



EINDHOVEN

Gemeente Eindhoven  
Stadhuisplein 10  
5611 EM Eindhoven

Eindhoven, 01 mei 2018

SafeHarbour Bv  
B.Building  
John M. Keynesplein 12-46  
1066 EP Amsterdam

Betreft : Letter of representation

Geachte heer/mevrouw,

Deze bevestiging wordt afgegeven in samenhang met uw opdracht tot het uitvoeren een ENSIA audit bij de gemeente Eindhoven.

De scope van de ENSIA audit is gericht op:

- DigiD aansluiting nr [REDACTED] Met aansluitnaam DigiD Eindhoven.
- SUWI aansluiting gemeente Eindhoven

\*\*\* en  
\*\*\*\*

Deze opdracht is uitgevoerd overeenkomstig Nederlands recht en de NOREA-richtlijn 3000D, "Richtlijn Assurance-opdrachten door IT-auditors" in de vorm van een directe opdracht.

Wij hebben, voor zover wij dat noodzakelijk en relevant achten om ons adequaat te informeren, navraag gedaan bij leidinggevenden en medewerkers van onze organisatie met relevante kennis en ervaring. Dienovereenkomstig, bevestigen wij naar ons beste weten en overtuiging het volgende:

### *Verantwoordelijkheid*

Wij bevestigen dat wij verantwoordelijk zijn voor:

- Het opzetten, implementeren en onderhouden van de maatregelen van interne beheersing gericht op het voorkomen en ontdekken van beveiligingsincidenten;
- Het aanleveren van alle informatie en inzicht geven tot systemen die relevant zijn voor het uitvoeren van de opdracht;



- Het niet onbenoemd blijven van de volgende zaken, indien deze zich hebben voorgedaan binnen onze organisatie:
  - Het niet naleven van wet- en regelgeving, fraude en ongecorrigeerde afwijkingen waar wij verantwoordelijk voor zijn.
  - Tekortkomingen in de opzet en bestaan van interne beheersingsmaatregelen;

## ***Bewering van het management***

Hierbij bevestigen wij dat:

- alle informatie is aangeleverd over beheersmaatregelen die we beschreven, ontworpen, geïmplementeerd en uitgevoerd hebben om de beheer doelstellingen te bereiken.
- u onbeperkte toegang heeft gekregen tot personen binnen onze gemeente die relevant zijn voor de uitvoering van uw werkzaamheden.

## ***Overige bevestigingen***

Wij bevestigen naar ons beste weten en overtuiging het volgende:

1. De beschrijving van de interne beheersmaatregelen waar hierboven naar verwezen wordt, zijn juist en volledig gepresenteerd, in alle van materieel belang zijnde aspecten.
2. Er zijn geen bewuste tekortkomingen in de opzet van interne beheersingsmaatregelen;
3. Wij hebben u alle relevante informatie verschaft die van belang is en kan zijn voor de opdracht.
4. Ons zijn geen overtredingen of vermoedelijke overtredingen bekend van het niet naleven van de relevante wet- en regelgeving die één of meer gebruikende entiteiten kunnen beïnvloeden;
5. Wij hebben u alle gebeurtenissen gemeld tot 22 maart 2018, de dag van de audit, die een significantie invloed zouden kunnen hebben op het Assurance-rapport. Er zijn sinds deze datum tot de dag van deze brief geen significante wijzigingen geweest.

Hoogachtend,

Gemeente Eindhoven

Namens

De gemeenteraad

\*\*

# Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Eindhoven legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

## Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigiD (aansluitnummer: [REDACTED]) en Suwinet aansluitingen bij de Gemeente Eindhoven. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK<sup>1</sup>) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI<sup>2</sup> en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA<sup>3</sup> voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

\*\*\* en  
\*\*\*\*

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring "bijlage 1 DigiD" blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD Gouw) en Suwinet (bijlage 2 Suwinet Eindhoven) geïnformeerd over de afwijkingen van de normen.

1 <https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/>

2 <https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten>

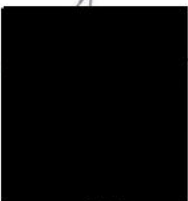
3 <https://www.ensia.nl/>



## Verklaring college

Het college verklaart dat bij gemeente Eindhoven op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID en Suwinet.

