

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Heemstede iBurgerzaken en aansluitnummer 1002557

Heemstede biedt de volgende functionaliteit aan waarvoor DigiD aansluiting Gemeente Heemstede iBurgerzaken voor authenticatie wordt gebruikt:

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

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken.

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door PinkRoccade Local Government.

Deze applicatie is extern benaderbaar via de volgende URL's:

- www.iburgerzaken.heemstede.nl

DigiD aansluiting Gemeente Heemstede iBurgerzaken bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door PinkRoccade Local Government in de vorm van een SAAS-oplossing.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Gemeente Heemstede iBurgerzaken. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL[s] 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 Heemstede heeft een deel van de DigiD webomgeving uitbesteed aan PinkRoccade Local Government. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. 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 onze leverancier valt. De overige normen worden afgedekt door onderstaande TPM van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Pink Roccade Local Government
Referentie/rapportnummer:	20191021 DBA-PRLG
Afgiftedatum:	21 oktober 2019
Naam RE-auditor:	F. Kossen
Ondertekend door RE-auditor:	Ja

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 SH0877H/19.

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

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.

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Heemstede Sigmax en aansluitnummer 1002455

Heemstede biedt de volgende functionaliteit aan waarvoor DigiD aansluiting Gemeente Heemstede Sigmax voor authenticatie wordt gebruikt:

- Parkeervergunningen aanvragen/verlengen/stopzetten

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- CityPermit

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

Deze applicatie is extern benaderbaar via de volgende URL:

www.parkeren.heemstede.nl

DigiD aansluiting Gemeente Heemstede Sigmax bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door Sigmax in de vorm van een SAAS-oplossing.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Gemeente Heemstede Sigmax. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL['s] 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 Heemstede heeft een deel van de DigiD webomgeving uitbesteed aan Sigmax. Als gevolg hiervan is een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. 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 onze leverancier valt. De overige normen worden afgedekt door onderstaande TPM van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Sigmax
Referentie/rapportnummer:	1910R.AH83
Afgiftedatum:	7 oktober 2019
Naam RE-auditor:	drs. A.J.A. Hassing
Ondertekend door RE-auditor:	Ja

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 SH0877H/19.

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/ 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

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.