Nota voor burgemeester en wethouders
Onderwerp
Collegeverklaring ENSIA

Team
DEV-SVC

1- Notagegevens	
Notanummer	2018-000771
Datum	10-04-2018
Programma:	
11 Bedrijfsvoering	
Portefeuillehouder	Burgemeester

2- Bestuursorgaan	
[X]B & W	24-04-2018
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Kolkman
- Weth. Grijsen	- Weth. Rorink

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	24-04-2018	[ ]Besloten	--

Routing	d.d.
Directeur	18-04-2018
Portefeuillehouder	18-04-2018

	par.
[ ]adj.secr.	--
[X]gem.secr.	18-04-2018
BIS Openbaar	
Status	Definitief2018-04-25

Bijlagen

B & W d.d.: 24-04-2018

Besloten wordt:
1 De collegeverklaring ENSIA 2017 inzake informatiebeveiliging DigiD en Suwinet af te geven;
2 de nota en het besluit openbaar te maken, behalve de 2 bijlages.

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…
2 niet openbare bijlages op grond van artikel 10 WOB
[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

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

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.

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 Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Collegeverklaring ENSIA

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 en Suwinet.

De verklaring omvat het op 31 december 2017 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 2017.

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 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.

DigiD en Suwinet

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 en Suwinet.
De verklaring omvat het op 31 december 2017 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 2017.

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

Voor de DigiD-aansluitnummers 999749 en 1000313 wordt niet aan alle geselecteerde normen voldaan.

Deze normen betreffen:

B-05 Attentiepunten:

- Evaluatie dienstverlening structureel vastleggen.
- Ondertekend actueel contract
- Ondertekende SLA met leverancier Kodision opvragen
- Ondertekende Bewerkingsovereenkomst leverancier Kodision

U/TV01 Attentiepunt:

- 2 maal per jaar controle uitvoeren op uitgegeven accounts. Alsmede verslag van bevindingen en opvolging hiervan.

U/NW.06 voldoet niet:
Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Actie bij Dimpact.

De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.

Er zijn 2 vertrouwelijke stukken bijgesloten die niet bestemd zijn om openbaar te maken. Het betreft 2 technische documenten die bestemd zijn voor de toezichthouder Logius en is conform VNG afspraken toegevoegd als separaat document behorende bij de collegeverklaring. Er is hierbij sprake van een Netwerkplan (IP-nummerplan) en Architectuurplaat, waarmee hackers gerichte aanvallen kunnen uitvoeren op de gemeentelijke ICT-infrastructuur.

Dit betreft vertrouwelijke bedrijfs- en fabricagegegevens die door personen of bedrijven aan de overheid zijn meegedeeld. Dit is een uitzonderingsgrond (artikel 10 uit de Wob).

Beoogd resultaat

Met ENSIA verantwoorden we ons gemeentebreed over informatieveiligheid. Dit voeren wij uit door middel van een zelfevaluatie. Suwinet en DigiD zijn in dit eerste jaar getoetst met een IT audit. De resultaten van deze IT audit worden ook gebruikt voor verantwoording aan het Rijk.

Kader

VNG-resolutie "Infomatieveiligheid randvoorwaarde voor de professionale gemeente" uit 2013

Argumenten voor en tegen

voor:

-transparant verantwoording afleggen

-voldoen aan de BIG

Extern draagvlak (partners)

Afgestemd in DOWR-verband

Financiële consequenties

nvt

Aanpak/uitvoering

De Collegeverklaring wordt gezamenlijk met het Assurance rapport meegenomen als bijlage bij de rapportage over informatieveiligheid in het jaarverslag aan de gemeenteraad.

Collegeverklaring gemeente Deventer ENSIA

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet
Het college van burgemeester en wethouders van de gemeente Deventer 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 Grootschalige 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 aansluitnummers 61667 en 1000305 en Suwinet. 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[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA[3] voor de selectie van normen). Opzet betekent dat alles netjes gedocumenteerd is. Bestaan betekent dat alles conform de documentatie aanwezig is. De werking wordt naar verwachting in toekomstige jaren getoetst. Werking betekent dat alles werkt zoals het zou moeten werken.

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.

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) en Suwinet (bijlage 2 Suwinet) geïnformeerd over de afwijkingen van de normen.

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

Voor de DigiD-aansluitnummers 61667 en 1000305 wordt niet aan alle geselecteerde normen voldaan.

Deze normen betreffen:

B-05 Attentiepunten:
- Evaluatie dienstverlening structureel vastleggen.
- Ondertekend actueel contract
- Ondertekende SLA met leverancier Kodision opvragen
- Ondertekende Bewerkingsovereenkomst leverancier Kodision

U/TV01 Attentiepunt:
- 2 maal per jaar controle uitvoeren op uitgegeven accounts. Alsmede verslag van bevindingen en opvolging hiervan.

