

Afdeling	: D&I - Dienstverlening & Informatie	B&W-voorstel: DJ-654650
Naam opsteller voorstel	: Harrie van Helvoort (0495-575571)	Zaaknummer: 643683
Portefeuillehouder	: A.A.M.M. (Jos) Heijmans	Publicatie: Openbaar

Onderwerp

Collegeverklaring Eenduidige Normatiek & Single Information Audit (ENSIA) 2018

Voorstel

1. Kennis te nemen van de vaststelling dat per 31 maart 2019 de beheersmaatregelen van de Digid aansluitingen voldoen aan de normen, waarbij opgemerkt wordt dat er een verbeterplan is vastgesteld t.a.v. DigiD Digitaal Loket Gemeente Weert (bijlage 7).
2. De Collegeverklaring Eenduidige Normatiek en Single Information Audit (ENSIA) 2018, waarin dit is vastgelegd, te ondertekenen.

Inleiding

Gemeenten moeten door middel van een audit/zelf-evaluatie kunnen aantonen dat de 'systemen' die digitaal in verbinding staan met de buitenwereld, voldoen aan bepaalde veiligheidsnormen. Voor het jaar 2018 geldt dit voor de DigiD aansluitingen van de gemeente en het elektronisch berichtenverkeer tussen Suwinet en haar afnemers. De ENSIA methodiek wordt hiervoor gehanteerd.

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

ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid, gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG).

ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken, de VNG, gemeenten, het ministerie van Sociale Zaken & Werkgelegenheid en het ministerie van Infrastructuur & Milieu.

Vanaf 2017 is het vanuit ENSIA verplicht om tijdens de jaarlijkse ENSIA audit (9 april 2019) een verklaring te hebben van het college waarin vastgelegd is wat de status is van de maatregelen t.a.v. informatiebeveiliging en privacy.

Beoogd effect/doel

Weert, 26 maart 2019	S		B	W	W	W	W	W
				GG	MvdH	TG	WvE	PS
		akkoord						
		bespreken						
Soort besluit: Besluit college		02.04.2019						

In te vullen door het B&W secretariaat:

- Akkoord
 Akkoord met tekstuele aanpassing door portefeuillehouder
 Anders, nl.:

- Niet akkoord
 Gewijzigde versie

- A-stuk
 B-stuk
 C-stuk

Beslissing d.d.: 02.04.2019

Nummer: 2

De secretaris,

Aantonen bij de ENSIA Audit dat de gemeente in control is t.a.v. informatiebeveiliging en Privacy.

Argumenten

Met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. Deze baseline is nu de kern van de verantwoording over informatieveiligheid aan de gemeenteraad.

Kanttekeningen en risico's

De Collegeverklaring maakt onderdeel uit van de jaarlijkse ENSIA Audit.

Financiële, personele en juridische gevolgen

Geen.

Uitvoering/evaluatie

De horizontale verantwoording bestaat uit de zelfevaluatie (zie bijlagen), een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag.

Communicatie/participatie

De gemeenteraad informeren via de TILS-lijst

Overleg gevoerd met

Intern:

J. Steijvers (DigiD Beheerder Publiekszaken),
R. van Leeuwen (DigiD beheerder WIZ),
L. Kroot (DigiD beheerder Enable-U),
T. Willems (SUWI Security Coördinator)

Extern:

Arjan Hassing (IT Auditor; 3Angles)

Bijlagen:

1. Rapportage-DigiD-Assessment-2018-Weert-1
2. Rapportage-DigiD-Assessment-2018-Weert-2
3. Rapportage-DigiD-Assessment-2018-Weert-3
4. Rapportage-DigiD-Assessment-2018-Weert-4
5. Bijlage Suwinet Collegeverklaring ENSIA 2018
6. Collegeverklaring Eenduidige Normatiek & Single Information Audit (ENSIA) 2018
7. Verbeterplan DigiD Digitaal Loket Gemeente Weert
8. Verantwoordingsrapportage BAG 2018
9. Verantwoordingsrapportage BGT 2018
10. Verantwoordingsrapportage BRO 2018

Collegeverklaring ENSIA 2018 inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Weert

Gemeentelijk kenmerk collegeverklaring ENSIA:	ENSIA2018Weert06
Naam auditfirma: 3angles B.V.	
Naam auditor: A. Hassing	

Doel en achtergrond verklaring

Het college van burgemeester en wethouders van de gemeente Weert geeft met deze verklaring aan in hoeverre de gemeente Weert 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), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige 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 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 Weert betreft dit in 2018 DigiD en Suwinet. De verklaring omvat het op 31 december 2018 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 2018.

