Gemeente Bergen op Zoom

Aan de leden en burgerleden
van de gemeenteraad
van Bergen op Zoom

U22-003437

- 7 APR. 2022

Uw kenmerk		Ons kenmerk		Datum	
Uw brief		Beh. door		Doorkiesnr.	
Onderwerp:	ENSIA 2021 Verantwoording informatieveiligheid	Cluster	Control & Audits,	Bijlage(n)	1

Beste leden en burgerleden,

Het veilig omgaan met informatie komt – terecht – steeds hoger op ieders agenda. Dat blijkt onder meer uit het feit dat het college sinds 2017 verantwoording over informatiebeveiliging aflegt aan de gemeenteraad. Dat gebeurt middels de Collegeverklaring. VNG en de Ministeries hebben hiervoor vanaf 2017 de methode ENSIA voorgeschreven (Eenduidige Normatiek Single Information Audit).

In deze brief lichten wij de totstandkoming en de resultaten van de bijgevoegde Collegeverklaring toe.

Zelfevaluatie

In de tweede helft van 2021 is een zelfevaluatie door lijnverantwoordelijken van de ambtelijke organisatie uitgevoerd. Deze heeft betrekking op de normenkaders van BPR, PUN, BIO, BAG, BGT, BRO, WOZ, DigiD en Suwinet. [1]

Assurance

Een onafhankelijke auditor heeft de uitvoering van de zelfevaluaties DigiD en Suwinet getoetst en vastgesteld dat deze een goed beeld geven van de werkelijkheid. Dit heeft hij bevestigd is het Assurance Report.

Verantwoorden

Middels deze brief en de Collegeverklaring legt het college verantwoording af aan de raad.

[1] BRP = Basisregistratie Personen; PUN = Paspoortuitvoeringsregeling Nederland; BIO = Baseline Informatieveiligheid Overheid; BAG = Basisregistraties Adressen en Gebouwen; BGT = Basisregistratie Grootschalige Topografie; BRO = Basisregistratie Ondergrond; WOZ=Wet Onroerende Zaken; DigID = Digitale Identiteit; Suwinet = Infrastructuur voor Structuur Werk en Inkomen

Jacob Obrechtlaan 4
4611 AR Bergen op Zoom
Contact: www.bergenopzoom.nl

Postbus 35
4600 AA Bergen op Zoom
I www.bergenopzoom.nl

T 140164
F (0164) 24 53 56
KvK 20169091

B nv BNG rek. nr. 28.50.00.942
B IBAN: NL41BNGH 0285000942
B BIC: BNGHNL2G

Bergen op Zoom, gemeente op de Brabantse Wal

Verbeteren

Wanneer niet geheel aan de normen wordt voldaan, dan wordt ook een verbeterplan opgesteld. Vanuit het DigiD-normenkader worden aan elke aansluiting (we hebben er drie) 20 eisen gesteld; we voldoen aan alle eisen.

- Digid iBurgerzaken: 20 van 20 voldoen (100%)
- Digid iZaaksysteem: 20 van 20 voldoen (100%)
- Digid Snelbalie: 20 van 20 voldoen (100%)

We stellen vast dat het doorvoeren van diverse verbeteringen door onze leveranciers én de eigen organisatie er de afgelopen jaren toe hebben geleid dat we aan alle gestelde normen voldoen.

- Suwinet: 9 van 17 voldoen (53%)

ISD Brabantse Wal is het enige organisatie-onderdeel dat gebruik maakt van Suwinet. Vanuit het Suwinet-normenkader worden 17 eisen gesteld; ISD Brabantse Wal voldoet niet aan de volgende eisen:

5.1.1 Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5.1.2 Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
9.2.1 Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9.2.2 Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9.2.5 Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9.2.6 De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
12.1.1 Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
18.1.4 Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

ISD Brabantse Wal heeft een verbeterplan opgesteld om alsnog aan de normen te voldoen. Daarin heeft zij aangegeven wie, wanneer, welke verbetering door voert, zodat ook aan de resterende eisen wordt voldaan. Het verantwoordelijk management heeft zich aan het verbeterplan gecommitteerd. Audits helpen ons om risico's meer gedetailleerd in beeld te krijgen zodat we onze beheersmaatregelen daarop kunnen afstemmen.

