Rijksoverheid

Handreiking

Verplichte richtlijnen websites en andere online middelen

De rijksoverheid kent diverse richtlijnen voor online middelen (websites, portalen, apps etc). Deze zijn te vinden op www.forumstandaardisatie.nl en www.eisenrijkswebsites.nl. Naast verplichte richtlijnen, zijn er ook aanbevolen richtlijnen en richtlijnen voor dienstverlening. De verplichte richtlijnen zijn gericht op veiligheid, bescherming persoonsgegevens, toegankelijkheid en transparantie, en vormen een minimumeis voor oplevering van webproducten. In deze factsheet zijn de verplichte richtlijnen voor rijkswebsites beschreven in een SMART eisenpakket voor aanbestedingen, en de toetsing ervan door de opdrachtgevers en opdrachtnemers.

Afwegingskader online middelen

In juli 2018 is in de voorlichtingsraad het afwegingskader online middelen vastgesteld. Wie namens de rijksoverheid een online middel wil inzetten, bespreekt dit eerst met de directie communicatie van zijn eigen ministerie. De directie toetst elke aanvraag aan het afwegingskader online middelen. Voor het lanceren van een nieuw online middel wordt als basis uitgegaan van het platform rijksoverheid (PRO) dat aan alle richtlijnen voldoet. PRO wordt kosteloos beschikbaar gesteld en dienstonderdelen worden met het platform blijvend ontzorgd. Alleen als PRO onvoldoende uitkomst biedt kan worden afgeweken van deze lijn. Na besluit kan een aanbesteding worden gestart. Ook voor het aanbesteden van online middelen gelden dezelfde eisen.

Onderstaande tabel geeft een overzicht van alle verplichte richtlijnen voor online middelen en een vertaling in eisen voor toevoeging aan een programma van eisen. In de laatste kolom is een voorbeeld opgenomen van de wijze waarop verificatie van de eis kan plaatsvinden. De eisen kunnen zowel voor de opdrachtnemer als opdrachtgever van toepassing zijn en gelden gedurende de looptijd van de opdracht. Enkele richtlijnen gelden alleen in een aantal concrete situaties (zwart onderstreept) en het is aan de opdrachtgever te bepalen of deze van toepassing zijn bij een aanbesteding. Achter de hyperlinks is meer informatie over de richtlijnen te vinden.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
Domeinnaambeleid	Voor domeinnamen van de rijksoverheid bestaan afspraken over het claimen van domeinnamen voor online middelen. Deze zorgen voor eenduidigheid, transparantie, kostenbeheersing en bescherming van de juridische positie. De Dienst Publiek en Communicatie (DPC) is registrar en houder van alle domeinnamen van de rijksoverheid. De vindbaarheid van het domein kan worden bevorderd door SEO en eventueel SEA.	De opdrachtnemer/-gever vraagt via de communicatie liaison van het ministerie een domeinnaam -die voldoet aan het domeinnaambeleid- aan bij de Dienst Publiek en Communicatie (DPC). Er worden geen domeinnamen defensief geclaimd. Afhankelijk van de doelgroep wordt een .nl, .eu of .com domein geclaimd.	Bij oplevering van het online middel wordt slechts één domeinnaam door de opdrachtgever gehanteerd en deze dient de extensie .nl, .eu of .com te hebben. Afwijkingen dienen te worden gesaneerd.
Websiteregister Rijksoverheid	In het websiteregister rijksoverheid staan alle websites van de rijksoverheid, hoe vaak de website gemiddeld per maand is bezocht en het voldoen aan de verplichte richtlijnen.	De opdrachtnemer/-gever draagt er via de communicatie liaison van het ministerie zorg voor dat het online middel in het websiteregister wordt opgenomen. De opdrachtnemer/-gever vraagt daarnaast via de communicatie liaison van het ministerie aansluiting op de webanalysetool aan en draagt er zorg voor dat bezoekersaantallen met volledig werkende ondersteuning worden gemeten.	De opdrachtgever toetst na oplevering of het online middel is opgenomen in het websiteregister en de bezoekersaantallen correct worden geregistreerd in de door AZ/DPC aangeboden webanalysetool.
