Regeling van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties [PM] 2023, nr CZW/S&B/…., houdende nadere eisen met betrekking tot informatieveiligheid, audits en auditverklaringen voor publieke dienstverleners (Regeling dienstverleners informatieveiligheidsaudits Wdo)

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Gelet op artikel 24, vierde lid, van het Besluit digitale overheid;

Besluit:

Hoofdstuk 1 Algemeen

Artikel 1.1 Begripsbepalingen

In deze regeling wordt verstaan onder:

- *aansluiting*: technische koppeling op de voor de toegang tot elektronische dienstverlening relevante voorzieningen;

- *audit*: audit als bedoeld in artikel 4, tweede lid, van de wet;

- *auditverklaring*: verklaring als bedoeld in artikel 4, tweede lid, van de wet;

- *besluit*: Besluit digitale overheid;

- *elektronische dienstenomgeving:* elektronische omgeving waarbinnen na een authenticatie toegang kan worden verkregen tot elektronische dienstverlening, waaronder wordt begrepen het verrichten van een handeling in het kader van die elektronische dienstverlening;

- *minister*: minister van Binnenlandse Zaken en Koninkrijksrelaties;

- *webapplicatie:* applicatie die bereikbaar is met een webbrowser of vergelijkbare software, en die ondersteuning biedt voor het Hypertext Transfer Protocol.

Hoofdstuk 2 Aanvullende eisen aan informatiebeveiliging

Artikel 2.1 Minimale beveiligingsmaatregelen

Bestuursorganen en aangewezen organisaties nemen ter beveiliging van de toegang tot een elektronische dienstenomgeving door middel van een webapplicatie de ICT-beveiligingsnormen in acht, die zijn opgenomen in de bijlage bij deze regeling.

Hoofdstuk 3 Audits en auditverklaring

Artikel 3.1 Audits

1. Een audit heeft betrekking op de conformiteit van een bestuursorgaan of aangewezen organisatie met artikel 2.1.

2. Een audit ziet op de opzet en het bestaan van maatregelen die voldoen aan de normen, die zijn opgenomen in de bijlage bij deze regeling en voor de normen in die bijlage met de aanduiding “U/TV.01”, “U/WA.02”, “C.07”, “C.08”en “C.09” ziet de audit op de opzet en werking van de maatregelen.

3. Wanneer een bestuursorgaan of aangewezen organisatie aan een derde partij werkzaamheden heeft uitbesteed die relevant zijn voor de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening en de daarmee samenhangende maatregelen ter beveiliging van ontwerp, ontwikkeling, onderhoud, ondersteuning en werking van die elektronische dienstverlening heeft een audit tevens betrekking op die werkzaamheden bij die derde partij.

Artikel 3.2 Auditor

Aan artikel 24, derde lid, van het besluit, is in ieder geval voldaan indien een audit wordt uitgevoerd door een auditor die is ingeschreven in het register van de Nederlandse Orde van Register EDP-Auditors.

Artikel 3.3 Auditverklaring per aansluiting op een elektronische dienstenomgeving

1. Een bestuursorgaan of aangewezen organisatie legt voor elke aansluiting op een elektronische dienstenomgeving die toegang geeft toe elektronische diensten van dat bestuursorgaan of die aangewezen organisatie een auditverklaring over aan de minister.

2. Indien verschillende bestuursorganen of aangewezen organisaties diensten aanbieden via dezelfde elektronische dienstenomgevingen kan voor die dienstenomgevingen een gezamenlijke verklaring worden ingediend.

Artikel 3.4 Eisen aan een auditverklaring

1. In de auditverklaring:

a. wordt een conclusie over de conformiteit weergegeven per norm, genoemd in bijlage 1 bij deze regeling;

b. indien voor een norm, genoemd in artikel 3.1, tweede lid, is geconcludeerd dat de werking van een maatregel niet voldoet aan de daarvoor geldende norm, wordt een conclusie gegeven over de het bestaan van de desbetreffende maatregel;

c. wordt beschreven tot welke diensten een elektronische dienstenomgeving toegang geeft;

d. wordt bij toepassing van artikel 3.3, tweede lid, onderbouwd dat voldaan is aan de voorwaarden bedoeld in dat lid.

2. Voor een auditverklaring wordt in voorkomend geval gebruik gemaakt van een door de minister vastgesteld model, waarbij voor verschillende toepassingen een verschillend model kan worden vastgesteld.

3. Een auditverklaring wordt ondertekend door de auditor onder wiens verantwoordelijkheid de audits zijn uitgevoerd waarop het rapport is gebaseerd.

Artikel 3.5 Actuele audit

1. De bevindingen in een auditverklaring zijn gebaseerd op een audit die niet eerder is uitgevoerd dan op 31 december van het jaar voorafgaand aan het jaar waarop de auditverklaring ziet.

2. In afwijking van het eerste lid kan een auditverklaring voor werkzaamheden die zijn uitbesteed aan een derde partij worden gebaseerd op een audit van die derde partij die niet eerder is uitgevoerd dan 12 maanden voorafgaand aan de datum waarop de verklaring aan de minister is verzonden.

