Nota voor burgemeester en wethouders
Onderwerp
Collegeverklaring ENSIA

Team
DOWR-I

1- Notagegevens	
Notanummer	2020-000228
Datum	17-02-2020
Programma:	
12 Bedrijfsvoering	
Portefeuillehouder	Burgemeester
	Burgemeester

2- Bestuursorgaan	
[X]B & W	07-04-2020
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Grijsen
- Weth. De Geest	- Weth. Verhaar
- Weth. Walder	- Weth. Rorink

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	07-04-2020	[ ]Besloten	--

Routing	d.d.
Burgemeester	01-04-2020
Gemeentesecretaris	01-04-2020
Programmamanager	31-03-2020

	par.
[ ]adj.secr.	--
[X]gem.secr.	01-04-2020
BIS Openbaar	
Status	Definitief2020-04-08

Bijlagen
Collegeverklaring-ENSIA-2019-inzake-Informatiebeveiliging-DigiD-en-Suwinet-Deventer
Verantwoordingsrapportage-BAG---2019-Deventer (Vertrouwelijk)
Verantwoordingsrapportage-BGT---2019-Deventer (Vertrouwelijk)
Verantwoordingsrapportage-BRO---2019-Deventer (Vertrouwelijk)
Assurancerapport DigID (Vertrouwelijk)

B & W d.d.: 07-04-2020

Besloten wordt:
1 De collegeverklaring ENSIA 2019 inzake informatiebeveiliging DigiD en Suwinet af te geven;
2 de verantwoordingsrapportages over de BAG, BGT en BRO vast te stellen;
3 de nota en het besluit openbaar te maken, met uitzondering van de bijlagen.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[ ] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[X]De nota en het besluit openbaar te maken, behalve…
De bijlage(n) niet openbaar maken vanwege de economische of financiële belangen van de gemeente (art. 10 lid 2 onder b) en het voorkomen van onevenredige benadeling (art. 10 lid 2 onder g).
[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

gemeente Deventer

Kennisgeving/ Bekendmaking Awb

Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

ADVIESRADEN:

Moet een van de adviesraden gehoord worden of op de hoogte gesteld?	Nee

Toelichting

Inleiding

ENSIA

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

.

Algemeen

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad en aan de rijksoverheid. Dit voeren wij uit door middel van een zelfevaluatie.Suwinet en DigiD zijn getoetst met een IT audit.

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 zorgt ENSIA ook voor de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), BasisregistratieGrootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuuruitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Collegeverklaring ENSIA

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover Assurance (goedkeurende verklaring) wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2019 betreft dit DigID en Suwinet. De verklaring omvat het op 31 december 2019 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De Collegeverklaring omvat niet de werking van de maatregelen over 2019. Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen voldoen aan de voor de ENSIA verantwoording geselecteerde normen en indien aan de orde welke onderdelen daarvan zijn uitgezonderd. Ook wordt melding gemaakt van eventuele verbetermaatregelen, die de gemeente gaat treffen.

Assurance rapport

Een bij de NOREA (Beroepsorganisatie IT-auditors) geregistreerde IT-auditor controleert de Collegeverklaring en stelt een Assurance rapport op. Deze werkzaamheden van de IT-auditor duiden we ook wel aan als de IT-audit. De IT-auditor verklaart in het Assurance rapport, dat de Collegeverklaring een getrouw beeld geeft. Getrouw betekent dat de collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de Collegeverklaring.

Verantwoordingsrapportages BAG, BGT en BRO

Aan de hand van de jaarlijkse zelfevaluatie Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT) en de Basisregistratie Ondergrond (BRO) zijn verantwoordingsrapportages opgesteld. Met het vaststellen van de verantwoordingsrapportages wordt horizontaal verantwoording afgelegd aan de gemeenteraad over de uitvoering van de Wet BAG, de Wet BGT en de Wet BRO. Verticaal wordt verantwoording afgelegd aan het Ministerie van Infrastructuur en Milieu, als formeel toezichthouder van de drie genoemde registraties.

