Bijlage 1 DigiD (1)

Gemeentelijk kenmerk bijlage 1 DigiD:	099462370
Naam auditfirma:	SafeHarbour
Naam auditor:	Ronald Driehuis
Datum: april 2019	

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Valkenburg aan de Geul en aansluitnummer 1002251

Dit is een bijlage bij de Collegeverklaring ENSIA 2018. 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 Gemeente Valkenburg aan de Geul en aansluitnummer 1002251.

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['s] / assurancerapportage['s] van onze serviceorganisatie[s]:

Leverancier 1	
Naam serviceorganisatie:	SIMgroep
Referentie/rapportnummer:	SIMGR-1801-11.601
Afgiftedatum:	27-11-2018
Naam RE-auditor:	C.M. Hollemans
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['s] / assurancerapportage['s] van onze serviceorganisatie[s] het gehele normenkader afdekken. De uitkomsten van de auditor zijn opgenomen in het assurancerapport met kenmerk SH0271. 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**	**(Optioneel) Getoetst bij leverancier 1**	**Totaal oordeel norm**
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet

Voor identificatiedoeleinden

Naam Audit organisatie SafeHarbour AUDIT PRIVACY SECURITY

Naam Auditor R. Driehuis RE CISA

Datum 12-4-2019

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	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

Voor identificatiedoeleinden

Naam Audit organisatie SafeHarbour AUDIT PRIVACY SECURITY

Naam Auditor R. Driehuis RE CISA

Datum 12-4-2019

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 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

Voor identificatiedoeleinden

Naam Audit organisatie SafeHarbour AUDIT PRIVACY SECURITY

Naam Auditor R. Driehuis RE CISA

Datum 12-4-2019

	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.

Voor identificatiedoeleinden

Naam Audit organisatie SafeHarbour AUDIT PRIVACY SECURITY

Naam Auditor R. Driehuis RE CISA

Datum 12-4-2019