

Collegeverklaring ENSIA 2019

inzake Informatiebeveiliging DigiD en Suwinet Gemeente Gennep

Gemeentelijk kenmerk collegeverklaring ENSIA:	369926
---	--------

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Gennep voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

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

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte en diepgang verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Gennep betreft dit in 2019 DigiD en Suwinet.

De verklaring omvat het op 31 december 2019 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2019.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener[s] vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk 369926-1) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener[s] worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener[s] worden uitgevoerd, wordt door de dienstverlener[s] verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener[s] dekken tezamen de normen inzake DigiD af.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 369926-1) en Suwinet (bijlage 2 Suwinet met kenmerk 369926-2) zijn de eventuele afwijkingen van de normen opgenomen.

De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 369926-1) en voor Suwinet (bijlage 2 Suwinet met kenmerk 369926-2) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Gennep op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in Verbeterplan opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1001501	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

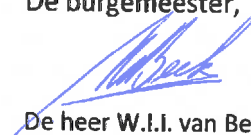
Gennep, 19 mei 2020

Burgemeester en Wethouders van Gennep,
De secretaris,



Mevrouw J.M. Nijland

De burgemeester,



De heer W.I.I. van Beek

Naam auditfirma:	BKBO bv (Bureau voor Kwaliteitsborging bij de Overheid)
Naam auditor:	drs. M.B.H. Ijpelaar RE CEH

Datum ondertekening auditor:	
Gemeentelijk kenmerk bijlage 1 DigiD:	369926-1

Bijlage 1 DigiD

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Gennep-Digitaal Loket en aansluitnummer 1001501

Gennep biedt de volgende functionaliteit aan waarvoor DigiD aansluiting Gemeente Gennep-Digitaal Loket voor authenticatie wordt gebruikt voor de volgende functionaliteiten: aanvraag rioolaansluiting, aanvraagformulier mantelzorgpas, aanvraagformulier subsidie afkoppelen hemelwater, bezwaar maken burger, contact Team Toegang, emigratie doorgeven, evenementenvergunning, gebruik achternaam veranderen, geheimhouding persoonsgegevens, ontheffing Blauwe zone eerste aanvraag, ontheffing Blauwe zone wijzigen kenteken, subsidie Stimulering Maatschappelijke Participatie, uittreksel Basis Registratie Personen, uittreksel burgerlijke stand en verhuizing doorgeven.

Deze functionaliteit wordt geboden door de volgende webapplicatie: SIMform.

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door SIMgroep.

Deze applicatie is extern benaderbaar via de volgende URL: <https://simsite.gennep.nl/>

DigiD aansluiting Gemeente Gennep-Digitaal Loket bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door Sentia in de vorm van Management Services.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Gemeente Gennep-Digitaal Loket. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL 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 Gennep heeft een deel van de DigiD webomgeving uitbesteed aan SIMgroep. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. 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 onze leverancier valt. De overige normen worden afgedekt door onderstaande TPM/assurancerapportage van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	SIMgroep
Referentie/rapportnummer:	SIMGR-1901-11.605
Afgiftedatum:	10 oktober 2019
Naam RE-auditor:	drs. F.W. (Wilfred) Hanekamp RE drs. ing. P.A. (Peter) Reezigt RE

Ondertekend door RE-auditor:	Ja
------------------------------	----

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM/ assurancerapportage 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 (zogenaaamde 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 BKBO/190805-10/AR.

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

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier1	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/ Privacy bevordering	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

DigiD Norm

B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.
Gemeentelijk kenmerk bijlage 2 Suwinet:	
369926-2	

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA 2019 van de gemeente Gennep. Deze verklaring heeft betrekking op het op 31 december 2019 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie Verantwoordingsstelsel ENSIA). Deze bijlage is opgesteld voor de gemeenteraad en het Ministerie van Sociale Zaken en Werkgelegenheid.

Onderwerp van de verklaring is het gebruik van Suwinet. Suwinet wordt niet in samenwerkingsverbanden gebruikt.

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie
Participatiewet (Pw)	Binnen de gemeente Gennep
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)	Binnen de gemeente Gennep
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente Gennep

Gebruik van Suwinet voor niet-SUWI-taken

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

Taak	Organisatie
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 Gennep

Normnaleving

Zoals in de collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2019 in opzet en bestaan aan de geselecteerde normen.