Tot slot

Het uiteindelijke doel is om de kwaliteit van onze informatiebeveiliging op een hoog niveau te houden. Het assurancerapport heeft uitgewezen, dat we voor 2019 onze zaken goed op orde hebben en extra maatregelen

niet nodig zijn. Verder is er een evaluatie ENSIA geweest waarin is geconstateerd, dat de Collegeverklaringen nog onvoldoende leesbaar zijn en is het streven om dit volgend jaar sterk te verbeteren.

Beoogd resultaat

Met ENSIA verantwoorden we ons gemeentebreed over informatieveiligheid.

Kader

VNG-resolutie "Informatieveiligheid randvoorwaarde voor de professionele gemeente" uit 2013.

Argumenten voor en tegen

Voor:

- transparant verantwoording afleggen
- voldoen aan de BIG (baseline informatiebeveiliging gemeenten)

Extern draagvlak (partners)

Afgestemd in DOWR verband.

Financiële consequenties

nvt

Aanpak/uitvoering

De Collegeverklaring wordt gezamenlijk met het Assurance DigID rapport, BAG rapport, BGT rapport, BRO rapport meegenomen, als bijlage bij de Nota. De bijlagen worden ook toegestuurd aan de toezichthouders van de desbetreffende Ministeries. Voor DigID, BAG, BGT en BRO is dit het Ministerie van Binnenlandse zaken. Voor Suwinet is dit het Ministerie voor Sociale Zaken en Werkgelegenheid.
In het jaarverslag Informatiebeveiliging (bij de jaarrekening) is een paragraaf ENSIA opgenomen, die aan de gemeenteraad wordt aangeboden.

Collegeverklaring ENSIA 2019

Inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Deventer

Gemeentelijk kenmerk collegeverklaring ENSIA:	2020-000228

Collegeverklaring ENSIA 2019 inzake Informatiebeveiliging DigiD en Suwinet.

Gemeente Deventer

Doel en achtergrond verklaring

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

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener[s] vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk **DigID 2020-000228** blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener[s] worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener[s] worden uitgevoerd, wordt door de dienstverlener[s] verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de normen inzake DigiD af. Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersmaatregelen van de gemeente.

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 **DigID 2020-000228**) en Suwinet (bijlage 2 Suwinet met kenmerk **Suwinet 2020-000228**) 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 **DigID 2020-000228**) en voor Suwinet (bijlage 2 Suwinet met kenmerk **Suwinet 2020-000228**) geïnformeerd over de afwijkingen van de normen.

Verklaring college

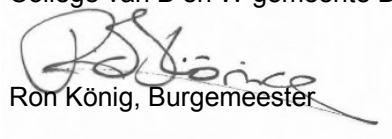
Het college verklaart dat bij gemeente Deventer op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1002175	Ja	Niet van toepassing
DigiD 1000305	Ja	Niet van toepassing
DigiD 1002973	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Deventer, 7 april 2020

College van B en W gemeente Deventer



Ron König, Burgemeester

Naam auditfirma:	RSM Risk Advisory Services B.V.
Naam auditor:	M. Hommes RE
Datum [ondertekenen auditor]	Handtekening of paraaf auditor:

Gemeentelijk kenmerk bijlage 1 DigiD:	DigID 2020-000228

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Deventer4 en aansluitnummer 1002175

Deventer biedt de volgende functionaliteit aan waarvoor DigiD aansluiting Deventer 4 voor authenticatie wordt gebruikt:

- Aangifte geboorte
- Aangifte verhuizing
- Aanvraag afschrift Burgerlijke stand
- Aanvraag afschrift Burgerlijke stand voor bedrijven
- Aanvraag bewijs van in leven zijn
- Aanvraag bewijs van Nederlanderschap
- Aanvraag uittreksel BRP
- Aanvraag uittreksel BRP voor bedrijven
- Verstrekking beperking
- Wijziging naamgebruik
- Melding huwelijk/geregistreerd partnerschap
- Aangifte overlijden

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken, versie 3.0.

