

## Bijlage E

### Bijlage 1a - 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](http://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 IAS1831\_0473\_22

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

| DigiD-norm     |  | Getoetst bij aansluithouder | Totaaloordeel norm |
|----------------|--|-----------------------------|--------------------|
| <b>B.01</b>    | Informatiebeveiligingsbeleid           | Voldoet niet                | Voldoet niet       |
| <b>B.05</b>    | Contractmanagement                     | Voldoet                     | Voldoet            |
| <b>U/TV.01</b> | Identificatie en authenticatie         | Voldoet                     | Voldoet            |
| <b>U/WA.02</b> | Webapplicatiebeheerproces              | Voldoet                     | Voldoet            |
| <b>U/WA.03</b> | Automatische data-invoercontrole       | Voldoet                     | Voldoet            |
| <b>U/WA.04</b> | Normaliseren uitvoer                   | Voldoet                     | Voldoet            |
| <b>U/WA.05</b> | Cryptografie/ Privacybevordering       | Voldoet                     | Voldoet            |
| <b>U/PW.02</b> | Garanderen webprotocollen              | Voldoet                     | Voldoet            |
| <b>U/PW.03</b> | Configureren webserver                 | Voldoet                     | Voldoet            |
| <b>U/PW.05</b> | Toegang tot beheermechanismen          | Voldoet                     | Voldoet            |
| <b>U/PW.07</b> | Hardening van platformen               | Voldoet                     | Voldoet            |
| <b>U/NW.03</b> | DMZ                                    | Voldoet                     | Voldoet            |
| <b>U/NW.04</b> | Protectie- en detectiemechanismen      | Voldoet                     | Voldoet            |
| <b>U/NW.05</b> | Scheiding beheer- en productieomgeving | Voldoet                     | Voldoet            |
| <b>U/NW.06</b> | Hardening van netwerken                | Voldoet                     | Voldoet            |
| <b>C.03</b>    | Vulnerability-assessments              | Voldoet                     | Voldoet            |
| <b>C.04</b>    | Penetratietesten                       | Voldoet                     | Voldoet            |
| <b>C.06</b>    | Signaleringsfuncties                   | Voldoet                     | Voldoet            |
| <b>C.07</b>    | Monitoringfuncties                     | Voldoet                     | Voldoet            |
| <b>C.08</b>    | Wijzigingenbeheer                      | Voldoet                     | Voldoet            |
| <b>C.09</b>    | Patchmanagement                        | Voldoet                     | Voldoet            |

## Bijlage 1b – 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 IAS1831\_0473\_22.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

| DigiD-norm |  | Getoetst bij aansluithouder | Totaaloordeel norm |
|------------|--|-----------------------------|--------------------|
| B.01       | Informatiebeveiligingsbeleid           | Voldoet niet                | Voldoet niet       |
| B.05       | Contractmanagement                     | Voldoet                     | Voldoet            |
| U/TV.01    | Identificatie en authenticatie         | Voldoet                     | Voldoet            |
| U/WA.02    | Webapplicatiebeheerproces              | Voldoet niet                | Voldoet niet       |
| 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 1c – DigiD - Parkeren Gemeente Haarlem - 1004599

### Totaaloverzicht getoetste normen ICT-beveiligingsassessment

#### DigiD-aansluiting Parkeren Gemeente Haarlem met aansluitnummer 1004599

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

- Het online vergunningen systeem voor de uigifte van vergunningen en ontheffingen op kenteken.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Parkeren Gemeente Haarlem

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Sigmax Law Enforcement BV.

Deze applicatie is extern benaderbaar via het volgende internetadres: [parkeren.haarlem.nl](http://parkeren.haarlem.nl)

DigiD-aansluiting Parkeren Gemeente Haarlem bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Sigmax Law Enforcement BV in de vorm van SaaS.

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

Gemeente Haarlem heeft een deel van de DigiD web-omgeving uitbesteed aan Sigmax Law Enforcement BV.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). 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(s) van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van de leverancier(s):

| SaaS-leverancier             |                                    |
|------------------------------|------------------------------------|
| Naam serviceorganisatie:     | Sigmax Law Enforcement BV          |
| Referentie/rapportnummer:    | TPM 1: 2209R.AH70<br>TPM 2: N.v.t. |
| Afgiftedatum:                | TPM 1: 29-09-2022<br>TPM 2: N.v.t. |
| Naam RE-auditor:             | 3angles                            |
| Ondertekend door RE-auditor: | Ja                                 |

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze leverancier(s) 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 IAS1831\_0473\_22.

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

| DigiD-norm     |  | Getoetst bij aansluitouder | Getoetst bij SaaS-leverancier | Totaaloordeel norm |
|----------------|--|----------------------------|-------------------------------|--------------------|
| <b>B.01</b>    | Informatiebeveiligingsbeleid           | Voldoet niet               | Voldoet                       | Voldoet niet       |
| <b>B.05</b>    | Contractmanagement                     | Voldoet                    | Voldoet                       | Voldoet            |
| <b>U/TV.01</b> | Identificatie en authenticatie         | Voldoet                    | Voldoet                       | Voldoet            |
| <b>U/WA.02</b> | Webapplicatiebeheerproces              | Voldoet                    | Voldoet                       | Voldoet            |
| <b>U/WA.03</b> | Automatische data-invoercontrole       | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/WA.04</b> | Normaliseren uitvoer                   | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/WA.05</b> | Cryptografie/ Privacybevordering       | Voldoet                    | Voldoet                       | Voldoet            |
| <b>U/PW.02</b> | Garanderen webprotocollen              | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/PW.03</b> | Configureren webserver                 | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/PW.05</b> | Toegang tot beheermechanismen          | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/PW.07</b> | Hardening van platformen               | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/NW.03</b> | DMZ                                    | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/NW.04</b> | Protectie- en detectiemechanismen      | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/NW.05</b> | Scheiding beheer- en productieomgeving | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>U/NW.06</b> | Hardening van netwerken                | Voldoet                    | Voldoet                       | Voldoet            |
| <b>C.03</b>    | Vulnerability-assessments              | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>C.04</b>    | Penetratietesten                       | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>C.06</b>    | Signaleringsfuncties                   | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>C.07</b>    | Monitoringfuncties                     | N.v.t.                     | Voldoet                       | Voldoet            |
| <b>C.08</b>    | Wijzigingenbeheer                      | Voldoet                    | Voldoet                       | Voldoet            |
| <b>C.09</b>    | Patchmanagement                        | N.v.t.                     | Voldoet                       | Voldoet            |