

BIJLAGE F Standaarden

Inhoudelijke standaarden

NEN-ISO 15489-1(:2016 NL)

NEN-ISO 15489-1 beschrijft in algemene termen de concepten en uitgangspunten voor het werken met informatie- en archiefmanagement.

NEN-ISO 16175(-1&2:2020 NL)

NEN-ISO 16175 biedt principes en functionele eisen voor software om digitale informatie te creëren en te beheren in kantooromgevingen.

NEN-ISO 23081-1(:2017 NL)

NEN-ISO 23081-1 beschrijft het beheren van metadatagegevens voor archiefbescheiden. Deze principes zijn door de tijd van toepassing op:

- Archiefbescheiden en de bijbehorende metagegevens;
- Alle processen die hierop van invloed zijn;
- Elk systeem waarin ze huizen;
- Elke organisatie die verantwoordelijk is voor het beheer van deze archiefbescheiden en de bijbehorende metagegevens.

ISO 26122(:2008 EN)

ISO 26122 biedt richtlijnen bij de analyse van werkprocessen vanuit het perspectief van het maken, vastleggen en controleren van records. Dit zowel op functioneel gebied door opdeling in processen als op volgorde van processtappen.

NEN-ISO 30300(:2020 EN)

NEN-ISO 30300 definieert de begrippen die toepasbaar zijn op managementsystemen voor archiefbescheiden. De norm bevat grondbeginselen en een verklarende woordenlijst.

NEN 2084(:2015 NL)

NEN 2084 geeft een structuur van een taxonomie van documenttypen. Voor Inholland hebben we op basis van de structuur van NEN 2084 onze documenttypen in een taxonomie vastgelegd. Zie 'Bijlage H Structuur van de taxonomie'.

Standaarden vanuit Forum Standaardisatie

Naast de inhoudelijke standaarden zijn wij als semipublieke instelling gedeeltelijk gehouden aan het volgen van de standaarden zoals vermeld op de pas-toe-of-leg-uit-lijst van Forum Standaardisatie. De standaarden die voor deze aanbesteding daarbij als relevant zijn bevonden zijn hieronder weergegeven. Een aantal zaken hierin zijn zeer specifiek voor overheden, maar de achterliggende technieken en doelen zijn dan nog steeds van toepassing voor Inholland.

DNSSEC

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>

IPv6 en IPv4

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>

NEN-ISO/IEC 27001

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

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

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

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>

OpenAPI Specification

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)

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

REST-API Design Rules

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>

RPKI

Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routing vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routing negeren.

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

SAML

SAML standaardiseert federatieve (web)browser-gebaseerde single-sign-on (SSO). Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.

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

TLS

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>