Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Dordrecht

Gemeentelijk kenmerk collegeverklaring ENSIA: 2021-0042544

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Dordrecht

Doel en achtergrond verklaring

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

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[1] 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 2020.

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 waar deze belegd zijn, is opgenomen in de bijlagen:

bijlage 1 DigiD met kenmerk 2021-0042544a

bijlage 2 Suwinet met kenmerk 2021-0042544b

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 Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).*

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in een verbeterplan opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD (1) 1002815	Ja	Niet van toepassing
DigiD (2) 1003443	Nee	Ja
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Dordrecht, 23 maart 2021,

College van B en W gemeente Dordrecht

De secretaris,

C.H.W.M. Post

De burgemeester

A.W. Kolff

Naam auditfirma: BDO Audit & Assurance B.V.

Naam auditor: Drs. W. Dalhuisen RE CISA

Datum:

Gemeentelijk kenmerk bijlage 1 DigiD: 2021-0042544a

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal loket gemeente Dordrecht en aansluitnummer 1002815

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

- Het genereren van aanvraagformulieren voor de gemeentelijke dienstverlening.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- InProces (klant-, zaak- en archiefsysteem)

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Visma Roxit BV.

Deze applicatie is extern benaderbaar via het volgende internetadres: loket.dordrecht.nl.

DigiD-aansluiting Digitaal loket gemeente Dordrecht bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Visma Roxit BV in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Digitaal loket gemeente Dordrecht. 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.

Dordrecht heeft een deel van de DigiD web-omgeving uitbesteed aan VISMA ROXIT BV. 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.

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 van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM van de gemeentelijke serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Visma Roxit BV
Referentie/rapportnummer:	AC/KV/RSN/09122020.2
Afgiftedatum:	09 december 2020
Naam RE-auditor:	Audit Connect BV, Agnes ter Agter RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM 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: wdn/esc/8114

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm:

DigiD Norm		Getoetst bij Gemeente	Getoetst bij Visma Roxit BV	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/Privacybevordering	• Voldoet	• Voldoet	• Voldoet
U/PW.02	Garanderen webprotocollen		• Voldoet	• Voldoet
U/PW.03	Configureren webserver		• Voldoet	• Voldoet
U/PW.05	Toegang tot beheermechanismen		• Voldoet	• Voldoet
U/PW.07	Hardening van platformen		• Voldoet	• Voldoet
U/NW.03	DMZ		• Voldoet	• Voldoet
U/NW.04	Protectie- en detectiemechanismen		• Voldoet	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments		• Voldoet	• Voldoet
C.04	Penetratietesten		• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Dordrecht - eDiensten en aansluitnummer 1003443

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

- Het genereren van aanvraagformulieren voor e-diensten burgerzaken

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- E-dienst Burgerzaken

Deze applicatie betreft een combinatie van maatwerk en standaard software en wordt onderhouden door Centric Nederland BV.

Deze applicatie is extern benaderbaar via het volgende internetadres: edienstenburgerzaken.dordrecht.nl

DigiD aansluiting Gemeente Dordrecht - eDiensten bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Centric Nederland BV in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Gemeente Dordrecht - eDiensten. 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.

Dordrecht heeft een deel van de DigiD web-omgeving uitbesteed aan Centric Nederland BV. 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.

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 van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM's van de gemeentelijke serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Centric Nederland BV
Referentie/rapportnummer:	NP9AQ7B_B en REQ5157460_B2
Afgiftedatum:	04 december 2020 en 8 maart 2021
Naam RE-auditor:	Ernst & Young Accountants LLP, Peter Kornelisse RE CISA CIPP
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM 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 wdn/esc/8114

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm

DigiD Norm		Getoetst bij Gemeente	Getoetst bij Centric Nederland BV	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie		• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/Privacybevordering	• Voldoet	• Voldoet	• Voldoet
U/PW.02	Garanderen webprotocollen		• Voldoet	• Voldoet
U/PW.03	Configureren webserver		• Voldoet niet	• Voldoet niet
U/PW.05	Toegang tot beheermechanismen		• Voldoet	• Voldoet
U/PW.07	Hardening van platformen		• Voldoet	• Voldoet
U/NW.03	DMZ		• Voldoet	• Voldoet
U/NW.04	Protectie- en detectiemechanismen		• Voldoet	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments		• Voldoet	• Voldoet
C.04	Penetratietesten		• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