Deze applicatie betreft geheel standaardpakket en wordt onderhouden door PinkRoccade LG.

Deze applicatie is extern benaderbaar via de volgende URL: https://iburgerzaken.deventer.nl.

DigiD aansluiting Deventer4 bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd Pink Roccade LG in de vorm van SAAS.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Deventer4. 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” van Logius.

Gemeente Deventer heeft een deel van de DigiD webomgeving uitbesteed aan Pink Roccade LG. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze service organisatie. 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 onze leverancier[s] valt. De overige normen worden afgedekt door onderstaande TPM van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	PinkRoccade Local Government B.V.
Referentie/rapportnummer:	20191021 DBA-PRLG
Afgiftedatum:	21 oktober 2019
Naam RE-auditor:	F. Kossen RE

	Drs. M. El Aarbaoui RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM 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 202003GEMDEV.

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

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet	• 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		• Voldoet	• Voldoet

	detectiemechanismen			
U/NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• 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	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

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 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket Gemeente Deventer en aansluitnummer 1000305

Deventer biedt de volgende functionaliteit aan waarvoor DigiD aansluiting Digitaal Loket Gemeente Deventer voor authenticatie wordt gebruikt:

- Aan- en afmelden hondenbelasting
- Belastingen; betalingsregeling
- Bezwaarschrift
- Bijstandsverlening; Uitkering
- Bodembescherming; intake
- Collectevergunning
- Demonstratie of betoging
- Evenement; aanwijzen verkeersregelaar
- Evenement; melding
- Evenementenvergunning
- Gegevensbescherming; AVG
- Gehandicaptenparkeerkaart
- Gehandicaptenparkeerplaats
- Gehandicaptenparkeerplaats; wijzigen kenteken
- Geluidontheffing
- Groenstrook; intake
- Grondgebruik t.b.v. activiteiten
- Grootburgerrecht
- Huisnummer toekenning; verzoek
- Inkomenstoeslag
- Inspraak Intake
- Kamerverhuur; omzettingsvergunning
- Kamerverhuur; voortzetting
- Kamerverhuur; wijzigen aantal kamers
- Kamerverhuur; wijzigen tenaamstelling omzettingsvergunning
- Kamperen buiten kampeerinrichting
- Kansspelvergunning
- Kinderopvang; gastouderbureau registratie
- Kinderopvang; gastouderbureau wijziging
- Kinderopvang; voorziening gastouderopvang registratie
- Kinderopvang; voorziening gastouderopvang wijziging
- Leerlingenvervoer
- Ligplaats woonschip
- Marktstandplaats
- Mobiele puinbreker
- Ontheffing straatartiest/fotograaf/filmen/leden werven
- Parkeerabonnement (garage) bewoners
- Parkeervergunning bewoners
- Parkeervergunning bewoners; wijziging
- Parkeervergunning bezoekers particulieren
- Planschadevergoeding
- Stookontheffing
- Straatnaamgeving
- Subsidie
- Subsidie amateurkunst projecten

- Subsidie amateurkunst structureel
- Subsidie kleintje cultuur
- Subsidie; wijkbudget
- Verklaring geen bezwaar
- WMO Melding
- Woning verhuren (Leegstandswet)
- Zienswijze Intake

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- e-Suite, versie 4.22

Deze applicatie betreft geheel standaard pakket en wordt ontwikkeld en onderhouden door Atos.

Deze applicatie is extern benaderbaar via de volgende URL: https://dloket.deventer.nl.

DigiD aansluiting Digitaal Loket Gemeente Deventer bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door SSC Twente in de vorm van fysieke hosting.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Digitaal Loket Gemeente Deventer. 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” van Logius.