Baseline Informatiebeveiliging Overheid (BIO) & ISO 27001 en 27002	De Baseline informatiebeveiliging Overheid (BIO) biedt een normenkader voor de beveiliging van de informatiehuishouding van de rijksoverheid. Hierdoor is het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen.	De opdrachtnemer biedt **bij uitwisseling van data** een managementsysteem voor informatie-beveiliging bij het te leveren online middel conform de open standaard ISO 27001 of daaraan gelijkwaardig. De opdrachtnemer heeft **bij uitwisseling van data** voor het te leveren online middel beheers-maatregelen op het gebied van informatiebeveiliging in werking die zijn gebaseerd op de open standaard ISO 27002 of daaraan gelijkwaardig.	• Akkoordverklaring door de opdrachtgever met toelichting hoe wordt geborgd dat het online middel aan de standaard voldoet. • ISO 27001 certificaat voor het online middel verstrekt door een RvA-geaccrediteerde organisatie, of een gelijkwaardig certificaat. Akkoordverklaring door de opdrachtgever met toelichtende beschrijving van getroffen beheersmaatregelen in relatie tot ISO 27002 of daaraan gelijkwaardig.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
ICT beveiligingsrichtlijnen voor webapplicaties	De ICT beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC) zijn criteria voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. Deze richtlijnen zijn een verdieping van de Baseline Informatiebeveiliging Overheid (BIO).	De opdrachtnemer draagt zorg dat het online middel voldoet aan de richtlijnen ICT beveiligingsrichtlijnen voor webapplicaties en toont dat aan. De basis voor de beveiliging is gelegen in de BIO.	De opdrachtgever verricht na oplevering een acceptatietest om te beoordelen of voor het online middel daadwerkelijk deze beveiligings-maatregelen zijn genomen.
Webarchivering	Rijksoverheidswebsites zijn officiële publicaties en portalen bieden officiële dienstverlening. De rijksoverheid is verantwoordelijk voor het archiveren van deze online middelen, zodat deze nu en in de toekomst te gebruiken zijn voor verschillende doeleinden en door verschillende doelgroepen.	De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor dagelijks archiveren **bij websites met platte content**. In de *footer* dient een verwijzing naar het archief te worden opgenomen.	De opdrachtgever verricht na oplevering een acceptatietest om te beoordelen of het online middel daadwerkelijk volgens deze afspraken archiveert naar de centrale archiefservice van de rijksoverheid (momenteel archiefweb.eu).
Overheid.nl Web Metadata Standaard (OWMS)	De Overheid.nl Web Metadata Standaard (OWMS) is de metadata-standaard voor informatie van de Nederlandse overheid op internet. De standaard is gebaseerd op de internationale metadatastandaard van het Dublin Core Metadata Initiative (DCMI).	De opdrachtnemer biedt op het online middel volledig werkende ondersteuning om het publiceren van webcontent (webpagina's, documenten, audiovisuele content) te voorzien van metadata die voldoet aan de OWMS-standaard versie 4.0.	De opdrachtnemer dient een akkoordverklaring op te leveren met een toelichting hoe wordt geborgd dat het online middel aan deze standaard voldoet. Bij oplevering wordt de correcte werking getest o.a. aan de hand van de XML-schemadefinitie van OWMS versie 4.0.