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 ENSIA2018Weert01) 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[s] dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring betrekking op de beheersingsmaatregelen 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 tot en met 4:

DigiD met kenmerk ENSIA2018Weert01 tot en met 04) en Suwinet (bijlage 5: Suwinet met kenmerk ENSIA2018Weert05) 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 tot en met 4: DigiD met kenmerk ENSIA2018Weert01 t.m. 04) en voor Suwinet (bijlage 5: Suwinet met kenmerk ENSIA2018Weert05) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Weert op 31 december 2018 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Per 31 maart 2019 voldoen de beoogde en ingerichte beheersingsmaatregelen in opzet en bestaan voor DigiD 1002411. Voor de uitzonderingen is een verbeterplan samengesteld (bijlage: Verbeterplan DigiD Digitaal Loket Gemeente Weert).

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 571063	Ja	Niet van toepassing
DigiD 1001325	Ja	Niet van toepassing
DigiD 1002287	Ja	Niet van toepassing
DigiD 1002411	Nee	Ja
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

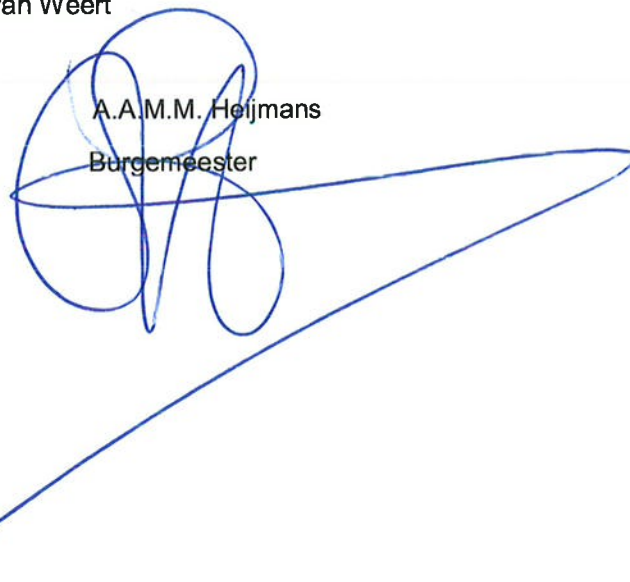
Weert, 2-4 2019

Burgemeester en Wethouders van Weert

G. Brinkman
Gemeentesecretaris

k.c.


A.A.M.M. Heijmans
Burgemeester





W-31368



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

> Retouradres Antwoordnummer 16073, 2501 VE Den Haag

Gemeente Weert
College van Burgemeester en Wethouders
T.a.v. de heer M. van Dijk
Postbus 950
6000 AZ Weert

Logius
Toegangsdiensten

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag
Antwoordnummer 16073
2501 VE Den Haag
www.logius.nl

Kenmerk
Logius/2019/U000111

Datum: 14 februari 2019
Betreft: ICT-beveiligingsassessments DigiD

Geachte heer Van Dijk,

Hartelijk dank voor het indienen van uw auditrapportage voor het ICT-beveiligingsassessment DigiD, betreffende de aansluiting '1002411 - Gemeente Weert- Digitaal Loket'.

Op basis van uw verbeterrapport stelt Logius vast dat u een aantal bevindingen heeft opgelost. In de bijlage wordt aangegeven voor welke normen dit geldt. Voor de overige openstaande normen uit het assessment heeft u nog geen verbeterrapport ingeleverd. Deze normen zijn in de bijlage voorzien van de door Logius verwachte oplevertermijn.

U dient een Register EDP auditor te laten vaststellen dat u alsnog voldoet aan alle normen. Hiervan stuurt u een bericht aan Logius, binnen de termijn die per norm is aangegeven in de bijlage bij deze brief.