Gemeente Deventer heeft een deel van de DigiD webomgeving uitbesteed aan Dimpact en Dimpact heeft het ontwikkelen van de webapplicatie en het beheer van de infrastructuur uitbesteed aan serviceorganisaties Atos en SSC Twente. Dimpact maakt voor haar beschrijving gebruik van de opnamemethode (‘inclusive method’). De beschrijving van de serviceorganisatie van haar systeem omvat tevens de aard van de diensten die door de subserviceorganisaties worden verleend. De relevante interne beheersingsdoelstellingen van die subserviceorganisaties en daarmee verband houdende interne beheersingsmaatregelen zijn opgenomen in de beschrijving van de serviceorganisatie van haar systeem en in de reikwijdte van de opdracht van de auditor van de serviceorganisatie. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. 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 onze leverancier[s] valt. De overige normen worden afgedekt door onderstaande TPM van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Dimpact (inclusief Atos en SSC Twente)
Referentie/rapportnummer:	DIMPA-1901-11.605
Afgiftedatum:	28 november 2019
Naam RE-auditor:	drs. F.W. Hanekamp RE ing. I.E. Veen RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM 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 202003GEMDEV.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet	• 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	• 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	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

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 1 DigiD (3)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Belastingloket en aansluitnummer 1002973

Deventer biedt de volgende functionaliteit aan waarvoor DigiD aansluiting Belastingloket voor authenticatie wordt gebruikt:

- Raadplegen aanslaggegevens
- Raadplegen openstaand saldo aanslag
- Raadplegen kopie aanslag
- Raadplegen taxatieverslagen
- Bezwaar indienen tegen aanslag/wozwaarde
- Contactformulier algemeen
- Formulier opvragen ledigingsgegevens
- Formulier kwijtschelding
- Formulier betalingsregeling
- Formulier automatische incasso

Deze functionaliteit wordt geboden door de volgende webapplicatie(s):

- PIP (Persoonlijke Internet Pagina), versie 1.55.0
- SIMform, versie 1.13.0

Deze applicatie betreft geheel standaard en wordt onderhouden door SIMgroep.

Deze applicatie is extern benaderbaar via de volgende URL: https://www.belastingloketdowr.nl/ en https://mijn.belastingloketdowr.nl/.

DigiD aansluiting Belastingloket bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door SIMgroep in de vorm van SAAS. SIMgroep heeft de hosting van de webapplicaties en een gedeelte van het beheer van de infrastructuur uitbesteed aan serviceorganisatie Sentia, in de vorm van Managed Services. SIMgroep maakt voor haar beschrijving gebruik van de opnamemethode (‘inclusive method’). De beschrijving van de serviceorganisatie haar systeem omvat tevens de aard van de diensten die door de subserviceorganisatie worden verleend. De relevante interne beheersingsdoelstellingen van die subserviceorganisatie en daarmee verband houdende interne beheersingsmaatregelen zijn opgenomen in de beschrijving van de serviceorganisatie van haar systeem en in de reikwijdte van de opdracht van de auditor van de serviceorganisatie.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Belastingloket. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL[‘s] 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 Deventer heeft een deel van de DigiD webomgeving uitbesteed aan SIMgroep. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. 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 onze leverancier valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	SIMgroep
Referentie/rapportnummer:	SIMGR-1901-11.605

Afgiftedatum:	10 oktober 2019
Naam RE-auditor:	drs. F.W. Hanekamp RE drs. ing. P.A. Reezigt RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM van onze serviceorganisatie het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is.

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 202003GEMDEV.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm

DigiD Norm		**Getoetst bij Gemeente**	**Getoetst bij leverancier 1**	**Totaal oordeel norm**
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet	• 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	• 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	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

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.

Gemeentelijk kenmerk bijlage 2 Suwinet:	Suwinet 2020-000228

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA 2019 van de gemeente Deventer. 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 niet in samenwerkingsverbanden gebruikt.

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)	Niet van toepassing
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	binnen de gemeente
Adresonderzoek door Burgerzaken	binnen de gemeente

Normnaleving

Zoals in de collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2019 in opzet en bestaan aan de geselecteerde normen.