Basiswettenbestand (BWB)	De open standaard BWB biedt een eenduidige manier van verwijzen naar (onderdelen van) wet- en regelgeving. De actuele versie maakt het mogelijk om in wet- en regelgeving te kunnen verwijzen naar: - taalversies en onderdelen van internationale verdragen, - wet- en regelgeving waarvan de indeling niet voldoet aan de gebruikelijke nummering van hoofdstukken en paragrafen, en - ruime begrippen zoals "enig artikel". De verplichting geldt voor internet- en webservices met juridische documenten en systemen die (veel) verwijzingen kennen naar wet- en regelgeving.	De opdrachtnemer heeft **bij gebruik van wet- en regelgeving** op het online middel een verwijzing naar de actuele versie van de open standaard Basiswettenbestand geïmplementeerd op het online middel.	Akkoordverklaring door de opdrachtgever met toelichtende beschrijving van getroffen beheersmaatregelen in relatie tot verwijzing naar het BWB bij gebruik van wet- en regelgeving.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
HTTPS, TLS & certificaten	HTTPS, TLS & Certificaten kunnen als een drie-eenheid worden gezien. HTTPS (Hyper Text Transfer Protocol Secure) verschijnt in de URL wanneer een website is beveiligd met een TLS certificaat. TLS staat voor Transport Layer Security. TLS zorgt ervoor dat de data die verstuurd wordt tussen de gebruiker en de website of tussen systemen onderling wordt versleuteld en zo onleesbaar wordt gemaakt. De rijksoverheid geeft PKIoverheid certificaten onder eigen beheer uit (zogenaamde Extended Validation), waardoor er controle is op de kwaliteit van het certificaat. PKIoverheid Extended Validation is, hoewel niet verplicht, het meest veilige certificaat.	De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor beveiligde verbindingen conform TLS (versie 1.0 - 1.3). Dit betekent dat: 1. Er een geldig (PKIoverheid-) certificaat is geïnstalleerd op het online middel 2. Op basis waarvan andere systemen een TLS-verbinding kunnen opzetten met het online middel 3. Waarvan de veiligheid van de TLS-configuratie voldoet aan de ICT-beveiligingsrichtlijnen voor TLS van NCSC	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de web- en mailtest op www.internet.nl.
Qualified Website Authentication Certificates	Op 1 juli 2016 Europese is wetgeving in werking getreden over onder meer certificaten voor authenticatie van websites. De verordening regelt de wederzijdse erkenning tussen de lidstaten van elektronische handtekeningen – zegels, -tijdstempels, - diensten voor aangetekende elektronische bezorging en certificaten voor de authenticatie van websites. Deze worden samen vertrouwensdiensten genoemd. Daarnaast regelt de verordening de erkenning van elektronische identiteiten, zoals DigiD en eHerkenning.	De opdrachtnemer levert het online middel met een Qualified Website Authentication Certificate. De opdrachtnemer/opdrachtgever draagt er via de liaison van het ministerie zorg voor dat het online middel een extended validation ontvangt op het webdomein.	De opdrachtgever toetst na oplevering en vervolgens per kwartaal of de opdrachtnemer het certificaat heeft geïmplementeerd (zichtbaar en werkend als Rijksoverheid certificaat in de adresbalk in de browser).
Domain Name System Security Extensions (DNSsec)	DNSsec is een uitbreiding op het Domain Name System (DNS). Het verhelpt een aantal kwetsbaarheden in DNS. Hierdoor wordt de 'bewegwijzering' van het internet veiliger en vertrouwder.	De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor DNSsec. Domeinnaam-informatie, zoals bijbehorende IP-adressen, zijn met een geldige DNSsec-handtekening ondertekend.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de web- en mailtest op www.internet.nl.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
DMARC	DMARC is een standaard voor het veiliger maken van e-mail verkeer door het tegengaan van spam en phisingmail door misbruik van domeinnamen bij e-mail te voorkomen. Deze richtlijn geldt voor uitgaande en inkomende e-mail en in domeinnaamsystemen (DNS).	De opdrachtnemer biedt **bij toepassen van mail** op het online middel volledig werkende ondersteuning voor DMARC. Beter is het de mailfunctie op het domein uit te schakelen (no_mail) wanneer geen gebruik wordt gemaakt van mail.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op www.internet.nl.