Gemeente Bergen op Zoom

Zelf-evaluatie op de Baseline Informatiebeveiliging Overheid (BIO)

Buiten de scope van de College-verklaring – maar binnen de scope van ENSIA – is een zelf-evaluatie op het BIO normenkader uitgevoerd.

Gelet op de grootste risico's die wij lopen ten aanzien van onze veilige informatieverwerking zijn voor 2022 belangrijke verbetervoorstellen in het zogenoemde IB Plan opgenomen:

- Versterken logische toegangsbeveiliging
- Basis op orde (waaronder incident management, wijzigingsbeheer en patch- en vulnerability-management)
- Bedrijfscontinuïteit
- *Disaster recovery*

Van veel technische beveiligingsmaatregelen heeft de ICT Service Provider (2021: ICT West-Brabant West) aangegeven dat deze zijn geïmplementeerd maar kon dat niet altijd worden aangetoond met bewijs van opzet en werking. Reeds voor de overstap naar Sogeti als ICT Service Provider zijn zekerheden verkregen over opzet en werking van alle relevante technische beveiligingsmaatregelen, onder meer door overlegging van het ISO 27001 certificaat en Verklaring van Toepasselijkheid. Hoewel deze overstap op zichzelf geen verbetermaatregel is, verwachten we wel dat de zelfevaluatie op de BIO over 2022 hierdoor een aanmerkelijk positiever resultaat geeft.

Inzage

Vanwege het technische karakter van de audit-documenten, stellen wij u in de gelegenheid om deze bij de Chief Information Security Officer in te zien. U kunt met de Griffier een afspraak daartoe maken.

Met vriendelijke groet,
het college van burgemeester en wethouders van Bergen op Zoom,

secretaris

Dhr. mr. drs. ing. M. van Vliet

burgemeester

Dhr. dr. F.A. Petter

Gemeente Bergen op Zoom

Informatiebeveiliging

ENSIA 2021

Collegeverklaring

Informatieveiligheid
DIGID en Suwinet

Gemeente Bergen op Zoom



Versie:	Definitief	Datum: 3 april 2022	
Auteur:	JLGM Baaten CISM | CISO		
Documentkenmerk:	B22-000937		
Voor akkoord:	Dhr. mr. drs. ing. M. van Vliet Gemeentesecretaris	Dhr. dr. F.A. Petter Burgemeester	

1 Doel en achtergrond verklaring

Met deze verklaring geven wij, het College van Burgemeester en Wethouders van de gemeente Bergen op Zoom, aan in welke mate de gemeente Bergen op Zoom voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet.
Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[1] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.
De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

2 Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2021.
De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen (en eventuele afwijkingen) en waar deze belegd zijn, is opgenomen in de bijlagen:

- Bijlage 1 DigiD met kenmerk B22-000938
- Bijlage 2 Suwinet met kenmerk B22-000939

3 Verklaring college

Het college verklaart dat bij de gemeente Bergen op Zoom op 31 december 2021de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD.
Het college verklaart dat voor Suwinet niet aan alle normen wordt voldaan. Wij hebben een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

[1] *ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), 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) en de Wet Onroerende Zaken (WOZ).*

4 Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD (1) 53882 iZaaksysteem	Ja	Niet van toepassing
DigiD (2) 1001253 Snelbalie	Ja	Niet van toepassing
DigiD (3) 1001029 iBurgerzaken	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	nvt	nvt

