



Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Oss

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Oss

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate Gemeente Oss 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 waar deze belegd zijn, is opgenomen in de bijlagen:

- Bijlage 1 DigiD met kenmerk Oss-ENSIA-2022-DigiD.
- Bijlage 2 Suwinet met kenmerk Oss-ENSIA-2022-Suwinet.

Verklaring college

Het college verklaart dat bij gemeente Gemeente Oss op 31 december 2022 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

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 1002739	Ja	Niet van toepassing
DigiD 1004363	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Oss, 11 april 2023

College van B en W gemeente Oss

De secretaris,

De burgemeester,

Henk Mensink

Wobine Buijs

Bijlage 1 DigiD - Gemeente Oss - Centric eDiensten Burgerzaken - 1002739

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Oss - Centric eDiensten Burgerzaken met aansluitnummer 1002739

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

- het verlenen van diensten door burgerzaken, zoals verstrekken van paspoorten, rijbewijzen, uittreksels.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- eDiensten Burgerzaken.

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

Deze applicatie is extern benaderbaar via het volgende internetadres:
<https://edienstenburgerzaken.oss.nl>.

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

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Oss - Centric 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 Oss heeft een deel van 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.

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 leverancier:

SaaS-leverancier	
Naam serviceorganisatie:	Centric Netherlands B.V.
Referentie/rapportnummer:	TPM: A2200025558
Afgiftedatum:	TPM: 14-10-2022
Naam RE-auditor:	B. (Brigitte) Beugelaar RE RA Partner
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM van onze leverancier het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaaemde 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 2C-2023-441.

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 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 1 DigiD - Gemeente Oss - Centric Mijn Inkomen - 1004363

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Oss - Centric Mijn Inkomen met aansluitnummer 1004363

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

- Diensten voor het sociale domein zoals uitkeringen verstrekken, zorg plannen, etc.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Selfservice Sociaal Domein, eDiensten, Mijn Inkomen, Mijn Regie.

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

Deze applicatie is extern benaderbaar via het volgende internetadres: <https://mijninkomen.oss.nl>.

DigiD-aansluiting Gemeente Oss - Centric Mijn Inkomen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Centric in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Oss - Centric Mijn Inkomen. 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 Oss heeft een deel van de DigiD web-omgeving uitbesteed aan Centric.

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 leverancier:

SaaS-leverancier	
Naam serviceorganisatie:	Centric
Referentie/rapportnummer:	TPM: A2200025558
Afgiftedatum:	TPM: 14-10-2022
Naam RE-auditor:	B. (Brigitte) Beugelaar RE RA
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM van onze leverancier 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 2C-2023-441.

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 SaaS-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 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2022 van gemeente Oss. 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 niet door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

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	
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente	
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente	
Wet gemeentelijke schuldhulpverlening (Wgs)	Binnen de gemeente	

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	
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing	
Adresonderzoek door Burgerzaken	Binnen de gemeente	

Naleving BIO-maatregelen

Zoals in de Collegeverklaring vermeld, voldoet gemeente Oss aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2022 in opzet en bestaan aan de geselecteerde controls.