U/NW.06 voldoet niet:
Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Actie bij Dimpact.

De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.

Deventer, 25 april 2018

Burgemeester en wethouders van de gemeente Deventer,

de secretaris
Marcel Kossen
College van B en W gemeente

de burgemeester
Andries Heidema

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/

Bijlage 1 DigiD

Rapportage DigiD Assessment - ENSIA 2017

Aansluiting nr. 61667

Vraag	Antwoord
Vraag 1: Bent u aansluithouder van DigiD aansluitingen?	Ja
Vraag 2: Hoeveel assessmentplichtige DigiD aansluitingen heeft u?	2

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting Vul het Logius aansluitnummer in:	61667
Naam DigiD aansluiting Vul de aansluitnaam in van de aansluiting:	Gemeente Deventer2
Externe infrastructuur-leverancier Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Ja
Naam leveranciers Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	Kodision Hosting
TPM datum Voer hier de datum in van het TPM rapport.	13-10-2017
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.	Kodision
TPM datum Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	13-10-2017
TPM kenmerk Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	AAS2017-240
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	De TPM’s worden middels de ENSIA tool aangeboden aan Logius.
SaaS-leverancier Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier Geef de naam op van de SaaS-leverancier.	Hosting
TPM datum Voer hier de datum in van het TPM rapport.	13-10-2017
TPM kenmerk Voer hier het kenmerk in van het TPM rapport.	AAS2017-240

Bij SaaS-leverancier: U kunt de TPM's hier uploaden	De TPM’s worden middels de ENSIA tool aangeboden aan Logius.
TPM aanwezigheid Leveren alle leveranciers een TPM op?	Nee
Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	Nee, de TPM 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
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
Externe auditor bedrijf Vul de namen in van het bedrijf van de externe auditors:	Accoris Audit Services BV
Externe auditor Vul de namen in van de externe auditors:	PCM Holierhoek RE RA
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?	Geen opmerkingen.

Bijlage vertrouwelijk:
Het Object van onderzoek is een technisch document wat bestemd is voor de toezichthouder Logius en is conform VNG afspraken toegevoegd als separaat document behorende bij deze collegeverklaring. Er is hierbij sprake van een Netwerkplan (IP-nummerplan) en Architectuurplaat, deze zijn vertrouwelijk en daarmee uitgesloten als publieke informatie (artikel 10 uit de Wob).

Totaaloverzicht getoetste normen ICT-beveiligingsassessment DiGiD-aansluiting van Gemeente Deventer.

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 61667.

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 TPM-rapportage van Kodision, AAS2017-240, 13-10-2017 ondertekend door de heer RCM Holierhoek RE RA.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage Kodision,AAS2017-240, 13-10-2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Het komt echter voor dat in een TPM een afwijkende lijst (User considerations Governance) wordt aangegeven. In dat geval moet dit tot uitdrukking komen in deze bijlage.

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet / niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet /niet van toepassing	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	AAS2017-240 (TPM[1])	Ja	Voldoet niet	Verbeterplan
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	Voldoet	AAS2017-240 (TPM)	Ja	Voldoet niet	Verbeterplan

[1] Third party mededeling afgegeven door de hostpartij.

	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.	Voldoet	AAS2017-240 (TPM)	Ja	Voldoet	Rapportnummer volgt na college-verklaring.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	AAS2017-240 (TPM)	Ja	Voldoet	Rapportnummer volgt na college-verklaring.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/PW.	De webserver is	Voldoet	AAS2017-	Nee	nvt	nvt

03	ingericht volgens een configuratie-baseline.		240 (TPM)			
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.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
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.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt

C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
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.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en	Voldoet	AAS2017-240 (TPM)	Ja	Voldoet	Rapportnummer volgt na college-verklaring.

	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.	Voldoet	AAS2017-240 (TPM)	Nee	nvt	nvt

Vragen vooraf

Vraag	Antwoord
Vraag 1: Bent u aansluithouder van DigiD aansluitingen?	Ja
Vraag 2: Hoeveel assessmentplichtige DigiD aansluitingen heeft u?	2

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting Vul het Logius aansluitnummer in:	1000305
Naam DigiD aansluiting Vul de aansluitnaam in van de aansluiting:	Digitaal Loket Gemeente Deventer
Externe infrastructuur-leverancier Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Ja
Naam leveranciers Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	Dimpact Atos SSC Twente
TPM datum Voer hier de datum in van het TPM rapport.	14-12-2017
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.	Atos
TPM datum Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	14-12-2017
TPM kenmerk Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	Referentie 2017.268
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	De TPM’s worden middels de ENSIA tool aangeboden aan Logius.
SaaS-leverancier Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier Geef de naam op van de SaaS-leverancier.	SSC Twente
TPM datum Voer hier de datum in van het TPM rapport.	14-12-2017
TPM kenmerk Voer hier het kenmerk in van het TPM rapport.	Referentie 2017.268