Artikel 3.6 Non-conformiteit werking van een maatregel

Indien in een auditverklaring is vermeld dat de werking van een maatregel niet voldoet aan de daarvoor geldende norm, verstrekt de indiener van die verklaring aanvullende informatie over:

a. de feiten en onderbouwing die tot dit conclusie leiden;

b. een analyse van de risico's die met die conclusie samenhangen;

c. en correctief actieplan waarin maatregelen zijn opgenomen om te borgen dat zo spoedig mogelijk aan de desbetreffende norm wordt voldaan.

Hoofdstuk 4 Gezamenlijke auditverklaring

Artikel 4.1 Criteria voor toepassing gezamenlijke auditverklaring

Het overleggen van een auditverklaring kan door verschillende bestuursorganen en aangewezen organisaties gezamenlijk plaatsvinden indien:

a. de toegang tot de elektronische dienstenomgeving waarop de auditverklaring ziet, wordt namens de desbetreffende bestuursorganen en aangewezen organisaties verzorgd door dezelfde derde partij;

b. de software en de processen die worden gebruikt door de derde partij, bedoeld in onderdeel a, en de functionaliteiten waarvoor deze worden gebruikt, bij alle bestuursorganen en aangewezen organisaties waarop de verklaring ziet, zijn gelijk en worden bij die organisaties uniform toegepast en de desbetreffende bestuursorganen en aangewezen organisaties hebben geen mogelijkheden om daarin aanpassingen door te voeren.

Artikel 4.2 Aanvullende eisen vereenvoudigde audit en auditverklaring

Onverminderd artikel 3.4 voorziet een auditverklaring bij toepassing van artikel 4.1 in:

a. een aanduiding van de bestuursorganen en aangewezen organisaties namens welke deze wordt ingediend;

b. een machtiging van de indienende partij om tot het indienen over te gaan namens de bestuursorganen en aangewezen organisaties bedoeld in onderdeel a;

c. een motivering van de toepassing van artikel 4.1.

Hoofdstuk 5 Slotbepalingen

Artikel 5.1 Citeertitel

Deze regeling wordt aangehaald als: Regeling dienstverleners informatieveiligheidsaudits Wdo.

Artikel 5.2 Inwerkingtreding

Deze regeling treedt in werking met ingang van [PM].

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Alexandra C. van Huffelen

Bijlage, ICT-beveiligingsnormen

Bijlage als bedoeld in artikel 2.1, tweede lid.

Tabel 3:

norm	Beschrijving (of domein)
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.
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 de 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 protectie- en detectiemechanismen.
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 assesments (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 ICTvoorzieningen.

Toelichting

1. Algemeen

Veiligheid en vertrouwen zijn in de digitale wereld, net als in de fysieke wereld, een absolute randvoorwaarde voor burgers en bedrijven om online met de overheid informatie te kunnen uitwisselen. Digitale informatie-uitwisseling is een essentieel onderdeel geworden voor het functioneren van de Nederlandse samenleving. Digitale communicatie is van groot belang voor het vertrouwen in en de integriteit van elektronische overheidsdienstverlening. Maar online veiligheid is verre van vanzelfsprekend, en er liggen dreigingen als phishing, botnets, cyberterorrisme en desinformatie op de loer. Iedereen moet erop kunnen vertrouwen dat de toegang tot de digitale dienstverlening van de overheid veilig is. Burgers en bedrijven die van die dienstverlening gebruik maken moeten ervan uit kunnen gaan dat hun gegevens en identiteit veilig zijn.

Een belangrijk speerpunt hierbij is het borgen van een (minimale) digitale volwassenheid op het gebied van informatieveiligheid bij overheden en de (semi-) publieke sector. Op grond van artikel 4 van de Wet digitale overheid moeten organisaties die publieke diensten aanbieden (hierna: publieke dienstverleners) voldoen aan regels gesteld over de werking, de betrouwbaarheid en de beveiliging van de toegang tot deze dienstverlening. Dat artikel schrijft ook voor dat deze organisaties een verklaring van een auditor moeten overleggen waaruit blijkt dat zij aan deze regels voldoen. Het wordt dus voor publieke dienstverleners wettelijk verplicht om aan informatieveiligheidseisen te voldoen en daarover jaarlijks te rapporteren.

Elektronische toegangsdiensten, dus inlogmiddelen en de daarbij horende ICT-voorzieningen, worden gezien als een vitale dienst en kunnen daarmee ook een aantrekkelijk doelwit zijn voor identiteitsfraude of ongewenste inmenging. Door kwetsbaarheden in deze voorzieningen te benutten kan toegang worden verkregen tot gevoelige informatie en kunnen personen of bedrijven schade leiden. Deze kwetsbaarheden kunnen zich op verschillende niveaus voordoen, van zeer technisch en gedetailleerd tot organisatorisch. Het kan bijvoorbeeld gaan om het invoeren van voor deze systemen onbekende tekens of ontbreken van voldoende lerend vermogen in een organisatie.

Met deze rapportages over informatieveiligheid wordt geborgd dat de beveiligingsrisico's van de door publieke dienstverleners gebruikte ICT-voorzieningen beperkt blijven. Het doel hiervan is om het stelsel voor toegang tot elektronische dienstverlening zo veilig mogelijk te houden en het risico op verstoring van de dienstverlening of inzage in vertrouwelijke gegevens door onbevoegden zo veel als mogelijk te beperken.

