Collegeverklaring Verantwoording Informatiebeveiliging 2017

Het college van burgemeester en wethouders van de gemeente Groningen legt met deze verklaring verantwoording af over informatiebeveiliging met betrekking tot DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek. Het doel van ENSIA is om op eenduidige wijze verantwoording over informatiebeveiliging af te leggen, zowel aan de gemeenteraad als aan toezichthouders binnen de rijksoverheid. ENSIA sluit aan op de gemeentelijke planning- en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie.[1]

Voor DigiD en Suwinet wordt zekerstelling gevraagd van een onafhankelijke auditor. De rapportage van de IT-auditor over deze verklaring is opgenomen in een apart assurancerapport. Zowel voor DigiD als voor Suwinet geldt dat er in 2017 vernieuwde versies van de onderliggende normenkaders zijn verschenen. Hierbij zijn de richtlijnen door de toezichthouders aangepast en zijn de eisen ten opzichte van voorgaande jaren strenger geworden.

Reikwijdte verklaring

Deze verklaring betreft de volgende DigiD- en Suwinet-aansluitingen:

- E-Loket (webformulieren voor informatie en aanvragen; 463402),
- MijnGKB (webportaal voor schuldhulpverlening; 1000913),
- Digitaal Loket (webapplicatie van Dimpact voor inzage in zaken; 1001913),
- CityPermit (webapplicatie voor aanvraag parkeervergunningen; 1001382),
- Suwinet-aansluiting voor de directies in het Sociaal Domein,
- Suwinet-aansluiting voor het Regionaal Meld- en Coördinatiepunt.

De verklaring heeft betrekking op het in opzet en bestaan voldoen aan de DigiD-normen[2] en de Suwinet-normen[3], waarbij deze zijn geselecteerd op grond van de notitie Verantwoordingsstelsel zoals gepubliceerd op de ENSIA website[4]. De normen zijn gebaseerd op internationale standaarden en zijn geschikt voor het doel van deze collegeverklaring. De collegeverklaring omvat niet de werking van de maatregelen over 2017.

Het beheer van een deel van de DigiD-aansluitingen valt onder verantwoordelijkheid van externe dienstverleners. Het betreft de webapplicaties MijnGKB en Digitaal Loket. De externe dienstverlener heeft de beheersmaatregelen voor deze aansluitingen aan de gemeente verantwoord. Met deze collegeverklaring en de verantwoording van de externe dienstverlener zijn alle geselecteerde normen getoetst.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn met de bijlagen Suwinet-bevindingen (bijlage 1) en DigiD-bevindingen (bijlage 2) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij de gemeente Groningen op 31 maart 2018 de interne beheersingsmaatregelen in opzet en bestaan nog niet volledig voldoen aan de geselecteerde normen inzake DigiD. Voor Suwinet geldt dat de gemeente Groningen volledig voldoet aan de binnen ENSIA getoetste normen.

---

[1] Naast DigiD en Suwinet heeft ENSIA betrekking op de verantwoording van gemeenten over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Grootschalige Topografie (BGT). De verantwoording met betrekking tot deze voorzieningen valt dit jaar nog buiten de collegeverklaring informatieveiligheid. Daarvoor dienen andere rapportages.

[2] Norm ICT-beveiligingsassessments DigiD versie 2.0 (https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/)

[3] Normenkader Afnemers, versie 1.01 (https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten)

[4] Zie bijlage 1 van deze notitie (https://www.ensia.nl/)

Risicoanalyse

Voor DigiD geldt dat er op basis van de bevindingen geen directe risico's zijn gesignaleerd voor de informatieveiligheid. Risico's op basis van de bevindingen zijn beperkt, mede omdat er aanvullende beheersmaatregelen zijn ingeregeld (o.a. monitoring).

Een deel van de bevindingen heeft betrekking op normen die van organisatorische aard zijn, zoals de doorvertaling van beveiligingseisen naar dienstverleners, functiescheiding, autorisatiebeheer en wijzigingenbeheer. Het aantoonbaar voldoen aan de eisen en richtlijnen - in zowel opzet als bestaan - is hierbij niet in alle gevallen mogelijk gebleken. Om deze risico's weg te nemen zijn aanvullende organisatorische beheersmaatregelen noodzakelijk.

Daarnaast zijn er vanuit securitytesten voor een tweetal DigiD aansluitingen kwetsbaarheden naar voren gekomen, die er (mede) toe leiden dat een aantal van de normen als 'voldoet niet' wordt aangeduid. De middels securitytesten vastgestelde kwetsbaarheden, hebben als risicoclassificatie 'laag' of 'middel'. Dit komt overeen met onze eigen interne risicobeoordeling. Om de risico's ten aanzien van deze kwetsbaarheden te beperken, dienen deze technisch verholpen te worden.

Voor de bevindingen gelden tenslotte onderstaande verklaringen en toelichtingen:

- In 2017 zijn vernieuwde versies van de onderliggende normenkaders verschenen, hierbij zijn de richtlijnen aangepast en zijn de eisen strenger geworden.
- De geplande uitfasering van de DigiD aansluiting voor het E-Loket heeft geleid tot acceptatie, van enkele als laag risico gekwalificeerde kwetsbaarheden. Hierdoor zijn bij de securitytesten ten behoeve van het E-Loket meer bevindingen gerapporteerd.
- In het kader van de voorgenomen outsourcing van de generieke ICT-infrastructuur is besloten om de verbetering van maatregelen en beheerprocedures waaraan DigiD eisen stelt bij de externe dienstverlener te beleggen.
- Vastgestelde verbeteringen van beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.

Groningen, 25 april 2018

burgemeester en wethouders van Groningen,

de burgemeester,

Peter den Oudsten

de secretaris,

Peter Teesink

Bijlage 1 Suwinet bevindingen (definitieve oordelen auditor)

Nr	Beschrijving van de beveiligingsrichtlijn	Suwinet-inkijk GMC	Suwinet-inkijk RMC
B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	Voldoet	Voldoet
B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	Voldoet	Voldoet
B.05	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	Voldoet	Voldoet
U.02	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.	Voldoet	Voldoet
U.03	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	Voldoet	Voldoet
U.11	De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet.	Voldoet	Voldoet
C.01	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën.	Voldoet	Voldoet
C.04	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).	Voldoet	Voldoet
C.05	Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles.	Voldoet	Voldoet
C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen)	Voldoet	Voldoet
C.07	De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.	Voldoet	Voldoet

Bijlage 2 DigiD bevindingen (definitieve oordelen auditor) – E-Loket

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij gebruikersorganisatie (Gemeente Groningen)	Kenmerk rapport
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een w ebapplicatie (als dienst) zijn de beveiligingseisen en -w ensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	**Voldoet niet**	2017.399
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouw bare 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	**Voldoet niet** [1]	2017.399
U/WA.02	Het w ebapplicatiebeheer is procesmatig en procedureel ingericht, w aarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten	**Voldoet niet**	2017.399
U/WA.03	De w ebapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer w ordt verw erkt	**Voldoet niet** [1]	2017.399
U/WA.04	De w ebapplicatie beperkt de uitvoer tot w aarden die (veilig) verw erkt kunnen w orden door deze te normaliseren	Voldoet	2017.399
U/WA.05	De w ebapplicatie garandeert de betrouw baarheid van informatie door toepassing van privacybevorderende en cryptografische technieken	**Voldoet niet** [1]	2017.399
U/PW.02	De w ebserver garandeert specifieke kenmerken van de inhoud van de protocollen	Voldoet	2017.399
U/PW.03	De w ebserver is ingericht volgens een configuratie-baseline	**Voldoet niet** [1]	2017.399
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en w ordt uitgevoerd conform het operationeel beleid voor platformen	Voldoet	2017.399
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar	Voldoet	2017.399

[1] Bevindingen gerapporteerd tijdens security testen (penetratie test)