Bergen op Zoom, 3 april 2022
het college van burgemeester en wethouders van Bergen op Zoom,

secretaris

Dhr. mr. drs. ing. M. van Vliet

burgemeester

Dhr. dr. F.A. Petter

Gemeente Bergen op Zoom

Informatiebeveiliging

ENSIA 2021
Collegeverklaring

Bijlage 1 DigID



Versie:	Definitief	Datum: 3 april 2022	
Auteur:	JLGM Baaten CISM | CISO		
Documentkenmerk:	B22-000938		
Voor akkoord:	Dhr. mr. drs. ing. M. van Vliet Gemeentesecretaris	Dhr. dr. F.A. Petter Burgemeester	

(1) DigID 53882 Bergen op Zoom (iZaaksuite WebNext)

DigiD-aansluiting

Naam: Bergen op Zoom (iZaaksuite 'WebNext')
Aansluitnummer: 53882

Bergen op Zoom biedt de volgende functionaliteit aan waarvoor deze DigiD-aansluiting voor authenticatie wordt gebruikt:

iZaaksuite / WebNext biedt de mogelijkheid om digitale diensten online aan te vragen bij de gemeente Bergen op Zoom via webformulieren

Deze functionaliteit wordt geboden door de volgende webapplicatie:

iZaaksuite / WebNext

Deze applicatie betreft een geheel standaard-pakket en wordt onderhouden door Pink Roccade Local Government.

Deze applicatie is extern benaderbaar via de volgende URL: izaaksuite.bergenopzoom.nl/

DigiD-aansluiting iZaaksuite / Webnext bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Pink Roccade Local Government in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting iZaaksuite / WebNext. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Bergen op Zoom heeft een deel van de DigiD web-omgeving uitbesteed aan Pink Roccade Local Government. 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 serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM van de leverancier:

ICT-leverancier	
Naam serviceorganisatie:	Pink Roccade Local Government
Referentie/rapportnummer:	20211119 DBA-PRLG DigiD WebNext-Bergen op Zoom
Afgiftedatum:	19 november 2021
Naam RE-auditor:	Duijnborgh Audit B.V.
Ondertekend door RE-auditor:	Frank Kossen RE; Laurens van Thiel CISA CISSP; Drs. Mohamed El Aarbaoui RE

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 IAS1286/21. Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de leverancier.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier	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/Privacybevordering	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

(2) DigID 1001253 Snelbalie Burgervariant

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting

Naam:	Snelbalie Burgervariant
Aansluitnummer:	1001253

Bergen op Zoom biedt de volgende functionaliteit aan waarvoor deze DigiD-aansluiting voor authenticatie wordt gebruikt:

Snelbalie Burgervariant is een frontoffice applicatie waarmee burgers zorgaanvragen snel, correct en eenduidig af kunnen handelen. Snelbalie Burgervariant produceert op basis van de aanvraag direct een beschikking die ter plekke geprint kan worden.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

eDiensten voor Aanvragen / Snelbalie Burgervariant

Deze applicatie betreft een geheel standaard-pakket en wordt onderhouden door Centric.

Deze applicatie is extern benaderbaar via de volgende URL: snelbalie.bergenopzoom.nl.

DigiD-aansluiting Snelbalie bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Centric in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Snelbalie. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Bergen op Zoom heeft een deel van de DigiD web-omgeving uitbesteed aan Centric. 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 serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM van de leverancier:

ICT-leverancier	
Naam serviceorganisatie:	Centric
Referentie/rapportnummer:	REQ6122941NKjb_C
Afgiftedatum:	28 oktober 2021
Naam RE-auditor:	Ernst & Young Accountants LLP
Ondertekend door RE-auditor:	Peter Kornelisse RE, Ernst & Young Accountants LLP

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 IAS1286/21. Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier	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/Privacybevordering	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

(3) DigID 1001029 iBurgerzaken

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting

Naam:	Gemeente Bergen op Zoom - Burgerzaken
Aansluitnummer:	1001029

Bergen op Zoom biedt de volgende functionaliteit aan waarvoor deze DigiD-aansluiting voor authenticatie wordt gebruikt:

iBurgerzaken ondersteunt de burgers bij het aanvragen van diverse online-diensten, zoals het aanvragen van een akte of afschrift burgerlijke stand, het doen van geboorteaangifte, het doen van aangifte van verhuizing of vestiging in de gemeente etc.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

iBurgerzaken

Deze applicatie betreft een geheel standaard-pakket en wordt onderhouden door Pink Roccade Local Government.

