de gelegenheid stellen van inwoners om informatie op te vragen uit de BRP en of door te geven binnen het burgerzaken domein. Zo is het onder andere mogelijk om uittreksels en afschriften aan te vragen en huwelijke of geboortes door te geven. Ook kunnen inwoners wijzigingen in hun situatie doorgeven aan de gemeente zoals verhuizingen en of emigraties.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- eDiensten Burgerzaken

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Centric Nederlands B.V.

Deze applicatie is extern benaderbaar via het volgende internetadres(sen):

[REDACTED]

DigiD-aansluiting eDiensten Burgerzaken bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Centric Nederlands B.V. in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting eDiensten Burgerzaken. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Centric Nederlands B.V.

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	
Naam serviceorganisatie:	Centric Nederlands B.V.
Referentie/rapportnummer:	A2200025558
Afgiftedatum:	14-10-2022
Naam RE-auditor:	KPMG [REDACTED] RE RA
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 2301241.

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	Niet van toepassing	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

Bijlage 5 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2022 van Gemeente Rotterdam. Onderwerp van de verklaring is het gebruik van Suwinet. Deze verklaring heeft betrekking op de Verantwoordingsrichtlijn GeVS 2022 welke is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO).

Suwinet-gegevens worden ten behoeve van de dienstverlening aan onze burgers wel door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. Gemeente Rotterdam heeft een deel van de Suwinet taken uitbesteed aan Wigo4it. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm. De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling (TPM) / assurancerapportage (AR) van onze serviceorganisatie.

Leverancier 1	
Naam serviceorganisatie:	Wigo4it
Referentie/rapportnummer:	AAS2022-1501
Afgiftedatum:	2 december 2022
Naam RE-auditor:	RE
Ondertekend door RE-auditor:	Ja

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	Binnen de gemeente	Ja Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente	Ja Ja
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente	Ja Ja
Wet gemeentelijke schuldhulpverlening (Wgs)	Binnen de gemeente	Ja Ja

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Niet van toepassing	Nee
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing	Nee
Adresonderzoek door Burgerzaken	Niet van toepassing	Nee

Naleving BIO-maatregelen

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2022 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2022:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
Binnen de gemeente	Participatiewet (Pw) Wet gemeentelijke schuldhulpverlening (Wgs)		
Binnen de gemeente	Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)		
Binnen de gemeente	Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)		