



De volgende open standaarden zijn in ieder geval van toepassing:

Digitoegankelijk (EN 301 549 met WCAG 2.1) (verplicht)

Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor mensen met permanente, tijdelijke of situationele functiebeperkingen. Zo krijgt iedereen dezelfde toegang tot overheidsinformatie.

Let op: per 1 juli 2018 zijn overheidsorganisaties wettelijk verplicht om Digitoegankelijk (EN 301 549 en WCAG 2.1) te gebruiken voor de toegankelijkheid van websites en mobiele applicaties. Kijk voor [meer informatie](#).

<https://www.forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21>

DKIM (verplicht)

DKIM faciliteert van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt.

<https://www.forumstandaardisatie.nl/open-standaarden/dkim>

DMARC (verplicht)

DMARC is een standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het eigen domein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie.

<https://www.forumstandaardisatie.nl/open-standaarden/dmarc>

DNSSEC (verplicht)

DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren. <https://www.forumstandaardisatie.nl/open-standaarden/dnssec>

HTTPS en HSTS (verplicht)

HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser).

Let op: per 1 juli 2023 zijn overheidsorganisaties wettelijk verplicht om HTTPS en HSTS te gebruiken voor beveiligen van publiek toegankelijke websites en webapplicaties. Kijk voor [meer informatie](#).

<https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts>

IPv6 en IPv4 (verplicht)

IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren. <https://www.forumstandaardisatie.nl/open-standaarden/ipv6-en-ipv4>

security.txt (verplicht)

security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is. <https://www.forumstandaardisatie.nl/open-standaarden/securitytxt>

SPF (verplicht)

Met SPF kan worden gecontroleerd of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden. <https://www.forumstandaardisatie.nl/open-standaarden/spf>

STARTTLS en DANE (verplicht)

STARTTLS in combinatie met DANE gaan af luisteren of manipuleren van mailverkeer door internetcriminelen tegen. <https://www.forumstandaardisatie.nl/open-standaarden/starttls-en-dane>

TLS (verplicht)

TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

<https://www.forumstandaardisatie.nl/open-standaarden/tls>



De volgende open standaarden zijn **mogelijk van toepassing**:

BWB (mogelijk relevant)

BWB biedt een eenduidige manier van elektronische verwijzingen naar geconsolideerde wetten en regelingen of delen daarvan, waarmee het citeren, vinden en verbinden van wet- en regelgeving sneller en eenvoudiger is en minder kans op fouten geeft. <https://www.forumstandaardisatie.nl/open-standaarden/bwb>

Geo-Standaarden (mogelijk relevant)

Geo-standaarden voorzien in uitwisseling van geografische informatie tussen organisaties, waarbij de ruimtelijke dimensie van significant belang is. <https://www.forumstandaardisatie.nl/open-standaarden/geo-standaarden>

JCDR (mogelijk relevant)

JCDR moet worden toegepast op elektronische verwijzingen naar decentrale regelgeving. De standaard beschrijft hoe dient te worden verwezen naar documenten die in de Centrale Voorziening Decentrale Regelgeving zijn opgeslagen. <https://www.forumstandaardisatie.nl/open-standaarden/jcdr>

NEN-ISO/IEC 27001 (mogelijk relevant)

NEN-ISO/IEC 27001 specificeert de eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

Gebruik de [ICO Wizard](#) om uw eisenpakketten te selecteren die passen bij de producten/diensten die u aanbesteedt. De ICO-Wizard bevat een uitgebreid pakket van informatiebeveiligingseisen die een rol spelen bij aanbestedingen en inkopen. Met behulp van selectievelden kunnen eisenpakketten worden geselecteerd die passen bij specifieke inkoopsegmenten of combinaties daarvan, en kunnen nadere verfijningen daarop worden toegepast. De eisen in de Wizard zijn gebaseerd op een stevig fundament dat is ontleend aan de markstandaard ISO27002. <https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27001>

NEN-ISO/IEC 27002 (mogelijk relevant)

NEN-ISO/IEC 27002 omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

ICO Wizard (mogelijk relevant)

Gebruik de [ICO Wizard](#) om uw eisenpakketten te selecteren die passen bij de producten/diensten die u aanbesteedt. De ICO-Wizard bevat een uitgebreid pakket van informatiebeveiligingseisen die een rol spelen bij aanbestedingen en inkopen. Met behulp van selectievelden kunnen eisenpakketten worden geselecteerd die passen bij specifieke inkoopsegmenten of combinaties daarvan, en kunnen nadere verfijningen daarop worden toegepast. De eisen in de Wizard zijn gebaseerd op een stevig fundament dat is ontleend aan de markstandaard ISO27002. <https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27002>

NL GOV Assurance profile for OAuth 2.0 (mogelijk relevant)

NL GOV Assurance profile for OAuth 2.0 zorgt ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige plaats vindt. <https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20>

ODF (mogelijk relevant)

<https://www.forumstandaardisatie.nl/open-standaarden/odf>

**OpenAPI Specification (mogelijk relevant)**

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. Met OAS 3.0 kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de programmatuur en zonder aanvullende documentatie.

<https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification>

PDF (NEN-ISO) (mogelijk relevant)

<https://www.forumstandaardisatie.nl/open-standaarden/pdf-nen-iso>

REST-API Design Rules (mogelijk relevant)

De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt ten behoeve van het ontsluiten van

overheidsinformatie en/of functionaliteit. <https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules>