

Collegeverklaring ENSIA 2019

Inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Haarlem

Gemeentelijk kenmerk collegeverklaring ENSIA	2020/0408162
Naam auditfirma	Duijnborgh Audit B.V.
Naam auditor	Dhr. F. Kossen, RE
Datum	21 april 2020

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Haarlem 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 Haarlem 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 (de werking) van de maatregelen over 2019.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverleners vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk 2020/0408162) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverleners worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverleners worden uitgevoerd, wordt door de dienstverleners verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverleners dekken tezamen de normen inzake DigiD af.

Gemeente Haarlem is contactgemeente voor RMC regio 25 (West-Kennemerland) bestaande uit de gemeenten Bennebroek, Beverwijk, Bloemendaal, Haarlem, Heemskerk, Heemstede, Velsen en Zandvoort. Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op het gebruik van Suwinet voor de RMC-taken. Ingevolge de ENSIA-afspraken legt de gemeente Haarlem als contactgemeente de verantwoording af van het gebruik van Suwinet in het kader van de RMC taken. Gemeenten die geen contactgemeente zijn, laten deze verantwoording achterwege.

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 2020/0408162) en Suwinet (bijlage 2 Suwinet met kenmerk 2020/0408162) 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 2020/0408162) en voor Suwinet (bijlage 2 Suwinet met kenmerk 2020/0408162) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat voor DigiD en Suwinet niet aan alle geselecteerde normen wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan opgenomen, zijn belegd en worden gemonitord.

Voor zowel DigiD als voor Suwinet is een aantal gesignaleerde uitzonderingen al in orde gemaakt, planning is om uiterlijk 1 juni 2020 aan alle normen te voldoen.

Het verbeterplan beschrijft welke opvolging (correctieve maatregelen) er door gemeente Haarlem worden getroffen en welke verbetertermijn wordt gehanteerd. De externe toezichthouder kan oordelen dat bepaalde verbetermaatregelen sneller getroffen dienen te worden dan gepland.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD aansluiting: 1000081	Nee	Ja
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Nee	Ja

Haarlem, 21 april 2020

College van B en W gemeente Haarlem

mr. C.M. Lenstra
Gemeentesecretaris/Algemeen Directeur

drs. J. Wienen
Burgemeester

Bijlage 1 DigiD Webapplicatie Digitaal loket

1000081 – Gemeente Haarlem

Gemeentelijk kenmerk bijlage 1 DigiD	NOG IN TE VULLEN 1
Naam audit firma	Duijnborgh Audit B.V.
Naam auditor	Dhr. F. Kossen, RE

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting 1000081 – Gemeente Haarlem

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Gemeente Haarlem - 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 versie 2.0" van Logius.

Gemeente Haarlem biedt de volgende functionaliteit aan waarvoor DigiD aansluiting voor authenticatie wordt gebruikt: *het online aanvragen van gemeentelijke diensten en het maken van afspraken hiervoor*. Deze functionaliteit wordt geboden door de volgende webapplicatie: Digitaal Loket. Deze applicatie betreft maatwerk en wordt beheerd en onderhouden door de gemeente Haarlem.

Deze applicatie is extern benaderbaar via de volgende URL: <https://haarlem.nl/ufs/LOGIN/../> en bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door de gemeente Haarlem.

De onderzochte DigiD koppeling is bij Logius bekend onder de naam: '1000081-Gemeente Haarlem'

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage 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 HLM192528. Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Totaal oordeel norm
B.05	Contractmanagement	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheer proces	Voldoet niet	Voldoet niet
U/WA.03	Automatische data invoer controle	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	Voldoet niet	Voldoet niet
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
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 niet	Voldoet niet
C.09	Patchmanagement	Voldoet niet	Voldoet niet

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.

Bijlage 2 Gebruik van Suwinet

Gemeentelijk kenmerk bijlage 2 Suwinet	NOG IN TE VULLEN 2
Naam audit firma	Duijnborgh Audit B.V.
Naam auditor	Dhr. F. Kossen, RE

Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA 2019 van de gemeente Haarlem. 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 wel in samenwerkingsverbanden gebruikt. Het gebruik van Suwinet door samenwerkingsverbanden valt binnen de reikwijdte van de verklaring.

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie
Participatiewet (Pw)	Binnen de gemeente
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)	Binnen de gemeente
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	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
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Binnen de gemeente
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing
Adresonderzoek door Burgerzaken	Binnen de gemeente

Normnaleving

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de **SUWI-taken** op 31 december 2019 in opzet en bestaan aan alle geselecteerde normen:

Organisatie	SUWI-taak	BIG-nummer en nummer SUWI-norm	Applicatie
Gemeente Haarlem	Pw/IOAW/IOAZ	BIG: 5.1.1 Suwinet: B.01	Suwinet-Inkijk
Gemeente Haarlem	Pw/IOAW/IOAZ	BIG: 8.2.2 en 11.2.1 Suwinet: U.02	Suwinet-Inkijk

Gemeente Haarlem	Pw/IOAW/IOAZ	BIG: 5.1.2 en 6.1 Suwinet: C.01	Suwinet-Inkijk
Gemeente Haarlem	Pw/IOAW/IOAZ	BIG: 10.10.1 en 10.10.2 Suwinet: C.06	Suwinet-Inkijk

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de **niet-SUWI-taken** in opzet en bestaan aan alle geselecteerde normen:

Organisatie	Niet SUWI-taak	BIG-nummer en nummer SUWI-norm	Applicatie
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 5.1.1 Suwinet: B.01	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 6.1.2 Suwinet: B.04	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 6.1.3 en 10.1.3 Suwinet: B.05	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 8.2.2 en 11.2.1 Suwinet: U.02	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 11.2.1 en 11.5.2 Suwinet: U.03	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 5.1.2 en 6.1 Suwinet: C.01	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 11.2.4 Suwinet: C.04	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 10.10.1 en 10.10.2 Suwinet: C.06	Suwinet-Inkijk
Gemeente Haarlem	RMC-taken, Adresonderzoek door Burgerzaken	BIG: 8.2.2 Suwinet: AP	Suwinet-Inkijk