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij gebruikersorganisatie (Gemeente Groningen)	Kenmerk rapport
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	Voldoet	2017.399
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen	Voldoet	2017.399
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd	Voldoet	2017.399
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	**Voldoet niet** [1]	2017.399
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie	Voldoet	2017.399
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie	Voldoet	2017.399
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht	Voldoet	2017.399
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	Voldoet	2017.399
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	2017.399
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen	**Voldoet niet**	2017.399

[1] Bevindingen gerapporteerd tijdens security testen (penetratie test)

Bijlage 2 DigiD bevindingen (definitieve oordelen auditor) – MijnGKB

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij de applicatieleverancier (externe dienstverlener)	Kenmerk rapport	Oordeel bij de hostingleverancier (externe dienstverlener)	Kenmerk rapport	Aanvullende beheersmaatregelen gebruikersorganisatie noodzakelijk?[1]	Oordeel bij gebruikersorganisatie (Gemeente Groningen)	Kenmerk rapport
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.	Voldoet	2017.028.2	Voldoet	AAS2018-289	Ja	**Voldoet niet**	2017.399
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	Voldoet	2017.028.2	Voldoet	AAS2018-289	Ja	Voldoet	2017.399
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten	Voldoet	2017.028.2	n.v.t.	-	Ja	Voldoet	2017.399
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt	Voldoet	2017.028.2	n.v.t.	-	Nee	n.v.t.	-
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren	Voldoet	2017.028.2	n.v.t.	-	Nee	n.v.t.	-
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken	Voldoet	2017.028.2	Voldoet	AAS2018-289	Ja	Voldoet	2017.399
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen	Voldoet	2017.028.2	n.v.t.	-	Nee	n.v.t.	-
U/PW.03	De webserver is ingericht volgens een configuratie-baseline	Voldoet	2017.028.2	n.v.t.	-	Nee	n.v.t.	-
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	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-

[1] Naar het oordeel van de auditor van de externe dienstverleners

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij de applicatieleverancier (externe dienstverlener)	Kenmerk rapport	Oordeel bij de hostingleverancier (externe dienstverlener)	Kenmerk rapport	Aanvullende beheersmaatregelen gebruikersorganisatie noodzakelijk?[1]	Oordeel bij gebruikersorganisatie (Gemeente Groningen)	Kenmerk rapport
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	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	n.v.t.	-	Voldoet	AAS2018-289	Nee	Voldoet	2017.399
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie	Voldoet	2017.028.2	n.v.t.	-	Nee	n.v.t.	-
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
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	n.v.t.	-	Voldoet	AAS2018-289	Nee	n.v.t.	-
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	2017.028.2	Voldoet	AAS2018-289	Ja	Voldoet	2017.399
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen	Voldoet	2017.028.2	Voldoet	AAS2018-289	Nee	n.v.t.	-

[1] Naar het oordeel van de auditor van de externe dienstverleners

Bijlage 2 DigiD bevindingen (definitieve oordelen auditor) – Digitaal Loket

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij de serviceorganisatie (externe dienstverlener)	Kenmerk rapport	Aanvullende beheersmaatregelen gebruikersorganisatie noodzakelijk?[1]	Oordeel bij gebruikersorganisatie	Kenmerk rapport
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een w ebapplicatie (als dienst) zijn de beveiligingseisen en -w ensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet	2017.268	Ja	Voldoet	2017.399
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouw bare 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	Voldoet	2017.268	Ja	**Voldoet niet**	2017.399
U/WA.02	Het w ebapplicatiebeheer is procesmatig en procedureel ingericht, w aarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten	Voldoet	2017.268	Ja	Voldoet	2017.399
U/WA.03	De w ebapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer w ordt verw erkt	Voldoet	2017.268	Nee	n.v.t.	-
U/WA.04	De w ebapplicatie beperkt de uitvoer tot w aarden die (veilig) verw erkt kunnen w orden door deze te normaliseren	Voldoet	2017.268	Nee	n.v.t.	-
U/WA.05	De w ebapplicatie garandeert de betrouw baarheid van informatie door toepassing van privacybevorderende en cryptografische technieken	Voldoet	2017.268	Ja	Voldoet	2017.399
U/PW.02	De w ebserver garandeert specifieke kenmerken van de inhoud van de protocollen	Voldoet	2017.268	Nee	n.v.t.	-
U/PW.03	De w ebserver is ingericht volgens een configuratie-baseline	Voldoet	2017.268	Nee	n.v.t.	-
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en w ordt uitgevoerd conform het operationeel beleid voor platformen	Voldoet	2017.268	Nee	n.v.t.	-
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar	**Voldoet niet**	2017.268	Nee	n.v.t.	-