Gemeentelijk kenmerk bijlage 2 Suwinet: 2021-0042544b

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2020 van de gemeente Dordrecht. Onderwerp van de verklaring is het gebruik van Suwinet. Deze verklaring heeft betrekking op de Verantwoordingsrichtlijn GeVS 2020 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. Dordrecht heeft een deel van de Suwinet taken en niet-SUWI-taken uitbesteed aan Gemeenschappelijke Regeling Drechtsteden – onderdeel Sociale Dienst Drechtsteden en Gemeenschappelijke Regeling Drechtsteden – onderdeel Gemeentebelastingen en Basisinformatie Drechtsteden. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisaties. 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 serviceorganisaties. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisaties 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 serviceorganisaties valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling (TPM) van onze serviceorganisaties.

Leverancier 1	
Naam serviceorganisatie:	Gemeenschappelijke Regeling Drechtsteden – onderdeel Sociale Dienst Drechtsteden (suwinet-inkijk)
Referentie/rapportnummer:	Wdn/esc/8149
Afgiftedatum:	17 maart 2021
Naam RE-auditor:	BDO Audit & Assurance BV Drs. W. Dalhuisen RE CISA
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)	Gemeenschappelijke Regeling Drechtsteden – onderdeel Sociale Dienst Drechtsteden	Ja, voor Suwinet-inkijk Nee, Voor DKD-inleesapplicaties. Dit is met de inclusive-methode beoordeeld
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Gemeenschappelijke Regeling Drechtsteden – onderdeel Sociale Dienst Drechtsteden	Ja, voor Suwinet-inkijk Nee, Voor DKD-inleesapplicaties. Dit is met de inclusive-methode beoordeeld
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Gemeenschappelijke Regeling Drechtsteden – onderdeel Sociale Dienst Drechtsteden	Ja, voor Suwinet-inkijk Nee, Voor DKD-inleesapplicaties. Dit is met de inclusive-methode beoordeeld

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	Niet van toepassing
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Gemeenschappelijke Regeling Drechtsteden – onderdeel Gemeentebelastingen en Basisinformatie Drechtsteden	Nee
Adresonderzoek door Burgerzaken	Gemeente Dordrecht – Dienstverlening Drechtsteden	Nee

Naleving BIO-maatregelen

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2020 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2020:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
Gemeenschappelijke Regeling Drechtsteden - onderdeel Sociale Dienst Drechtsteden	Participatiewet (Pw)	5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 9.2.6 10.1.1 12.1.1 12.4.1 12.4.2	DKD-Inlezen met Suwinet SDD - Liaan Berichtenplatform
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 12.1.1 12.4.1 12.4.2	Suwinet SDD - Liaan e-Dienstverlening (SaaS)
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 12.1.1 12.4.1 12.4.2	Suwinet SDD - Liaan SZ Inlichtingenbureau
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 10.1.1 12.1.1 12.4.1 12.4.2	Suwinet SDD - Centric koppelvlak
Gemeenschappelijke Regeling Drechtsteden - onderdeel Sociale Dienst Drechtsteden	Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 9.2.6 10.1.1 12.1.1 12.4.1	DKD-Inlezen met Suwinet SDD - Liaan Berichtenplatform

		12.4.2	
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 12.1.1 12.4.1 12.4.2	Suwinet SDD - Liaan e-Dienstverlening (SaaS)
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 12.1.1 12.4.1 12.4.2	Suwinet SDD - Liaan SZ Inlichtingenbureau
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 10.1.1 12.1.1 12.4.1 12.4.2	Suwinet SDD - Centric koppelvlak
Gemeenschappelijke Regeling Drechtsteden - onderdeel Sociale Dienst Drechtsteden	Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 9.2.6 10.1.1 12.1.1 12.4.1 12.4.2	DKD-Inlezen met Suwinet SDD - Liaan Berichtenplatform
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 12.1.1 12.4.1 12.4.2	Suwinet SDD - Liaan e-Dienstverlening (SaaS)
		5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 12.1.1 12.4.1	Suwinet SDD - Liaan SZ Inlichtingenbureau

12.4.2	
5.1.1 5.1.2 6.1.2 9.2.1 9.2.2 9.2.5 10.1.1 12.1.1 12.4.1 12.4.2	Suwinet SDD - Centric koppelvlak