Om te voorkomen dat gegevens of gevoelige informatie over gebruikte technologieën in verkeerde handen vallen of voor onbevoegden inzichtelijk worden, is het van belang dat de publieke dienstverleners hun informatieveiligheid te allen tijde op orde hebben. Om de hierboven genoemde risico's zoveel mogelijk te beperken, stelt de minister regels aan de informatiebeveiliging van publieke dienstverleners.

De hoofdlijnen van deze regels zijn opgenomen in de artikelen 16 tot en met 24 van het Besluit digitale overheid. In deze ministeriële regeling worden meer gedetailleerde nadere regels gesteld over de beveiliging van webapplicaties die worden gebruikt voor toegang tot digitale dienstverlening en de wijze waarop publieke dienstverleners aantonen dat zij aan deze eisen voldoen. Het gaat bijvoorbeeld om beveiligingsmaatregelen die in ieder geval moeten worden genomen, nadere eisen aan de omvang van de audit, de kwalificaties van de auditor en aan de inrichting van een

auditverklaring, en de mogelijkheid om verschillende modellen voor te schrijven voor de aan te leveren rapportage.

Controle op de informatieveiligheid van publieke dienstverleners biedt burgers vertrouwen dat de authenticatiemiddelen die kunnen gebruikt om toegang te krijgen tot elektronische overheidsdiensten veilig kunnen worden gebruikt. Het verplicht publieke dienstverleners inzicht te geven in de informatieveiligheid van de op het stelsel aangesloten webapplicaties.

Deze regels zijn een voortzetting van de regels die al aan publieke dienstverleners werden gesteld voor het gebruik van DigiD voor hun elektronische diensten. Tot de inwerkingtreding van deze regeling werd daarvoor tussen deze dienstverleners en Logius een overeenkomst gesloten waarin dezelfde veiligheidsnormen en auditseisen waren opgenomen als voorwaarde voor het aansluiten op DigiD. Onder het regime van de Wet digitale overheid wordt niet langer aangesloten op DigiD, maar op een stelsel voor toegang. De eisen in deze regeling borgen derhalve het veilige functioneren van het stelsel voor zover dienstverleners daar invloed op kunnen hebben.

2. Juridisch kader

2.1. Toepassingsbereik: bestuursorganen en aangewezen organisaties

Artikel 4 van de Wet digitale overheid bevat de juridische basis voor de regels die aan publieke dienstverleners worden gesteld met betrekking tot de toegang tot publieke dienstverlening. Dat artikel is van toepassing op bestuursorganen en aangewezen organisaties. Onder bestuursorganen wordt als gevolg van artikel 1 van de Wet digitale overheid verstaan bestuursorganen als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht. De aanwijzing van organisaties vindt plaats in de wet en in de bijlage bij de wet en kan worden aangevuld met een aanwijzing op grond van het tweede tot en met vierde lid van artikel 2. Aangewezen organisaties zijn organisaties met een publieke taak, die niet vallen onder de reikwijdte van het begrip “bestuursorgaan”. Het gaat bijvoorbeeld om rechterlijke instanties, zorgaanbieders, pensioenuitvoerders en instellingen voor hoger onderwijs. In deze toelichting worden bestuursorganen en aangewezen organisaties aangeduid als publieke dienstverleners.

2.2. Eisen aan de werking, de beveiliging en betrouwbaarheid van de toegang

Het eerste lid van artikel 4 van de Wet digitale overheid bepaalt dat publieke dienstverleners moeten “voldoen aan bij of krachtens algemene maatregel van bestuur te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten op verschillende betrouwbaarheidsniveaus”. Op grond van dat artikel zijn regels gesteld in het Besluit digitale overheid.

In artikel 16 van het Besluit digitale overheid worden eisen gesteld aan het informatieveiligheidsbeleid van publieke dienstverleners. Artikel 19 bevat specifieke regels voor de ICT-voorzieningen en informatiesystemen die bij het verlenen van toegang worden gebruikt. Deze regels vormen het algemene kader waaraan publieke dienstverleners moeten voldoen. Artikel 19, eerste lid, van het Besluit digitale overheid bepaalt bijvoorbeeld onder meer dat functiescheiding moet worden toegepast bij deze systemen en voorzieningen. Als gevolg van het vierde lid van dat artikel moeten publieke dienstverleners bij het beveiligingsniveau passende beveiligingsmaatregelen nemen.

Op grond artikel 24 tweede lid, van het Besluit digitale overheid worden bij ministeriële regeling nadere beveiligingsregels waaraan publieke dienstverleners moeten voldoen en waarvan de conformiteit met een auditrapportage moet worden aangetoond. In de onderhavige regeling zijn deze nadere regels gesteld voor webapplicaties, bijvoorbeeld over scheiden van risicovolle delen van het netwerk van de delen van het netwerk die vanaf het internet bereikbaar zijn en worden de normen vastgesteld waaraan die applicaties moeten voldoen. Deze regeling is van toepassing op de ICT-systemen en informatiesystemen die door de publieke dienstverleners zelf worden beheerder, maar ook voor delen daarvan waarvoor het beheer door de desbetreffende publieke dienstverlener is uitbesteed.

2.3 Audit en auditverklaring

Artikel 4, tweede lid, van de Wet digitale overheid bepaalt dat publieke dienstverleners een verklaring van een auditor moeten overleggen waaruit blijkt of zij voldoen aan de gestelde regels. Het derde lid van dat artikel biedt een basis voor het stellen van regels over de wijze waarop publieke dienstverleners aantonen dat zij aan de gestelde regels voldoen. Dat artikellid maakt het dus mogelijk om nadere regels te stellen over de wijze waarop de audit wordt uitgevoerd, de kwalificaties van de auditor en de wijze waarop over de bevindingen van de audit wordt gerapporteerd.

In artikel 24 van het Besluit digitale overheid is vastgelegd dat een auditverklaring ziet op een kalenderjaar en dat deze jaarlijks voor 1 mei moet worden overgelegd. In het tweede lid is bepaald dat bij een audit wordt beoordeeld welke maatregelen zijn genomen en welke procedures worden gevolgd, dat een inhoudelijke beoordeling plaatsvindt van de wijze waarop die maatregelen zijn opgezet. Verder wordt in het derde lid voorgeschreven dat de audit moet worden uitgevoerd door een auditor die onafhankelijk en gekwalificeerd is. Het vierde lid biedt een basis voor het stellen bij ministeriële regeling van nadere regels over de audit, de verklaring en de auditor. Met deze regeling worden deze nadere regels gesteld.

3. Nadere eisen aan de beveiliging van webapplicaties

Met deze ministeriële regeling worden de beveiligingsnormen vastgesteld waar een webapplicatie die wordt gebruik voor toegang tot elektronische overheidsdiensten aan moet voldoen. Deze eisen zijn opgenomen in de bijlage bij deze regeling. Het gaat om een voor deze toepassing relevante selectie van de ICT-beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum[1].

Zoals in het voorgaande is aangegeven kunnen de beveiligingsrisico's zich op verschillende niveaus manifesteren, van zeer technisch tot organisatorisch en op het domein van beveiligingsbeleid. De beveiligingsmaatregelen hebben daarom niet alleen betrekking op de webapplicatie, maar ook op de beheeromgeving en de omringende hard- en softwareomgeving die noodzakelijk is om de webapplicatie te laten functioneren. De richtlijnen worden verdeeld in verschillende domeinen.

1. Beleidsdomein (normen aangeduid met B)
   Hier bevinden zich elementen die aangeven wat in organisatiebrede zin bereikt kan worden en bevat daarom conditionele en randvoorwaardelijke elementen die van toepassing zijn op

[1] 'ICT-Beveiligingsrichtlijnen voor Webapplicaties', Nationaal Cyber Security Centrum, September 2015

de overige lagen, zoals doelstellingen, informatiebeveiligingsbeleid, strategie en vernieuwing, organisatiestructuur en architectuur.

2. Uitvoeringsdomein (normen aangeduid met (TV, WA, PW en NW)
   In dit domein wordt de implementatie van de ICT-diensten uiteengezet, zoals toegangsvoorzieningen, webapplicaties, platformen, webservers en netwerken.
3. Beheersingsdomein (normen aangeduid met C)
   Evaluatieaspecten en meetaspecten zijn in dit domein opgenomen. Daarnaast treffen we hier ook de beheerprocessen aan, die noodzakelijk zijn voor de instandhouding van ICT-diensten. De informatie uit de evaluaties en de beheerprocessen is niet alleen gericht op het bijsturen van de geïmplementeerde webapplicaties, maar ook om het bijsturen en/of aanpassen van de eerder geformuleerde conditionele elementen die gebaseerd zijn op “onzekere” informatie en aannames, visie en uitgestippeld beleid. Een voorbeeld van een dergelijke aanname is een inschatting van de capaciteitsbehoefte. In de praktijk kan (en zal) het gebruik anders zijn dan oorspronkelijk verondersteld. Dan is een mechanisme nodig dat de daadwerkelijke belasting meet en een proces waarin eventueel noodzakelijke veranderingen worden vastgesteld en doorgevoerd.

Hierna wordt inhoudelijk op de verschillende normen ingegaan.

B.01 Beveiligingsbeleid

Op grond van deze norm is een publieke dienstverlener gehouden om informatiebeveiligingsbeleid te formuleren en daarin specifieke aandacht te besteden aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. Hiermee wordt ervoor gezorgd dat er in alle lagen van de organisatie aandacht is voor de specifieke risico’s die samenhangen met de door de dienstverlener gebruikte webapplicaties.

Daarbij kan bijvoorbeeld worden gedacht aan een dataclassificatieschema, waarin wordt bepaald welke mate van vertrouwelijkheid wordt toegekend aan bepaalde gegevens.

