Collegeverklaring informatiebeveiliging
DigiD en Suwinet
Gemeente Haarlem

Gemeentelijk kenmerk collegeverklaring ENSIA:	20210104139

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 de 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 2020.

De beheersingsmaatregelen inzake DigiD 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 af. Het overzicht van normen eventuele afwijkingen en waar deze belegd zijn, is opgenomen in de bijlagen:

Bijlage 1 DigiD (1) met kenmerk 20210104139

Bijlage 1 DigiD (2) met kenmerk 20210104139

Bijlage 2 Suwinet met kenmerk 20210104139

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

Object	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD (1) 1000081	Nee	Ja
DigiD (2) 1003227	Nee	Ja
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Nee	Ja

Haarlem, 23 maart 2021

College van burgemeester en wethouders gemeente Haarlem

mr. C.M. Lenstra
Gemeentesecretaris/Algemeen Directeur

drs. J. Wienen
Burgemeester

Naam auditfirma:	Duijnborgh Audit
Naam auditor:	Frank Kossen RE

Gemeentelijk kenmerk bijlage 1 DigiD:	20210104139

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket en aansluitnummer 1000081

Gemeente Haarlem biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Digitaal Loket 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 Digitaal Loket 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 Digitaal Loket. 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 HLM202528.

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	• Voldoet
U/WA.03	Automatische data invoer controle	• 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	Monitoring functies	• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet
C.09	Patchmanagement	• Voldoet	• Voldoet

* Voor de norm U/PW.03 geldt dat aan de testaanpak wordt voldaan, behalve op de eisen voor ‘unsafe-inline’ en ‘unsafe-eval’. Gemeente Haarlem heeft voor het gebruik van ‘unsafe-inline’ en ‘unsafe-eval’ een ontwikkelplan opgesteld waarbij redelijkerwijs kan worden aangenomen dat vóór 1 november 2021 aan de gehele testaanpak voor de norm kan worden voldaan, dan wel dat er afdoende maatregelen zijn genomen om de risico’s van het gebruik van ‘unsafe-inline’ en ‘unsafe-eval’ te mitigeren.

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Haarlem - MijnHaarlem en 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 HLM202528.

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	• Voldoet
U/WA.03	Automatische data invoer controle	• 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	Monitoring functies	• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet
C.09	Patchmanagement	• Voldoet	• Voldoet

* Voor de norm U/PW.03 geldt dat aan de testaanpak wordt voldaan, behalve op de eisen voor ‘unsafe-inline’ en ‘unsafe-eval’. Gemeente Haarlem heeft voor het gebruik van ‘unsafe-inline’ en ‘unsafe-eval’ een ontwikkelplan opgesteld waarbij redelijkerwijs kan worden aangenomen dat vóór 1 november 2021 aan de gehele testaanpak voor de norm kan worden voldaan, dan wel dat er afdoende maatregelen zijn genomen om de risico’s van het gebruik van ‘unsafe-inline’ en ‘unsafe-eval’ te mitigeren.

Gemeentelijk kenmerk bijlage 2 Suwinet:	20210104139

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2020 van de 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 dient de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking te worden 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	Niet van toepassing	Nee
Adresonderzoek door Burgerzaken	Binnen de gemeente	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
Binnen de gemeente	Participatiewet (Pw)	7.2.2 10.1.1 12.1.1 12.4.2	Suwinet-Inkijk DKD-Inlezen met MensCentraal
Binnen de gemeente	Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	7.2.2 10.1.1 12.1.1 12.4.2	Suwinet-Inkijk DKD-Inlezen met MensCentraal
Binnen de gemeente	Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	7.2.2 10.1.1 12.1.1 12.4.2	Suwinet-Inkijk DKD-Inlezen met MensCentraal

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

Organisatie	Niet-SUWI-taak	BIO-maatregel	Applicatie
Binnen de gemeente	Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	6.1.2 7.2.2 9.2.1 9.2.2 9.2.5 9.2.6 12.4.1 18.1.4	Suwinet-Inkijk
Niet van toepassing	Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing	Niet van toepassing
Binnen de gemeente	Adresonderzoek door Burgerzaken	6.1.2 7.2.2 9.2.1 9.2.2 9.2.5 9.2.6 12.4.1 18.1.4	Suwinet-Inkijk