

Collegeverklaring ENSIA 2020

inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Collegeverklaring ENSIA 2020 inzake Informatiebeveiliging DigiD en Suwinet

Gemeentelijk kenmerk collegeverklaring ENSIA:	21bb04968
--	-----------

Gemeente Rotterdam

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Rotterdam voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Gemeenten (BIG), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte en diepgang verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Rotterdam betreft dit in 2020 DigiD en Suwinet.

De verklaring omvat het op 31 december 2020 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2020.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener[s] vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk 21bb04968) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverleners worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverleners worden uitgevoerd, wordt door de dienstverleners verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverleners dekken tezamen de normen inzake DigiD af.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 21bb04968) en Suwinet (bijlage 2 Suwinet met kenmerk 21bb04968) zijn de eventuele afwijkingen van de normen opgenomen.

Verklaring college

Het college verklaart dat voor DigiD en voor Suwinet nog niet aan alle gestelde normen wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in afzonderlijke verbeterplannen opgenomen, zijn belegd en worden gemonitord.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD	Ja	Niet van toepassing
DigiD	Nee	Ja
DigiD	Ja	Niet van toepassing
DigiD	Ja	Niet van toepassing
Suwinet DKD Inlezen	Nee	Ja
Suwinet	Nee	Ja

Rotterdam, 20-04-2021

Burgemeester en Wethouders van Rotterdam,

De secretaris,

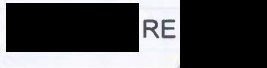




V.J.M. Roozen

De burgemeester,



A. Aboutaleb

Naam auditfirma:	Concern Auditing Gemeente Rotterdam
Naam auditor:	 RE  26-04-2021
	

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Rotterdam

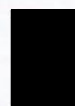
Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Gemeente Rotterdam. De zelfevaluatie heeft zich gericht op de webapplicatie, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

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 leveranciers valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage's van onze serviceorganisaties:

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie het gehele normenkader afdekken. Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm

DigiD Norm		Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• nvt	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet Niet	• nvt	• Voldoet Niet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• nvt	• Voldoet
U/WA.03	Automatische data invoer controle	• Voldoet	• nvt	• Voldoet
U/WA.04	Normaliseren uitvoer	• Voldoet	• nvt	• Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet Niet	• nvt	• Voldoet Niet
U/PW.02	Garanderen webprotocollen	• Voldoet	• nvt	• Voldoet
U/PW.03	Configureren webserver	• Voldoet Niet	• nvt	• Voldoet Niet

U/PW.05	Toegang tot beheermechanismen	• Voldoet	• nvt	• Voldoet
U/PW.07	Hardening van platformen	• Voldoet	• nvt	• Voldoet
U/NW.03	DMZ	• Voldoet	• nvt	• Voldoet
U/NW.04	Protectie- en detectiemechanismen	• Voldoet	• nvt	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	• Voldoet	• nvt	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• nvt	• Voldoet
C.03	Vulnerability-assessments	• Voldoet	• nvt	• Voldoet
C.04	Penetratietesten	• Voldoet	• nvt	• Voldoet
C.06	Signaleringsfuncties	• Voldoet	• nvt	• Voldoet
C.07	Monitoring functies	• Voldoet	• nvt	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• nvt	• Voldoet
C.09	Patchmanagement	• Voldoet	• nvt	• Voldoet



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

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting [REDACTED]. De zelfevaluatie heeft zich gericht op de webapplicatie, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Gemeente Rotterdam heeft een deel van de DigiD webomgeving uitbesteed aan Innovadis. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze service organisatie[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 onze leveranciers valt. De overige normen worden afgedekt door onderstaande TPM's van onze serviceorganisaties:

Leverancier 1	
Naam serviceorganisatie:	[REDACTED]
Referentie/rapportnummer:	[REDACTED]
Afgiftedatum:	[REDACTED]
Naam RE-auditor:	[REDACTED]
Ondertekend door RE-auditor:	Ja

Leverancier 2	
Naam serviceorganisatie:	[REDACTED]
Referentie/rapportnummer:	[REDACTED]
Afgiftedatum:	[REDACTED]
Naam RE-auditor:	[REDACTED]
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurance rapportages van onze serviceorganisaties 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. Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm

DigiD Norm		Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet	• Voldoet

U/TV.0 1	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet	• Voldoet
U/WA.0 2	Webapplicatiebeheer proces	• Voldoet	• Voldoet		• Voldoet
U/WA.0 3	Automatische data invoer controle		• Voldoet		• Voldoet
U/WA.0 4	Normaliseren uitvoer		• Voldoet		• Voldoet
U/WA.0 5	Cryptografie/ Privacy bevordering	• Voldoet	• Voldoet	• Voldoet	• Voldoet
U/PW.0 2	Garanderen webprotocollen		• Voldoet		• Voldoet
U/PW.0 3	Configureren webserver		• Voldoet		• Voldoet
U/PW.0 5	Toegang tot beheermechanismen			• Voldoet	• Voldoet
U/PW.0 7	Hardening van platformen			• Voldoet	• Voldoet
U/NW.0 3	DMZ			• Voldoet	• Voldoet
U/NW.0 4	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
<p>■</p> <p>Hoeft volgens de gemeente en volgens hoofdstuk "verantwoordelijkheden gebruikersorganisatie" van de TPM van de serviceorganisatie niet bij de gemeente getoetst te worden.</p>					

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 hardeningsrichtlijn 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 (3)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting [REDACTED] en aansluitnummer [REDACTED]

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting [REDACTED]. De zelfevaluatie heeft zich gericht op de webapplicatie de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Gemeente Rotterdam heeft een deel van de DigiD webomgeving uitbesteed aan [REDACTED]

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[s] valt. De overige normen worden afgedekt door onderstaande TPM/assurancerapportage van onze serviceorganisatie:

Leverancier 1

Naam serviceorganisatie:

Referentie/rapportnummer:

Afgiftedatum:

Naam RE-auditor:

Ondertekend door RE-auditor:

Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage 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 [REDACTED]

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per 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
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	• 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

Hoeft volgens de gemeente en volgens hoofdstuk "verantwoordelijkheden gebruikersorganisatie" van de TPM van de serviceorganisatie niet bij de gemeente getoetst te worden.

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 privacy bevorderende en crypto grafische 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 (beveiliging)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.



Bijlage 1 DigiD (4)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Aansluiting [REDACTED] - Gemeente Rotterdam en aansluitnummer [REDACTED]

Het object van zelfevaluatie is de web omgeving van DigiD aansluiting [REDACTED]. De zelfevaluatie heeft zich gericht op de webapplicatie de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Gemeente Rotterdam heeft een deel van de DigiD we omgeving uitbesteed aan het bedrijf [REDACTED]

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 onze leverancier valt. De overige normen worden afgedekt door onderstaande TPM/ assurancerapportage van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	[REDACTED]
Referentie/rapportnummer:	[REDACTED]
Afgiftedatum:	[REDACTED]
Naam RE-auditor:	[REDACTED]
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / 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.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm

DigiD Norm	Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• 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	• Voldoet Niet
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 privacy bevorderende en crypto grafische 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 (beveiliging)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.



Gemeentelijk kenmerk bijlage 2 Suwinet:

21bb04968

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de collegeverklaring ENSIA 2020 van de gemeente Rotterdam. Deze verklaring heeft betrekking op het op 31 december 2020 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie Verantwoordingsstelsel ENSIA). Deze bijlage is opgesteld voor de gemeenteraad en het Ministerie van Sociale Zaken en Werkgelegenheid. Onderwerp van de verklaring is het gebruik van Suwinet. Suwinet wordt niet in samenwerkingsverbanden gebruikt. Alle Suwinet voorzieningen waar de gemeente gebruik van maakt, zijn opgenomen in de collegeverklaring

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie
Participatiewet / IOAW/ IOAZ	binnen de gemeente

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)	binnen de gemeente
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	binnen de gemeente
Adresonderzoek door Burgerzaken	binnen de gemeente

Normnaleving

Zoals in de Collegeverklaring vermeld, voldoen de interne beheersmaatregelen inzake Suwinet op 31 december 2020 in opzet en bestaan aan de geselecteerde normen.

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de **SUWI-taken** op 31 december 2020 in opzet en bestaan aan alle geselecteerde normen:

Organisatie	SUWI Taak	BIG-nummer en nummer SUWI-norm	Applicatie
Gemeente Rotterdam	Participatiewet/IOAW/IOAZ	10.1.1 12.1.1 12.4.1	
Gemeente Rotterdam	Participatiewet/IOAW/IOAZ	6.12 7.2.2	

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de **niet-SUWI-taken** in opzet en bestaan aan alle geselecteerde normen

Gemeente Rotterdam	IOAW/IOAZ	12.4.1	
--------------------	-----------	--------	--