Eindhoven,

College van  te Eindhoven

\*\*


# Bijlage 1 DigiD eGouw Eindhoven

## Rapportage DigiD Assessment - ENSIA 2017

### gemeente Eindhoven

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting: Vul het Logius aansluitnummer in:	██████
Naam DigiD aansluiting: Vul de aansluitnaam in van de aansluiting:	DIGID Eindhoven
Externe infrastructuur-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Nee
Naam leveranciers: Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	
TPM datum: Voer hier de datum in van het TPM rapport.	
Applicatieleverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Ja
Naam leverancier: Geef de naam op van de applicatieleverancier.	GouwIT
TPM datum: Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	10-10-2017
TPM kenmerk: Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	BKBO/171010.201/AR
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	
SaaS-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Nee
Naam leverancier: Geef de naam op van de SaaS-leverancier.	
TPM datum: Voer hier de datum in van het TPM rapport.	
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	
Bij SaaS-leverancier: U kunt de TPM's hier uploaden	
TPM aanwezigheid: Leveren alle leveranciers een TPM op?	Ja
Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	
Reikwijdte TPM: Hebben de TPM's dezelfde scope als de DigiD aansluiting?	Ja
Reikwijdte TPM: Hanteren de TPM's hetzelfde normenkader als het DigiD normenkader 2.0?	Ja

\*\*\* en  
\*\*\*\*

Reikwijdte TPM: Zijn de TPM's maximaal 1 jaar oud?	Ja
Reikwijdte TPM: Heeft u als coördinator vastgesteld dat de overige normen, buiten de 5 waar u verantwoordelijk voor bent, door de TPM worden afgedekt?	Ja
Reikwijdte TPM: Zijn de TPM's eerder gebruikt voor een DigiD assessment voor dezelfde aansluiting?	Nee
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	
Externe auditor: Vul de namen in van de externe auditors:	
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Nee
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	B.05 U/TV.01 U/WA.02 U/WA.05 U/PW.02 U/PW.03 C.04 C.08 C.09

\*\*

Paraaf: 

## Bijlage 1B - Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting [REDACTED] en DIGID Eindhoven.

Gemeente Eindhoven biedt de volgende functionaliteit aan waarvoor DigiD aansluiting [REDACTED] voor authenticatie wordt gebruikt: Een webportaal waarbinnen de eGouw module een aantal vaste formulieren toont voor de communicatie tussen burger en gemeentelijke dienst belastingen, die gebruik maakt van Gouw Belastingen.

Deze applicatie betreft standaard software en wordt onderhouden door GouwIT

Deze applicatie is extern benaderbaar via de volgende URL(s):

<https://belastingbalie.eindhoven.nl/egouw/>

Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Paraaf: [REDACTED]

\*\*\* en  
\*\*\*\*

\*\*



## Bijlage 1C - Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van de gemeente Eindhoven

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting [REDACTED] en DIGID Eindhoven.

\*\*\* en  
\*\*\*\*

Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst: B.05, U/TV.01, U/WA.02, U/WA.05. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van GouwIT, BKBO/171010.201/AR, 10-10-2017, ondertekend door mr [REDACTED]

\*\*

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van GouwIT, BKBO/171010.201/AR, 10-10-2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Norm	Beschrijving van de norm	Getoetst bij leverancier	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruiker	Referentie/ rapportnummer
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.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Ja	Voldoet	Dit rapport



Norm	Beschrijving van de norm	Getoetst bij leverancier	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruiker	Referentie/ rapportnummer
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.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Nee	Voldoet	Dit rapport
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Ja	Niet van toepassing	
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	DIGID koppeling: gemeente Eindhoven2BKBO/171010.201/AR			

Norm	Beschrijving van de norm	Getoetst bij leverancier	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruiker	Referentie/ rapportnummer
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR			
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Ja	Voldoet	
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Nee	Voldoet	
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Nee	Voldoet	

Norm	Beschrijving van de norm	Getoetst bij leverancier	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruiker	Referentie/ rapportnummer
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.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
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.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	

Norm	Beschrijving van de norm	Getoetst bij leverancier	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruiker	Referentie/ rapportnummer
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Nee	Voldoet	
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	
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.		DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	



Norm	Beschrijving van de norm	Getoetst bij leverancier	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruiker	Referentie/ rapportnummer
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR	Ja	Voldoet	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet	DIGID koppeling: gemeente Eindhoven2 BKBO/171010.201/AR		Voldoet	

Paraaf: 

\*\*

## Bijlage 2 Suwinet Eindhoven

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet van de gemeente Eindhoven.

De gemeente Eindhoven gebruikt Suwinet voor de volgende werkzaamheden: uitvoering Wet werk en inkomen; schuldhulpverlening; arbeidsintegratie; sociale werkvoorziening; budgethulp; krediethulpverlening en het ondersteunen van jongeren tussen de 18 en 23 die de school hebben verlaten zonder een startkwalificatie.

De Suwinet diensten worden geboden door de volgende webapplicaties die door BKWI ter beschikking worden gesteld via het besloten netwerk Gemnet:

- Suwinet Inkijk
- Suwinet Mail

### Afwijkingen van de normen

Tijdens de ENSIA zelfevaluatie zijn geen afwijkingen ten opzichte van het normenkader gesignaleerd.

Paraaf: 

\*\*