B.05 Contractmanagement

In sommigen gevallen besteedt een publieke dienstverlener beveiligingswerkzaamheden waarop deze regeling ziet uit. In dat geval wordt van de uitbestedende partij verwacht dat deze contractueel borgt dat de ingehuurde partij ook voldoet aan de relevante beveiligingseisen. Daarmee wordt het beveiligingsniveau ook gehandhaafd, wanneer de verantwoordelijkheid voor de ontwikkeling of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

TV.01 Toegangsvoorzieningsmiddelen

De publieke dienstverlener formuleert in het toegangsvoorzieningsbeleid richtlijnen voor de organisatorische en technische inrichting van de processen en middelen die noodzakelijk zijn voor de toegang en het gebruik van digitale overheidsdiensten. Hiermee wordt gerealiseerd dat de bevoegdheid van gebruikers kan worden aangetoond en dat zijn daadwerkelijk toegang kunnen krijgen tot de informatiesystemen waarvoor zij bevoegd zijn. Daarmee worden de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen die informatiesystemen gegarandeerd.

WA.02 Webapplicatiebeheer

De publieke dienstverlener richt het webapplicatiebeheer procesmatig en procedureel in, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. Op basis van taken, verantwoordelijkheden en bevoegdheden zijn de verschillende (beheer)rollen geïdentificeerd. Hiermee wordt voorkomen dat hiertoe niet geautoriseerde gebruikers toegang krijgen tot beheerfuncties binnen de applicatie.

WA.03 Webapplicatie-invoer

De publieke dienstverlener zorgt ervoor dat de mogelijkheid tot (on)opzettelijke manipulatie van de webapplicatie beperkt wordt, door voordat de invoer wordt verwerkt deze te normaliseren en te valideren. Denk hierbij bijvoorbeeld aan het converteren van alle invoer naar een veilig formaat of het weigeren van foute, ongeldige of verboden invoer. Hiermee wordt voorkomen dat de webapplicatie kan worden gemanipuleerd, waardoor de vertrouwelijkheid, integriteit of beschikbaarheid van de webapplicatie aangetast worden.

WA.04 Webapplicatie-uitvoer

Van publieke dienstverleners wordt verwacht dat zij de uitvoer die de door hen gebruikte webapplicatie kan verwerken normaliseren. Daarmee worden de mogelijkheden om het systeem te manipuleren beperkt.

WA.05 Betrouwbaarheid van gegevens

Van publieke dienstverleners wordt ook verwacht dat zij door toepassing van privacybevorderende en cryptografische technieken de betrouwbaarheid van opgeslagen en verzonden informatie garanderen. Dat kan bijvoorbeeld gebeuren door gevoelige gegevens in databases en bestanden te versleutelen.

PW.02 Webprotocollen

Manipulatie van de logica van de webserver of webapplicatie kan leiden tot wijziging of verlies van gegevens of onrechtmatige inzage daarvan. Om dat te voorkomen dient de publieke dienstverlener er zorg voor te dragen dat de inhoud van de protocollen aan specifieke kenmerken voldoet. Hierbij gaat het bijvoorbeeld om het beperken van ontvangen en verzonden informatie tot die informatie die voor het functioneren van de protocollen van belang is.

PW.03 Webserver

De publieke dienstverlener draagt er zorg voor dat ongewenste vrijgave van informatie tot een minimum wordt beperkt, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

PW.05 Toegang tot beheermechanismen

Een dienstverlener wordt geacht uitsluitend beveiligde protocollen te gebruiken voor toegang tot beheermechanismen. Verder gebruiken zij sterke authenticatiemethoden voor de toegang tot de beheermechanismen. Daarmee wordt misbruik van beheervoorzieningen voorkomen.

PW.07 Hardening van platformen

Een publieke dienstverlener beperkt de functionaliteit van het platform tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde diensten.

NW.03 Netwerkzonering

De publieke dienstverlener zorgt ervoor dat het netwerk is gescheiden in logische en fysieke domeinen, in het bijzonder tussen het interne netwerk en het internet. Hiermee wordt een beveiligde netwerkinfrastructuur geboden.

NW.04 Protectie- en detectiefunctie

De publieke dienstverlener beschermt netwerkcomponenten en het netwerkverkeer door middel van protectie- en detectiemechanismen. Zo wordt voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed, bijvoorbeeld door (d)DoS aanvallen.

NW.05 Beheer- en productieomgeving

De publieke dienstverlener voorkomt misbruik van de beheervoorzieningen vanaf het internet, door binnen de productieomgeving zijn beheer- en productieverkeer van elkaar af te schermen.

NW.06 Hardening van netwerken

Een publieke dienstverlener beperkt het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde diensten.

C.03 Vulnerability-assessments

De publieke dienstverlener identificeert de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie door middel van procesmatig en procedureel uitgevoerde vulnerability assessments. Hiermee worden risico's tijdig onderkend en tegengegaan.

C.04 Penetratietestproces

De publieke dienstverleners voeren penetratietests uit die zien op de voor de toegang relevante infrastructuur van de webapplicatie. Het uitvoeren van deze tests en opvolgen van de uitkomsten daarvan is procedureel en procesmatig geborgd in de organisatie.

Met de tests wordt inzicht verkregen in de weerstand die een webapplicatie biedt tegen pogingen om het te compromitteren en worden de kansen op het succesvol binnendringen of misbruiken van webapplicatie verkleind.

C.06 Logging

Het is noodzakelijk dat eventuele schendingen van functionele eisen en beveiligingseisen worden gedetecteerd, zodat vervolgens de juistheid van de uitgevoerde vervolgacties, zowel op strategisch als operationeel niveau, kunnen worden vastgesteld. In de webapplicatieomgeving moeten daarom effectieve, efficiënte en goed beveiligde signaleringsfuncties voor registratie en detectie van dergelijke schendingen zijn ingericht.

