Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Haarlem

Gemeentelijk kenmerk collegeverklaring ENSIA: [2022/381296

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Haarlem

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate gemeente Haarlem 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 2021.

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 2022/381296
- Bijlage 2 Suwinet met kenmerk 2022/381296

Verklaring college

Het college verklaart dat bij gemeente Haarlem op 31 december 2021 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake Suwinet.
Voor DigiD wordt niet aan alle normen wordt voldaan. Wij hebben een verbeterplan 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), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet) en de Wet Onroerende Zaken (WOZ).

Gemeentelijk kenmerk collegeverklaring ENSIA:	**[2022/381296**

Samenvattend beeld

Onderwerp	**Wordt aan alle normen voldaan?**	**Zijn de uitzonderingen in een verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?**
DigiD 1003227	Ja	N.v.t.
DigiD 1000081	Nee	Ja
Suwinet voor SUWI-taken	Ja	N.v.t.
Suwinet voor niet-SUWI-taken	Ja	N.v.t.

Haarlem, 29 maart 2022

College van B&W Gemeente Haarlem

mr. C.M. Lenstra
Gemeentesecretaris/Algemeen Directeur

drs. J. Wienen
Burgemeester

Naam auditfirma:	Duijnborgh Audit
Naam auditor:	F. Kossen RE

Bijlage 1 (a) DigiD - Gemeente Haarlem - MijnHaarlem - 1003227

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Haarlem - MijnHaarlem met aansluitnummer 1003227

Gemeente Haarlem biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Haarlem - MijnHaarlem voor authenticatie wordt gebruikt:

- Identificatie voor toegang tot persoonlijke zaken in het zaaksysteem, digitaal postvak, afspraken en inzage in de brp gegevens.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- MijnHaarlem

Deze applicatie betreft een combinatie van maatwerk en standaard software en wordt onderhouden door gemeente Haarlem.

Deze applicatie is extern benaderbaar via het volgende internetadres: mijn.haarlem.nl.

DigiD-aansluiting Gemeente Haarlem - MijnHaarlem bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door gemeente Haarlem in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Haarlem - MijnHaarlem. 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.

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 **HLM212528**.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD-norm		Getoetst bij gemeente	Totaaloordeel norm
B.05	Contractmanagement	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheer proces	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	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
C.03	Vulnerability-assessments	Voldoet	Voldoet
C.04	Penetratietesten	Voldoet	Voldoet
C.06	Signaleringsfuncties	Voldoet	Voldoet
C.07	Monitoringfuncties	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet
C.09	Patchmanagement	Voldoet	Voldoet

Bijlage 1 (b) DigiD - Gemeente Haarlem - 1000081

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Haarlem met aansluitnummer 1000081

Gemeente Haarlem biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Haarlem 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 geheel maatwerk en wordt onderhouden door gemeente Haarlem.

Deze applicatie is extern benaderbaar via het volgende internetadres: www.haarlem.nl

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

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

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 **HLM212528**.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD-norm		Getoetst bij gemeente	Totaaloordeel norm
B.05	Contractmanagement	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheer proces	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	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
C.03	Vulnerability-assessments	Voldoet	Voldoet
C.04	Penetratietesten	Voldoet	Voldoet
C.06	Signaleringsfuncties	Voldoet	Voldoet
C.07	Monitoringfuncties	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet
C.09	Patchmanagement	**Voldoet niet**	**Voldoet niet**

(*) 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 vóór 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 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2021 van gemeente Haarlem. 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 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	Nee
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente	Nee
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente	Nee

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)	Gemeente Haarlem is contactgemeente en voert de RMC-taak uit voor de gemeenten Beverwijk, Bloemendaal, Haarlem. Heemskerk, Heemstede, Velsen en Zandvoort	Nee
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Binnen de gemeente	Nee
Adresonderzoek door Burgerzaken	Binnen de gemeente	Nee

Naleving BIO-maatregelen

Zoals in de Collegeverklaring vermeld, voldoet gemeente Haarlem aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2021 in opzet en bestaan aan de geselecteerde controls.