Bijlage 1 DigiD (1)

Gemeentelijk kenmerk bijlage 1 DigiD:	03. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1 DigiD cv

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting iBurgerzaken en aansluitnummer 1002498

Dit is een bijlage bij de Collegeverklaring ENSIA 2020. Deze bijlage wordt opgesteld voor elke individuele DigiD-aansluiting waarover wij verantwoording afleggen. Het doel van deze samenvatting is om het College en Logius een totaaloverzicht te verschaffen over de resultaten van DigiD-aansluiting iBurgerzaken en aansluitnummer 1002498.

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:	PinkRoccade Local Government B.V.
Referentie/rapportnummer:	20201112 DBA-PRLG
Afgiftedatum:	12 november 2020
Naam RE-auditor:	Frank Kossen RE en Drs. M. El Aarbaoui RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM['s] / assurancerapportage 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 SH1298/20.

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

DigiD-norm		Getoetst bij Gemeente	(Optioneel) 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

Zie voor toelichting op de DigiD-normen Tabel 1.

Bijlage 1 DigiD (2)

Gemeentelijk kenmerk bijlage 1 DigiD:	03. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1 DigiD cv

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting MijnGKB en aansluitnummer 1000913

Dit is een bijlage bij de Collegeverklaring ENSIA 2020. Deze bijlage wordt opgesteld voor elke individuele DigiD-aansluiting waarover wij verantwoording afleggen. Het doel van deze samenvatting is om het College en Logius een totaaloverzicht te verschaffen over de resultaten van DigiD-aansluiting MijnGKB en aansluitnummer 1000913.

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's / assurancerapportages van onze serviceorganisaties:

Leverancier 1	
Naam serviceorganisatie:	Innovadis
Referentie/rapportnummer:	AAS2020-874
Afgiftedatum:	28 oktober 2020
Naam RE-auditor:	J.R. Möhle RE
Ondertekend door RE-auditor:	Ja

Leverancier 2	
Naam serviceorganisatie:	Previder
Referentie/rapportnummer:	AAS2020-873
Afgiftedatum:	28 oktober 2020
Naam RE-auditor:	J.R. Möhle RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage 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 SH1298/20.

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

DigiD-norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Getoetst bij leverancier 2	Totaal oordeel norm
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	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	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	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement		Voldoet	Voldoet	Voldoet

Zie voor toelichting op de DigiD-normen Tabel 1.

Bijlage 1 DigiD (3)

Gemeentelijk kenmerk bijlage 1 DigiD:	03. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1 DigiD cv

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal loket en aansluitnummer 1001913

Dit is een bijlage bij de Collegeverklaring ENSIA 2020. Deze bijlage wordt opgesteld voor elke individuele DigiD-aansluiting waarover wij verantwoording afleggen. Het doel van deze samenvatting is om het College en Logius een totaaloverzicht te verschaffen over de resultaten van DigiD-aansluiting Digitaal loket en aansluitnummer 1001913.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. In deze bijlage zijn de resultaten opgenomen van de uitgevoerde zelfevaluatie DigiD. Deze zelfevaluatie is toegepast op dat deel van het normenkader die niet onder uitbesteding aan onze leveranciers valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Dimpact
Referentie/rapportnummer:	2011R.AH120
Afgiftedatum:	1 december 2020
Naam RE-auditor:	drs. A.J.A. Hassing RE RA
Ondertekend door RE-auditor:	Ja

De uitkomsten uit de zelfevaluatie zijn getoetst door een RE-gecertificeerde IT-auditor. Deze heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage van onze serviceorganisatie het gehele normenkader afdekken. De uitkomsten van de auditor zijn opgenomen in het assurancerapport met kenmerk SH1298/20.

Onderstaande tabel toont de resultaten van de normen die zijn getoetst bij de serviceorganisatie én de bij ons getoetste normen. Het kan voorkomen dat een norm deels bij een leverancier getoetst is en deels bij de gemeente getoetst is (zogenaamde gedeelde 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 niet [1]	Voldoet niet [1]
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

Zie voor toelichting op de DigiD-normen Tabel 1.

[1] Voor de norm U/PW.03 geldt dat aan de testaanpak wordt voldaan, behalve op de eisen voor 'unsafe-inline' en 'unsafe-eval'. Sigmax Law Enforcement B.V. heeft voor het gebruik van 'unsafe-inline' en 'unsafe-eval' een ontwikkelplan opgesteld waarbij redelijkerwijs kan worden aangenomen dat vóór 1 november 2021 aan de gehele testaanpak voor de norm kan worden voldaan, dan wel dat er afdoende maatregelen zijn genomen om het gebruik van 'unsafe-inline' en 'unsafe-eval' te mitigeren.

Bijlage 1 DigiD (4)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting CityPermit en aansluitnummer 1001382

Gemeentelijk kenmerk bijlage 1 DigiD:	03. Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet Groningen, bijlage 1 DigiD cv

Dit is een bijlage bij de Collegeverklaring ENSIA 2020. Deze bijlage wordt opgesteld voor elke individuele DigiD-aansluiting waarover wij verantwoording afleggen. Het doel van deze samenvatting is om het College en Logius een totaaloverzicht te verschaffen over de resultaten van DigiD-aansluiting CityPermit en aansluitnummer 1001382.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. In deze bijlage zijn de resultaten opgenomen van de uitgevoerde zelfevaluatie DigiD. Deze zelfevaluatie is toegepast op dat deel van het normenkader die niet onder uitbesteding aan onze leveranciers valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Sigmax
Referentie/rapportnummer:	2009R.AH58
Afgiftedatum:	18 november 2020
Naam RE-auditor:	Drs. A.J.A. Hassing RE RA
Ondertekend door RE-auditor:	Ja

De uitkomsten uit de zelfevaluatie zijn getoetst door onze RE-gecertificeerde IT-auditor. Deze heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage van onze serviceorganisatie het gehele normenkader afdekken. De uitkomsten van de auditor zijn opgenomen in het assurancerapport met kenmerk SH1298/20.

Onderstaande tabel toont de resultaten van de normen die zijn getoetst bij de serviceorganisatie én de bij ons getoetste normen. Het kan voorkomen dat een norm deels bij een leverancier getoetst is en deels bij de gemeente getoetst is (zogenaamde gedeelde 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 niet [2]	Voldoet niet [2]
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

Zie voor toelichting op de DigiD-normen Tabel 1.

[2] Voor de norm U/PW.03 geldt dat aan de testaanpak wordt voldaan, behalve op de eisen voor 'unsafe-inline' en 'unsafe-eval'. Sigmax Law Enforcement B.V. heeft voor het gebruik van 'unsafe-inline' en 'unsafe-eval' een ontwikkelplan opgesteld waarbij redelijkerwijs kan worden aangenomen dat vóór 1 november 2021 aan de gehele testaanpak voor de norm kan worden voldaan, dan wel dat er afdoende maatregelen zijn genomen om het gebruik van 'unsafe-inline' en 'unsafe-eval' te mitigeren.

Tabel 1. Toelichting DigiD-normen

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.

Groningen, 30 maart 2021

Burgemeester en wethouders van gemeente Groningen

Burgemeester,

Koen Schuiling

Gemeentesecretaris,

Christien Bronda