[1] Naar het oordeel van de auditor van de externe dienstverlener

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij de serviceorganisatie (externe dienstverlener)	Kenmerk rapport	Aanvullende beheersmaatregelen gebruikersorganisatie noodzakelijk?[1]	Oordeel bij gebruikersorganisatie	Kenmerk rapport
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	Voldoet	2017.268	Nee	n.v.t.	-
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen	Voldoet	2017.268	Nee	n.v.t.	-
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd	Voldoet	2017.268	Nee	n.v.t.	-
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	2017.268	Ja	Voldoet	2017.399
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie	Voldoet	2017.268	Nee	n.v.t.	-
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie	Voldoet	2017.268	Nee	n.v.t.	-
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht	Voldoet	2017.268	Nee	n.v.t.	-
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	Voldoet	2017.268	Nee	n.v.t.	-
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	2017.268	Ja	Voldoet	2017.399
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen	Voldoet	2017.268	Nee	n.v.t.	-

[1] Naar het oordeel van de auditor van de externe dienstverlener

Bijlage 2 DigiD bevindingen (definitieve oordelen auditor) – CityPermit

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij de applicatieleverancier (externe dienstverlener)	Kenmerk rapport	Aanvullende beheersmaatregelen gebruikersorganisatie noodzakelijk?[1]	Oordeel bij gebruikersorganisatie	Kenmerk rapport
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.	Voldoet	1709R.AH91	Ja	**Voldoet niet**	2017.399
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	Voldoet	1709R.AH91	Ja	**Voldoet niet** [2]	2017.399
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten	n.v.t.	-	Ja	Voldoet	2017.399
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt	Voldoet	1709R.AH91	Nee	Voldoet	2017.399
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren	Voldoet	1709R.AH91	Nee	Voldoet	2017.399
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken	Voldoet	1709R.AH91	Ja	Voldoet	2017.399
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen	Voldoet	1709R.AH91	Nee	Voldoet	2017.399
U/PW.03	De webserver is ingericht volgens een configuratie-baseline	Voldoet	1709R.AH91	Nee	**Voldoet niet** [2]	2017.399
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	n.v.t.	-	Ja	Voldoet	2017.399
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar	n.v.t.	-	Ja	Voldoet	2017.399

[1] Naar het oordeel van de auditor van de externe dienstverleners

[2] Bevindingen gerapporteerd tijdens security testen (penetratie test)

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel bij de applicatieleverancier (externe dienstverlener)	Kenmerk rapport	Aanvullende beheersmaatregelen gebruikersorganisatie noodzakelijk?[1]	Oordeel bij gebruikersorganisatie	Kenmerk rapport
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	n.v.t.	-	Ja	Voldoet	2017.399
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen	n.v.t.	-	Ja	Voldoet	2017.399
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd	n.v.t.	-	Ja	Voldoet	2017.399
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	n.v.t.	-	Ja	Voldoet	2017.399
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie	n.v.t.	-	Ja	Voldoet	2017.399
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie	n.v.t.	-	Ja	Voldoet	2017.399
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht	n.v.t.	-	Ja	Voldoet	2017.399
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	n.v.t.	-	Ja	Voldoet	2017.399
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	1709R.AH91	Ja	**Voldoet niet**	2017.399
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen	n.v.t.	-	Ja	Voldoet	2017.399

[1] Naar het oordeel van de auditor van de externe dienstverleners

[2] Bevindingen gerapporteerd tijdens security testen (penetratie test)