Heeft u nog vragen en/of opmerkingen, dan kunt u contact opnemen met ons Servicecentrum. Dit is bereikbaar op telefoonnummer 0900 - 555 4 555 en per e-mail op servicecentrum@logius.nl. Het Servicecentrum is geopend op werkdagen van 8.00 tot 17.00.

Wilt u algemene informatie over DigiD assessments ontvangen per e-mail (2 á 3 keer per jaar), dan kunt u zich hiervoor aanmelden via het algemeen contactformulier op www.logius.nl/contact/. U kunt deze link delen binnen uw organisatie.

Hoogachtend,

De minister van Binnenlandse Zaken en Koninkrijksrelaties, voor deze,

Jorik van 't Hof
Projectleider ICT-beveiligingsassessments DigiD

Bijlage - overwegingen

Op basis van uw verbeterrapport heeft u een aantal punten opgelost, deze zijn in onderstaande tabel opgenomen met daarbij de status "opgelost". Daarnaast stelt Logius vast dat u nog niet alle van de onderstaande normen van de ICT-beveiligingsassessments DigiD heeft opgelost. Logius vraagt u deze alsnog op te lossen voor de aangegeven opleverdatum.

Datum

14 februari 2019

Ons Kenmerk

Logius/2019/U000111

Norm naam / Beveiligingsrichtlijn

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 de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.

Opleverdatum:

Te voldoen voor 15-05-2019

Norm naam / Beveiligingsrichtlijn

U/PW.03 De webserver is ingericht volgens een configuratie-baseline.

Opleverdatum:

Te voldoen voor 15-05-2019

Norm naam / Beveiligingsrichtlijn

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.

Opleverdatum:

Te voldoen voor 15-05-2019

Norm naam / Beveiligingsrichtlijn

U/PW.07 Voor het configureren van platformen is een hardeningrichtlijn beschikbaar.

Opleverdatum:

Te voldoen voor 15-03-2019

Norm naam / Beveiligingsrichtlijn

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.

Opleverdatum:

Opgelost per 13-02-2019

Bijlage - overwegingen

Op basis van uw verbeterrapport heeft u een aantal punten opgelost, deze zijn in onderstaande tabel opgenomen met daarbij de status "opgelost". Daarnaast stelt Logius vast dat u nog niet alle van de onderstaande normen van de ICT-beveiligingsassessments DigiD heeft opgelost. Logius vraagt u deze alsnog op te lossen voor de aangegeven opleverdatum.

Datum

14 februari 2019

Ons Kenmerk

Logius/2019/U000111

Norm naam / Beveiligingsrichtlijn

U/NW.05 Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.

Opleverdatum:

Te voldoen voor 15-05-2019

Norm naam / Beveiligingsrichtlijn

U/NW.06 Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.

Opleverdatum:

Te voldoen voor 15-03-2019

Norm naam / Beveiligingsrichtlijn

C.06 In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

Opleverdatum:

Te voldoen voor 15-05-2019

Norm naam / Beveiligingsrichtlijn

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.

Opleverdatum:

Te voldoen voor 15-05-2019

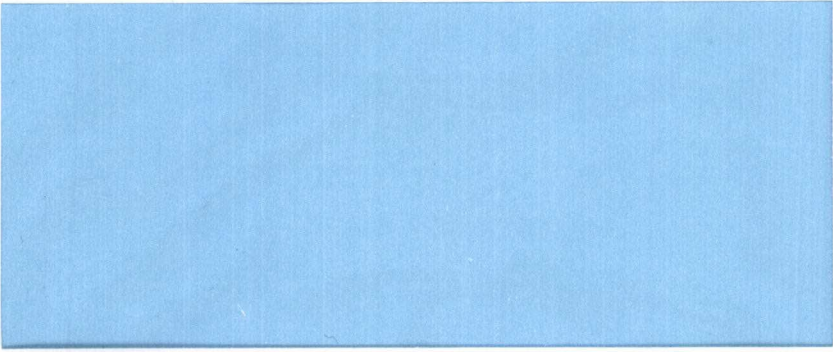
Norm naam / Beveiligingsrichtlijn

C.09 Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICTvoorzieningen.

Opleverdatum:

Te voldoen voor 15-03-2019

PostNL
Port betaald
Port Payé
Pays-Bas



RX3CC #7621X0X#00#0000#