Domain Keys Identified Mail (DKIM)	DKIM koppelt e-mail aan een domeinnaam met behulp van een digitale handtekening. Hierdoor kan de ontvanger zien welke domeinnaam en achterliggende organisatie verantwoordelijk is voor het zenden van de e-mail. Spam- en phishingmails kunnen daardoor beter worden gefilterd.	De opdrachtnemer biedt **bij toepassen van mail** op het online middel volledig werkende ondersteuning voor DKIM. Dit betekent dat: 1. Op het systeem een publiek/privaat sleutelpaar is gegenereerd of kan worden gegenereerd; 2. De publieke DKIM-sleutel is gepubliceerd in de DNS van de e-maildomeinnaam; 3. Alle uitgaand e-mailberichten worden ondertekend met de private DKIM-sleutel; 4. Alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van een eventuele DKIM-handtekening en het systeem hieraan mogelijke acties verbindt. Beter is het de mailfunctie op het domein uit te schakelen (no_mail) wanneer geen gebruik wordt gemaakt van mail.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op www.internet.nl.
Sender Policy Framework (SPF)	Sender Policy Framework (afgekort SPF) is een protocol dat tot doel heeft te helpen spam te verminderen, door vast te stellen of de verzender van een mailbericht gerechtigd is om een bericht te verzenden namens de afzender van het bericht.	De opdrachtnemer biedt **bij toepassen van mail** op het online middel volledig werkende ondersteuning voor SPF. Dit betekent dat: 1. IP-adressen van de verzendende systemen als SPF-record worden geregistreerd in de DNS van de verzendende domeinnaam; 2. Alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van het verzendend IP-adres tegen het IP-adres dat in SPF-record staat van de verzendende domeinnaam. Beter is het de mailfunctie op het domein uit te schakelen (no_mail) wanneer geen gebruik wordt gemaakt van mail.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op www.internet.nl.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
STARTTLS en DANE	STARTTLS in combinatie met DANE gaan het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen.	De opdrachtnemer biedt **bij toepassen van mail** op het online middel volledig werkende ondersteuning voor STARTTLS (SMTP over STARTTLS, oftewel ESMTPS) in combinatie met DANE. Verzendende mailservers kunnen daarmee een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) opzetten. Dit voorkomt dat aanvallers het mailverkeer kunnen afluisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers). Beter is het de mailfunctie op het domein uit te schakelen (no_mail) wanneer geen gebruik wordt gemaakt van mail.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op www.internet.nl.
Toegankelijkheid (EN301549 en WCAG2.1)	EN301549 is een Europese toegankelijkheidsstandaard die omschrijft aan welke eisen een (web) toepassing moet voldoen om toegankelijk te zijn voor mensen met een functiebeperking. Voor webcontent verwijst EN301549 naar een andere internationale standaard: WCAG 2.1 van het World Wide Web consortium (W3C).	De opdrachtnemer zorgt ervoor dat het online middel minimaal voldoet aan de open standaard Toegankelijkheid (WCAG2.0).	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis, bijv. op paginaniveau met Achecker of op siteniveau met Powermapper.
Internet Protocol versie 6 (IPv6)	Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder systeem binnen het netwerk een uniek nummer (IP-adres) heeft. De belangrijkste motivatie voor de ontwikkeling van IPv6 was het vergroten van de hoeveelheid beschikbare adressen ten opzichte van de voorganger IPv4.	De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor IPv4 én IPv6 (dual stack). Dit betekent in ieder geval dat gebruikers online middelen kunnen bezoeken, e-mail kunnen verzenden en ontvangen, en andere systemen kunnen bereiken via IPv4 en via IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de web- en mailtest op www.internet.nl.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
Portable Document Format (PDF)	PDF is een formaat voor de uitwisseling van documenten waarvan de pagina opmaak vastligt. Het uitgangspunt van PDF is dat gebruikers documenten kunnen uitwisselen, bekijken en afdrukken, onafhankelijk van de omgeving waarin ze worden aangemaakt, bekeken of afgedrukt.	De opdrachtgever biedt op het online middel volledig werkende ondersteuning voor het genereren, en/of beheren, en/of publiceren van documenten in duurzaam toegankelijke PDF formaat.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis, bijv. met Powermapper.