C.07 Monitoring

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

Het doorvoeren van wijzigingen in de toegangsvoorzieningen kan voor kwetsbaarheden zorgen. Daarom is het wenselijk dat dat dergelijke wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd. Van publieke dienstverleners wordt daarom vereist dat wijzigingenbeheer procesmatig en procedureel zodanig wordt uitgevoerd dat wijzigingen in de webapplicaties voor toegang tijdig, geautoriseerd en getest worden doorgevoerd.

C.09 Patchmanagement

Publieke dienstverleners dragen er zorg voor organisatorisch en procedureel is geborgd dat de meest actuele beveiligingsupdates zijn geïnstalleerd in de webapplicaties die nodig zijn voor toegang tot publieke diensten. Daarmee wordt zeker gesteld dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt.

Deze normen zijn overgenomen uit de voorwaarden die tot inwerkingtreding van deze regeling golden op basis van overeenkomsten tussen publieke dienstverleners en Logius voor het gebruik van DigiD. De normen zijn in de afgelopen jaren tot stand gekomen door overleg met betrokkenen en bestaat uit meerdere richtlijnen uit elk domein. Hiermee borgt het een goede verbinding van beleid, uitvoering en beheersing van de te nemen maatregelen op het gebied van informatieveiligheid. Met het overnemen in deze regeling worden in de inhoud van de normen geen wijzigingen aangebracht.

Met het steeds groter wordende belang van de digitale overheid, en een toenemende noodzaak voor het behouden van de informatieveiligheid geeft een toetsing op alleen opzet en bestaan niet meer afdoende betrouwbaarheid over de informatieveiligheid. Het toetsen op werking geeft een hogere betrouwbaarheid in de continuïteit van de informatieveiligheid. De volgende normen worden daarom ook op werking getoetst:

- U/TV.01 Toegangsvoorzieningsmiddelen
- U/WA.02 Webapplicatiebeheer
- C.07 Monitoring
- C.08 Wijzigingenbeheer
- C.09 Patchmanagement

4. Nadere eisen aan audits en auditverklaring

4.1 Audits

Deze regeling bevat nadere regels over de audits die publieke dienstverleners moeten uitvoeren op grond van artikel 4, tweede lid van de Wet digitale overheid. Deze audits moeten als gevolg van deze regeling betrekking hebben op de technische inrichting van een webapplicatie die wordt gebruikt om toegang te geven tot elektronische dienstverlening. Daarbij moeten ook aan derde partijen uitbesteedde werkzaamheden worden beoordeeld, voor zover die relevant zijn voor de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening.

Deze audit heeft betrekking op de koppeling van een identificatiemiddel met de webapplicaties van een aangesloten organisatie. Voor burgers en bedrijven wordt hiermee geborgd dat het gebruik van identificatiemiddelen veilig en betrouwbaar is. Een audit en de daarbij behorende auditverklaring verplichten publieke dienstverleners inzicht te geven in de informatieveiligheid van de toegang tot elektronische diensten.

Op grond van artikel 24 van het Besluit digitale overheid moeten audits worden uitgevoerd door een onafhankelijke en deskundige auditor. Deze regeling bepaalt dat daaraan in ieder geval is voldaan wanneer de audit wordt uitgevoerd door een EDP-registerauditor. Dat is een auditor die is ingeschreven bij de Nederlandse Orde van Register EDP-Auditors.

4.2 Auditverklaring

Deze regeling specificeert de eisen waaraan een auditverklaring moet voldoen. Een aantal eisen ziet op de wijze waarop de bevindingen en conclusies in de auditverklaring worden gepresenteerd. Zo schrijft de regeling onder meer voor dat bij het weergeven van de bevindingen en conclusies onderscheid moet worden gemaakt tussen de verschillende normen zoals die in de bijlage bij deze regeling zijn vastgesteld. Worden binnen een elektronische dienstomgevingen verschillende diensten aangeboden, dan moeten ook voor de verschillende diensten per norm de bevindingen en conclusies worden beschreven.

Artikel 3.3, tweede lid, biedt de mogelijkheid om een enkele auditsverklaring over te leggen indien verschillende publieke dienstverleners via dezelfde elektronische dienstenomgeving diensten aanbieden. Wanneer van die mogelijkheid gebruik wordt gemaakt moet in de auditverklaring worden onderbouwd dat sprake is van elektronische dienstomgevingen die op dezelfde wijze functioneren.

Verder moet worden onderbouwd dat de auditor die de audits uitvoert en die de auditverklaring heeft opgesteld, voldoet aan de eisen in artikel 24 van het Besluit digitale overheid. Dat besluit bepaald dat een auditor onafhankelijk en deskundig moet zijn. In deze ministeriële regeling is vastgelegd dat aan die eisen in ieder geval wordt voldaan door een NOREA-auditor die specifieke kennis heeft over de materie waarop deze regeling ziet.