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

DigiD-aansluiting iBurgerzaken bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Pink Roccade Local Government in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting iBurgerzaken. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Bergen op Zoom heeft een deel van de DigiD web-omgeving uitbesteed aan Pink Roccade Local Government. 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 serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM van de leverancier:

ICT-leverancier	
Naam serviceorganisatie:	Pink Roccade Local Government
Referentie/rapportnummer:	20211026DBA-PRLG
Afgiftedatum:	26 oktober 2021
Naam RE-auditor:	Duijnborgh Audit B.V.
Ondertekend door RE-auditor:	Frank Kossen RE; Laurens van Thiel CISA CISSP; Drs. Mohamed El Aarbaoui RE

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 IAS1286/21. Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier	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/Privacybevordering	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

== einde document ==

Gemeente Bergen op Zoom

Informatiebeveiliging

ENSIA 2021
Collegeverklaring

Bijlage 2 Suwinet



Versie:	Definitief	Datum: 3 april 2022	
Auteur:	JLGM Baaten CISM | CISO		
Documentkenmerk:	B22-000939		
Voor akkoord:	Dhr. mr. drs. ing. M. van Vliet Gemeentesecretaris	Dhr. dr. F.A. Petter Burgemeester	

1 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2021 van de gemeente Bergen op Zoom. Onderwerp van de verklaring is het gebruik van Suwinet. Deze verklaring heeft betrekking op de Verantwoordingsrichtlijn GeVS 2020 welke is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO).

Onderwerp van de verklaring is het gebruik van Suwinet. Suwinet wordt in samenwerkingsverbanden gebruikt. Het gebruik van Suwinet door samenwerkingsverbanden valt binnen de reikwijdte van de verklaring.

Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. Bergen op Zoom heeft een deel van de Suwinet taken uitbesteed aan ISD Brabantse Wal. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm. De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling (TPM) van onze serviceorganisatie.

Leverancier 1	
Naam serviceorganisatie:	ISD Brabantse Wal
Referentie/rapportnummer:	IAS1286_21
Afgiftedatum	9 december 2021
Naam RE-auditor:	Ronald Driehuis en Daan Koot
Ondertekend door RE-auditor:	ja

2 Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM
Participatiewet (Pw)	ISD Brabantse Wal	IAS1286_21
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	ISD Brabantse Wal	IAS1286_21
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	ISD Brabantse Wal	IAS1286_21

3 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	Niet van toepassing
Adresonderzoek door Burgerzaken	Niet van toepassing

4 Naleving BIO-maatregelen

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2021 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2020:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
ISD Brabantse Wal	PW, IOAW, IOAZ	5.1.1 Actueel IB Beleid ISDBW	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	5.1.2 Actueel IB Beleid ISDBW	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	9.1.2 Registratie- en afmeldprocedure irt beheer toegangsrechten	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	9.2.2 Gebruikerstoegangs-verleningsprocedure irt toegangsrechten	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	9.2.5 Regelmatige beoordeling toegangsrechten door eigenaar	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	9.2.6 Verwijderen/aanpassen toegangsrechten bij uitdienst of wijzigen rol	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	12.1.1 Documenteren en beschikbaar stellen bedieningsprocedures	Suwinet-Inkijk
ISD Brabantse Wal	PW, IOAW, IOAZ	18.1.4. Waarborgen privacy	Suwinet-Inkijk

== einde document ==