Rijkshuisstijl Online	Rijkshuisstijl Online is een uniforme vormgeving voor de herkenbaarheid en positionering van de Rijksoverheid. Afhankelijk van de afspraken met het ministerie kan een dienstonderdeel afwijken van de rijkshuisstijl. Ook voor campagnes kan in overleg met het ministerie worden afgeweken van de rijkshuisstijl.	De opdrachtnemer past **zo nodig** alle rijkshuisstijl onderdelen die van toepassing zijn op het online middel toe, conform de eisen op de website www.rijkshuisstijl.nl.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis.
Security Assertion Markup Language (SAML)	De Security Assertion Markup Language (SAML), is een XML-gebaseerd raamwerk voor het communiceren van gebruikers authenticatie, rechten, en attribuut informatie. SAML biedt organisatie entiteiten de mogelijkheid om claims te maken over de identiteit, attributen en rechten van een subject (een entiteit welke vaak een menselijke gebruiker is) aan andere entiteiten zoals Internet applicaties of diensten.	De opdrachtnemer biedt **bij toepassen van een inlog** op het online middel volledig werkende ondersteuning voor SAML versie 2.0, zodat gebruikers via eenmalig in- en uitloggen veilige toegang hebben tot verschillende gekoppelde webdiensten. Daarbij hoort het succesvol doorlopen en aantonen van Interoperability Certification Program van Kantara of vergelijkbaar. Voorbeelden van SAML toepassingen voor overheidsdiensten aan burgers en bedrijfsleven zijn DigiD, eHerkenning en eIDAS.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis.
Telecommunicatiewet (Cookiewet)	Volgens de cookiebepaling in de Telecommunicatiewet moet de website haar bezoekers informeren en toestemming krijgen voor het gebruik van cookies. Dit geldt ook voor andere methodes van informatie wegschrijven	De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor functionele/webanalyse cookies die voldoen aan de Telecommunicatiewet.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, bijv. met de Ghostery plugin of app. Er dient geen gebruik te worden gemaakt van third party cookies, enkel van webanalyse cookies.

Naam richtlijn	Toelichting op richtlijn	Eis	Verificatie van de eis
Algemene Verordening Gegevensbescherming	Voor sommige diensten van de rijksoverheid zijn persoonsgegevens van burgers nodig. Maar de burger heeft het recht op privacy en bescherming van zijn gegevens. Daarom zijn dienstverleners verplicht om persoonsgegevens goed te beschermen. En ze alleen te verwerken als ze daar een goede reden voor hebben.	De opdrachtgever dient **bij toepassen van persoonsgegevens** op het online middel te garanderen dat het online middel en opdrachtgever voldoet aan de vereisten van de Algemene Verordening Gegevensbescherming. De opdrachtgever bepaalt de classificatie van persoonsgegevens en bepaalt wat passende technische- en organisatorische maatregelen zijn. De opdrachtnemer neemt deze passende maatregelen ter bescherming van de persoonsgegevens. De opdrachtgever sluit met de opdrachtnemer een verwerkersovereenkomst (zie bijlage 1, Handreiking), waarbij afspraken worden gemaakt over de verantwoording bijv. mogen uitvoeren van audits bij de opdrachtnemer, TPM verklaring. De opdrachtgever blijft verantwoordelijk voor de naleving van de AVG en dient maatregelen te nemen zoals opname in AVG register of het verrichten van een DPIA.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis en de genomen maatregelen. De opdrachtgever heeft daarnaast met de opdrachtnemer een verwerkersovereenkomst afgesloten.
Wet hergebruik overheidsinformatie	In 2015 is de Wet hergebruik van overheidsinformatie (Who) in werking getreden. Burgers en bedrijven kunnen een verzoek indienen tot het verstrekken van overheidsinformatie. Deze informatie kan worden gebruikt door natuurlijke personen of rechtspersonen voor commerciële of niet-commerciële doeleinden. Het voornaamste doel daarbij is het creëren van economische meerwaarde	De opdrachtnemer en opdrachtgever dragen er zorg hergebruik van overheidsinformatie wordt toegepast op het online middel, en neemt daartoe passende technische- en organisatorische maatregelen.	De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis.

Dit is een uitgave van de
Rijksoverheid
Postbus 20350 | 2511 vx Den Haag
www.rijksoverheid.nl
September 2019