4.2.2 Gezamenlijke auditverklaring

In bepaalde gevallen is het mogelijk om meerdere elektronische dienstomgevingen via een gezamenlijke audit te laten plaatsvinden. Dit kan in situaties waarin meerdere publieke dienstverleners gebruik maken van één ICT-leverancier die de publieke dienstverleners ontzorgt in het aansluiten en verantwoorden. Er worden enkele extra criteria gesteld, zoals dat de software en processen bij de verschillende publieke dienstverlener uniform worden toegepast. Daarvoor is het onder meer noodzakelijk dat publieke dienstverleners zelf geen mogelijkheden hebben om de werking van de software of ondersteunende processen te wijzigingen.

Een voorbeeld waarbij gebruik wordt gemaakt van een gezamenlijke auditverklaring is het platform ZorgDomein, dat voor verschillende huisartsen de elektronische dienstomgeving beheert en verantwoordt. ZorgDomein kan op grond van deze regeling namens alle aangesloten partijen een enkele auditverklaring aanleveren, indien wordt voldaan aan de eisen in deze regeling.

Hoewel een gezamenlijke auditverklaring meerdere voordelen oplevert voor de publieke dienstverlener (de organisatie ontzorgt hen echter zowel op technisch als administratief vlak), is het belangrijk te melden dat er extra eisen gelden voor zowel de organisatie als de publieke dienstverlener. Zo moeten alle elektronische dienstomgevingen die een gezamenlijke auditverklaring willen afleggen, onder andere, gebruik maken van hetzelfde platform van de organisatie en dezelfde functionaliteit daarvan gebruiken (maatwerk is niet toegestaan). Ook dient de organisatie die de gezamenlijke auditverklaring aflegt geaccrediteerd te zijn door Logius. Ten slotte is het belangrijk om te vermelden dat de publieke dienstverlener altijd eindverantwoordelijk is voor de elektronische dienstomgeving.

5. Uitvoering, toezicht en handhaving

De minister is verantwoordelijk voor het opstellen van de regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten. De minister heeft tevens de verantwoordelijkheid om toe te zien op de naleving van de in artikel 4 van de Wet digitale overheid opgestelde eisen. Op grond van artikel 17, vierde lid, van de Wet digitale overheid is Logius aangewezen om de naleving van de opgestelde regels te toetsen.

6. Regeldruk en administratieve lasten

Deze regeling bevat voorschriften die van toepassing zijn op organisaties die publieke diensten verlenen. Behalve bestuursorganen in de zin van artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht zijn dat onderwijsinstellingen, pensioenbeheerders en zorgverleners.

Deze partijen, zowel de bestuursorganen als de genoemde semi-overheidsinstanties, waren al gehouden om de in deze regeling opgenomen audits te laten uitvoeren. Ook de omvang van de audits en de eisen aan de rapportage wordt opgesteld wijzigen niet met deze regeling. Zoals in het

voorgaande is aangegeven wordt met deze regeling een bestaande privaatrechtelijke praktijk onder de Wet digitale overheid publiekrechtelijk vastgelegd. Daarom heeft deze regeling geen gevolgen voor de regeldruk voor deze organisaties.

7. Consultatie
[PM]

Artikelsgewijze toelichting

Artikel 1.1

Elektronische dienstenomgeving

Het begrip “elektronische dienstenomgeving” is van belang, omdat een publieke dienstverlener voor verschillende elektronische dienstenomgeving een separate auditverklaring moet aanleveren. In deze regeling wordt aangesloten bij de feitelijke inrichting van de elektronische dienstverleningsomgeving zoals die door een publieke dienstverlener wordt aangeboden. Daarbij geeft een inloghandeling met een authenticatie toegang tot een of meerdere diensten. Deze elektronische omgeving waartoe een authenticatie toegang geeft wordt in deze regeling aangemerkt als een elektronische dienstenomgeving. Een publieke dienstverlener kan dus meerdere elektronische dienstenomgeving hebben, wanneer sets met elektronische diensten zijn gegroepeerd in verschillende omgevingen en wanneer een separate authenticatie nodig is om bij een andere omgeving in te loggen.

Bij sommige dienstverleners is het mogelijk om met een “single sign on” toegang te krijgen tot verschillende omgevingen. Het kan bijvoorbeeld gaan om een gemeente die een elektronische omgeving heeft waarbinnen een parkeervergunning kan worden aangevraagd en een andere omgeving waarbinnen zaken met betrekking tot het socialezekerheidsrecht kunnen worden geregeld. Bij single sign on wordt het mogelijk om na een authenticatie voor een van deze omgevingen ook zonder nadere handeling toegang te krijgen tot de andere omgeving.

Toepassing van deze methode houdt echter niet in dat geen sprake is van een tweede authenticatie. De authenticatiehandeling wordt eenmalig uitgevoerd door de persoon die toegang probeert te krijgen en deze blijft gedurende een bepaalde periode geldig.

Bij het inloggen in een andere omgeving wordt op basis van de eerder uitgevoerde authenticatiehandeling opnieuw een authenticatieverklaring uitgegeven. Feitelijk is daarmee sprake van een separate, nieuwe authenticatie. Wanneer met single sign on toegang mogelijk is tot meerdere elektronische omgevingen is daarom ook sprake van meerdere elektronische dienstomgevingen, omdat in die gevallen telkens een (vereenvoudigde) authenticatie wordt uitgevoerd.

