Gemeentelijk kenmerk collegeverklaring ENSIA:	Zaaknr 1168162 / Docnr 3561287

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Bloemendaal

Gemeentelijk kenmerk collegeverklaring ENSIA: Zaaknr 1168162 / Docnr 3561287

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Bloemendaal

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate Gemeente Bloemendaal 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.

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 2022.

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: Zaaknr 1168162 / Docnr 3561288.
- Bijlage 2 Suwinet met kenmerk: Zaaknr 1168162 / Docnr 3561289.

Verklaring college

Het college verklaart dat voor DigiD niet aan alle normen wordt voldaan. Wij hebben een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord. Het college verklaart dat bij gemeente Bloemendaal op 31 december 2022 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake Suwinet.

---

[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), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet) en de Wet Onroerende Zaken (WOZ).

Gemeentelijk kenmerk collegeverklaring ENSIA:	Zaaknr 1168162 / Docnr 3561287

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1003011	Nee	Ja
DigiD 1002551	Ja	Niet van toepassing
DigiD 1002449	Nee	Ja
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Bloemendaal, 11 april 2023

College van B&W gemeente Gemeente Bloemendaal

P. Dubbe	Secretaris	
E. Roest	Burgemeester	

Naam auditfirma:	2-Control BV
Naam auditor:	J. de Klerk RE
Datum:	

Bijlage 1 DigiD - Parkeer Vergunningen Bloemendaal - 1002449

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Parkeer Vergunningen Bloemendaal met aansluitnummer 1002449

Gemeente Bloemendaal biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Parkeer Vergunningen Bloemendaal voor authenticatie wordt gebruikt:

- Parkeervergunningen aanvragen/wijzigen/verlengen

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Citypermit

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Sigmax Law Enforcement BV.

Deze applicatie is extern benaderbaar via het volgende internetadres: parkeren.bloemendaal.nl

DigiD-aansluiting Parkeer Vergunningen Bloemendaal bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Sigmax Law Enforcement BV in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Parkeer Vergunningen Bloemendaal. 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.

Gemeente Bloemendaal heeft een deel van de DigiD web-omgeving uitbesteed aan Sigmax Law Enforcement BV.
Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). 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(s) van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van de leverancier(s):

SaaS-leverancier	
Naam serviceorganisatie:	Sigmax Law Enforcement BV
Referentie/rapportnummer:	TPM 1: 2211R.AH144 TPM 2: N.v.t.
Afgiftedatum:	TPM 1: 18-11-2022 TPM 2: N.v.t.
Naam RE-auditor:	A.J.A. Hassing RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze leverancier(s) 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 2C-2023-460.

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

Gemeentelijk kenmerk bijlage 1 DigiD:	Zaaknr 1168162 / Docnr 3561288

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij SaaS-leverancier	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet niet	Voldoet	Voldoet niet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet

Bijlage 1 DigiD - Gemeente Bloemendaal - 1002551

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Bloemendaal met aansluitnummer 1002551

Gemeente Bloemendaal biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Bloemendaal voor authenticatie wordt gebruikt:

- Verhuizing doorgeven
- Aangifte geboorte / overlijden
- Uittreksel BRP
- Bewijs van in leven zijn
- Akte Burgerlijke Stand
- Aanvraag reisdocument
- Aanvraag rijbewijs

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door PinkRoccade BV.

Deze applicatie is extern benaderbaar via het volgende internetadres: iburgerzaken.bloemendaal.nl

DigiD-aansluiting Gemeente Bloemendaal bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door PinkRoccade BV in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Bloemendaal. 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.

Gemeente Bloemendaal heeft een deel van de DigiD web-omgeving uitbesteed aan PinkRoccade BV. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). 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(s) van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van de leverancier(s):

SaaS-leverancier	
Naam serviceorganisatie:	PinkRoccade BV
Referentie/rapportnummer:	TPM 1: 20221010 DBA-PRLG TPM 2: N.v.t.
Afgiftedatum:	TPM 1: 10-10-2022 TPM 2: N.v.t.
Naam RE-auditor:	F.Kossen RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze leverancier(s) 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 2C-2023-460.

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

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij SaaS-leverancier	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet

Bijlage 1 DigiD - GBKZ digitale loket - 1003011

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting GBKZ digitale loket met aansluitnummer 1003011

Gemeente Bloemendaal biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting GBKZ digitale loket voor authenticatie wordt gebruikt:

- Bezwaar maken tegen verschillende soorten aanslagen
- Kwijtschelding aanvragen
- Automatische incasso regelen

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Het zaaksysteem Mozard

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Mozard BV.

Voor het verifiëren van de identiteit van de gebruiker maakt de DigiD aansluithouder gebruik van de SIAM applicatie van Anoigo.

Deze applicatie is extern benaderbaar via het volgende internetadres: www.eloket.gbkz.nl

DigiD-aansluiting GBKZ digitale loket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door OGD ict-diensten in de vorm van fysieke hosting,

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting GBKZ digitale loket. 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.

Gemeente Bloemendaal heeft een deel van de DigiD web-omgeving uitbesteed aan OGD ict-diensten. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). 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(s) van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM's / assurancerapportages van de leverancier(s):

IT-leverancier	
Naam serviceorganisatie:	OGD ict-diensten
Referentie/rapportnummer:	TPM 1: 2C-2022-435 TPM 2: N.v.t.
Afgiftedatum:	TPM 1: 30-12-2022 TPM 2: N.v.t.
Naam RE-auditor:	J. de Klerk RE
Ondertekend door RE-auditor:	Ja

Applicatieleverancier	
Naam serviceorganisatie:	MOZARD BV
Referentie/rapportnummer:	TPM 1: IAS1040_22_A TPM 2: Nvt
Afgiftedatum:	TPM 1: 02-11-2022 TPM 2: Nvt

Applicatieleverancier	
Naam RE-auditor:	D.J.A.Koot RE / R.Driehuis RE
Ondertekend door RE-auditor:	Ja

Applicatieleverancier	
Naam serviceorganisatie:	Anoigo
Referentie/rapportnummer:	TPM 1: 2023-GBKZ0111RB TPM 2: Nvt
Afgiftedatum:	TPM 1: 11-01-2023 TPM 2: Nvt
Naam RE-auditor:	R.J.M. Bardoel RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) 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 2C-2023-460.

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

DigiD-norm		**Getoetst bij aansluithouder**	**Getoetst bij IT-leverancier**	**Getoetst bij applicatie - leverancier Mozard**	**Getoetst bij applicatie - leverancier Anoigo**	**Totaal oordeel norm**
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet niet	Voldoet	Niet van toepassing	Voldoet niet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij IT-leverancier	Getoetst bij applicatie - leverancier Mozard	Getoetst bij applicatie - leverancier Anoigo	Totaal oordeel norm
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet	Niet van toepassing	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Niet van toepassing	Niet van toepassing	Voldoet