Bij SaaS-leverancier: U kunt de TPM's hier uploaden	De TPM’s worden middels de ENSIA tool aangeboden aan Logius.
TPM aanwezigheid Leveren alle leveranciers een TPM op?	Nee
Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	Nee, de TPM 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
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
Externe auditor bedrijf Vul de namen in van het bedrijf van de externe auditors:	Referentie 2017.268
Externe auditor Vul de namen in van de externe auditors:	Drs. W. Schiphorst RE
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Ja. Norm U.TV07 voldoet niet. Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Actie bij Dimpact.
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	U.TV07. Zie document Referentie 2017.268

Bijlage vertrouwelijk:
Het Object van onderzoek is een technisch document wat bestemd is voor de toezichthouder Logius en is conform VNG afspraken toegevoegd als separaat document behorende bij deze collegeverklaring. Er is hierbij sprake van een Netwerkplan (IP-nummerplan) en Architectuurplaat, deze zijn vertrouwelijk en daarmee uitgesloten als publieke informatie (artikel 10 uit de Wob).

Totaaloverzicht getoetste normen ICT-beveiligingsassessment DiGiD-aansluiting van Gemeente Deventer.

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 1000305.

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, U/NW.06. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van TPM-rapportage van Dimpact, referentie/2017.268, 14-12-2017 ondertekend door de heer drs. W. Schiphorst RE.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van TPM-rapportage van Dimpact referentie/2017.268, 14-12-2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Het komt echter voor dat in een TPM een afwijkende lijst (User considerations Governance) wordt aangegeven. In dat geval moet dit tot uitdrukking komen in deze bijlage.

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet / niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet /niet van toepassing	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	Referentie 2017.268 (TPM)[2]	Ja	Voldoet niet	Verbeterplan
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	Voldoet	Referentie 2017.268 (TPM)	Ja	Voldoet niet	Verbeterplan

[2] Third party mededeling uitgegeven door hostpartij.

	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.	Voldoet	Referentie 2017.268 (TPM)	Ja	Voldoet	Rapportnummer volgt na college-verklaring.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	Referentie 2017.268 (TPM)	Ja	Voldoet	Rapportnummer volgt na college-verklaring.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/PW.	De webserver is	Voldoet	Referentie	nee	nvt	nvt

03	ingericht volgens een configuratie-baseline.		2017.268 (TPM)			
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.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet niet	Referentie 2017.268 (TPM)	Ligt als vraag bij Dimpact.	nvt	nvt
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.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	Referentie 2017.268 (TPM)	Ja	Voldoet niet	Verbeterplan

C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
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.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en	Voldoet	Referentie 2017.268 (TPM)	Ja	Voldoet	Rapportnummer. volgt na college-verklaring.

	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.	Voldoet	Referentie 2017.268 (TPM)	nee	nvt	nvt

Bijlage 2 Suwinet

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

Naast het gebruik van Suwinet voor wettelijke SUWI-taken heeft de gemeente voor de volgende taken (een) overeenkomst(en) afgesloten conform Regeling Suwi bijlage 3 Aansluitprotocol GeVS voor het gebruik van Suwinet als niet-SUWI-partij:

- Gerechtsdeurwaarder (voert deze taak ook voor gemeente Olst-Wijhe uit)
- Burgerzaken

Het gebruik van Suwinet als niet-SUWI-partij is onderdeel van de Collegeverklaring.[3]
De gemeente Deventer heeft geen taken uitbesteed aan externe organisaties.

Afwijkingen van de normen
Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

- nvt

Ingeval niet-SUWI-taken: Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de niet-SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

- nvt

[3] Toelichting: zie www.vng.nl/files/vng/2017-08_vng_factsheet_suwinet_voor_gemeenten_v1.pdf

Totaaloverzicht geselecteerde normen

Norm	Beschrijving norm	Toelichting norm	Zelf evaluatie oordeel	Externe audit oordeel
B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet.	VOLDOET	VOLDOET
B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	Het voorkomen dat risico's optreden als gevolg van het ontbreken van coördinatie op het gebied van activiteiten aangaande de bescherming van de eigen delen van Suwinet.	VOLDOET	VOLDOET
B.05	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat.	VOLDOET	VOLDOET
U.02	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.	Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken.	VOLDOET	VOLDOET
U.03	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten.	VOLDOET	VOLDOET
U.11	De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet.	Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten.	VOLDOET	VOLDOET

C.01	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën.	Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau	VOLDOET	VOLDOET
C.04	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).	Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden.	VOLDOET	VOLDOET
C.05	Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles.	Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen.	VOLDOET	VOLDOET
C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen).	Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie.	VOLDOET	VOLDOET
C.07	De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.	Bewerkstelligen dat zich geen leemtes in de beveiliging van IAA (Identificatie, Authenticatie en Autorisatie) mechanismen voordoen.	VOLDOET	VOLDOET