Artikel 2.1

Met dit artikel worden de ICT-beveiligingsnormen vastgesteld, waaraan een door publieke dienstverleners gebruikte webapplicatie moet voldoen. Deze normen zijn van toepassing op de beveiliging van de toegang van publieke dienstverlening. Het gaat dus om de systemen en processen die worden gebruik voor het inloggen, maar ook voor het informatieverkeer via de webapplicatie tussen de publieke dienstverlener en de persoon die gebruik maakt van de publieke dienst. In hoofdstuk 3 van deze toelichting wordt uitgebreid ingegaan op de inhoud van de ICT-normen.

De verplichting om aan deze normen te voldoen geldt voor bestuursorganen en aangewezen organisaties. Onder bestuursorganen worden, als gevolg van artikel 2, eerste lid van de wet, verstaan bestuursorganen in de zin van artikel 1:1, eerste lid, onderdeel a van de Algemene wet bestuursrecht (de zogenaamde a-organen).

Op grond van artikel 1 van de wet is een “aangewezen organisatie” een organisatie “als bedoeld in artikel 2, tweede lid” van de wet. Het betreft organisaties die zijn genoemd in de bijlage bij de wet (instellingen voor hoger onderwijs, pensioenuitvoerders en bepaalde zorgaanbieders) en organisaties die bij ministerieel besluit zijn aangewezen. Omdat de begripsbepaling in de wet geldt voor de wet en “daarop berustende bepalingen” is deze ook in deze regeling van toepassing.

Artikel 3.1

In dit artikel wordt bepaald waarop een audit moet zien. Het eerste lid schrijft voor dat een audit ziet op de vraag of een publieke dienstverlener voldoet aan de normen in artikel 2.1. Voor al deze normen moet enkel het bestaan en de opzet van genomen maatregelen worden onderzocht. Voor sommige normen, namelijk de normen “U/TV.01”, “U/WA.02”, “C.07”, “C.08”en “C.09” wordt ook op de werking in de praktijk getoetst. Dat is vastgelegd in het tweede lid van artikel 2.1.

In het derde lid wordt geregeld dat ook moet worden gerapporteerd over processen en maatregelen die onder de rapportageplicht vallen wanneer deze werkzaamheden zijn uitbesteed aan een derde partij.

Artikel 3.2

Artikel 24 van het Besluit digitale overheid bepaalt dat een audit en de verklaring moet worden uitgevoerd en opgesteld “door een onafhankelijke en gekwalificeerde auditor”. In artikel 3.2 van deze regeling is vastgelegd dat daarvan in ieder geval sprake is wanneer een register EDP-auditor deze werkzaamheden uitvoert. Dat is een auditor die is geregistreerd bij de Nederlandse Orde van Register EDP-Auditors. Wanneer de audit niet is uitgevoerd door een EDP-auditor zal moeten worden gemotiveerd dat de uitvoerende auditor voldoet aan de geldende algemene eisen van onafhankelijkheid en deskundigheid die op grond van artikel 24 van het Besluit digitale overheid van kracht zijn.

Artikel 3.3

<u>Eerste lid</u>

Per elektronische dienstomgeving moet een auditverklaring worden aangeleverd. In de toelichting bij artikel 1.1 wordt uitvoerig ingegaan op het begrip “elektronische dienstomgeving”.

<u>Tweede lid</u>

Het tweede lid van dit artikel regelt dat voor diensten die door verschillende publieke dienstverleners worden aangeboden binnen dezelfde elektronische ruimte ook kan worden volstaan met een enkele auditverklaring. Daarvan kan bijvoorbeeld sprake zijn wanneer een gemeente binnen een elektronische dienstomgeving diensten aanbiedt van het college van burgemeester en wethouders en van de gemeenteraad. Op het terrein van het omgevingsrecht zal hiervan in sommige gevallen sprake zijn.

Artikel 3.4

Tweede lid

Op grond van dit artikellid kan een model worden vastgesteld voor de auditrapportage. Dit lid maakt het mogelijk om voor verschillende toepassingen verschillende modellen toe te passen.

Artikel 3.5

Met dit artikel worden regels gesteld aan over de audit die aan de rapportage ten grondslag ligt. Het eerste lid bevat de hoofdregel, namelijk dat de audit niet eerder dan 31 december van het jaar voor het jaar waarop de rapportage ziet mag zijn uitgevoerd. Een uitzondering, geregeld met het tweede lid, is wanneer werkzaamheden zijn uitbesteed. In dat geval mag voor die werkzaamheden de rapportage worden gebaseerd op een andere auditrapportage over die werkzaamheden die niet ouder is dan 12 maanden. Die twaalf maanden worden berekend vanaf het moment van indiening.

Deze regels zien op het moment van het uitvoeren van een audit. In sommige gevallen worden voor een audit bijvoorbeeld logboeken gebruikt met gegevens van een eerder moment. Daar staat deze regeling niet aan in de weg.

Artikel 4.1 en 4.2

Deze artikelen regelen dat het mogelijk is om in bepaalde gevallen en gezamenlijke auditverklaring in te dienen. Op de inhoud van deze artikelen wordt ingegaan in paragraaf 4.2.2 van het algemene deel van deze toelichting.