



Rijksoverheid



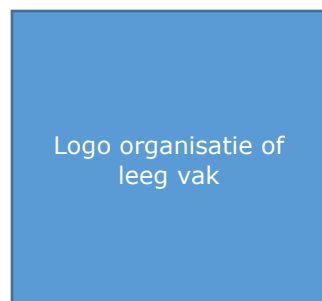
Inter provinciaal Overleg



UNIE VAN
WATERSCHAPPEN

Bijlage 18 ICO-report voorwaarden maatwerkpakket

Selectie Inkoop-eisen Cybersecurity Overheid



Logo organisatie of
leeg vak

Samengesteld door
Organisatie

RVO

Datum

22-2-2021

Inleiding

De steeds toenemende digitalisering en daarin meekomende risico's op diefstal en misbruik van gegevens maakt het noodzakelijk om voortdurend te blijven werken aan informatieveiligheid. De overheid hanteert daarbij als gezamenlijk kader de [Baseline Informatiebeveiliging Overheid](#) (BIO). Naast maatregelen die de organisaties zelf betreffen, moeten ook inkopen en uitbestedingen voldoen aan veiligheidseisen.

De overheid wil met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en diensten stimuleren. In de eerste plaats omdat zij zelf veilig moet zijn, maar ook kan zij als belangrijke gebruiker van ICT-diensten bredere impact creëren. Door cybersecuritycriteria op te nemen in aanbestedingen, inkopen en contracten wil de overheid nadrukkelijk sturen op de veiligheid van haar eigen uitbestedingen en daarnaast een proces stimuleren dat leidt tot een algemene verhoging van de veiligheid van ICT-middelen in de markt.

Dit rapport geeft de veiligheidseisen weer van een of meer opgegeven inkooponderdelen.

Deze eisen zijn gericht op basisbeveiligingsniveaus (BBN) 1 en 2 van de BIO. Hogere beveiligingsniveaus zijn altijd maatwerk. Het gebruik van de ICO-hulpmiddelen is geen substituuut voor eigen risicoafweging.

Op basis van risicoafwegingen van de behoeftesteller kunnen eisen worden geschrapt, verzacht of verzaamd. Dit blijkt uit de eventueel bij de eisen gemaakt opmerkingen.

Selectiecriteria

De volgende criteria zijn van toepassing voor de selectie van inkoop-eisen.

Inkooponderdelen	Maatwerk of maatwerkpakket
Proceseis	nee
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Eisen meenemen die te maken hebben met louter schaalgrootte	nee
Prioriteit	hoog
Aantal geselecteerde eisen	27

De eisen op de volgende pagina's zijn gebaseerd op de BIO en onderliggende uitwerkingen. Bij elk van de eisen is aangegeven uit welk brondocument die afkomstig is en onder welke code die daarin voorkomt. Hieronder staan de links naar de vindplaatsen van de brondocumenten. Daarin is per eis een nadere specificatie opgenomen.

[Applicatieontwikkeling algemeen](#)

[Clouddiensten](#)

[Communicatievoorzieningen](#)

[DIGID Applicaties](#)

[Huisvesting IV](#)

[Maatwerk of maatwerkpakket](#)

[Mobiele Applicaties](#)

[Server-platform](#)

[Toegangsbeveiliging](#)

Per 22 juli 2020 is SSD-versie 3 de basis voor het onderdeel maatwerk en maatwerkapplicaties. Eisen voor dit onderdeel die voor deze datum zijn geselecteerd met de ICO-wizard, zijn gebaseerd op de versie SSD2.0. Deze kan [hier](#) worden bekeken.

Disclaimer:

De inkoop-eisen op de navolgende pagina's zijn samengesteld op basis van de bovenaan deze pagina ingevoerde criteria. De eisen en selecties die toegepast zijn, steunen op een proces van intensieve en brede, interbestuurlijke samenwerking. Het kan echter voorkomen dat er toch sprake is van omissies of onjuistheden. Het is de verantwoordelijkheid van de gebruiker zelf te beoordelen, mede in het licht van zijn eigen risicoafweging, of behoefte bestaat aan wijziging van de eisen in het rapport.

De eisen die wettelijk vanuit de AVG zijn opgesteld en van belang zijn bij een inkooptraject, blijven onverminderd van kracht.

Geselecteerde inkoop Eisen

Hardening van technische componenten

Referentie code norm:	SSD-1
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie voldoet aan het hardeningbeleid. De software en het platform zijn daartoe geconfigureerd volgens de bijbehorende hardeningrichtlijn. Het configureren is procesmatig en procedureel ingericht.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Veilige gegevensopslag

Referentie code norm:	SSD-2
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.
Verificatie methode(n):	Testen.

Toelichting:

Veilige externe componenten

Referentie code norm:	SSD-3
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Applicaties maken gebruik van veilige en actief onderhouden externe componenten.
Verificatie methode(n):	Testen.

Toelichting:

Veilige communicatie

Referentie code norm:	SSD-4
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)
Samenvatting eis:	De applicatie past versleuteling toe op de communicatie van gegevens die passend is bij het classificatieniveau van de gegevens, zowel over interne als externe netwerken en controleert hierop. Van te beschermen gegevens worden alleen de noodzakelijke gecommuniceerd.
Verificatie methode(n):	Testen. Daarnaast Internet.nl.
Toelichting:	

Authenticatie van gebruikers en systemen

Referentie code norm:	SSD-5
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Applicaties stellen de identiteit van gebruikers en systemen vast op basis van een mechanisme voor identificatie en authenticatie, waarbij de authenticatiegegevens in een centrale authenticatievoorziening worden beheerd.
Verificatie methode(n):	Testen.
Toelichting:	

Gebruikersrechtenbeheer

Referentie code norm:	SSD-7
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De rechten die gebruikers hebben binnen een applicatie (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.
Verificatie methode(n):	Testen.
Toelichting:	

Autoriseer toegang

Referentie code norm:	SSD-8
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie dwingt de door de opdrachtgever voorgeschreven beperkende set van rechten en privileges af met alleen de voor de gebruiker en systemen noodzakelijke toegang.
Verificatie methode(n):	Testen.

Toelichting:

Registreren van inlogpogingen

Referentie code norm:	SSD-9
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie registreert gelukke en mislukte login-pogingen.
Verificatie methode(n):	Testen.

Toelichting:

Sessie-beëindiging

Referentie code norm:	SSD-12
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	SAML (authenticatie)
Samenvatting eis:	De applicatie beëindigt een sessie na een vooringestelde periode van inactiviteit van de gebruiker via automatische sessie-beëindiging.
Verificatie methode(n):	Testen. Daarnaast Internet.nl.

Toelichting:

Onweerlegbaarheid

Referentie code norm:	SSD-13
-----------------------	--------

Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie ondersteunt de onweerlegbaarheid voor daartoe aangewezen transacties via cryptografische technieken.
Verificatie methode(n):	Testen.

Toelichting:

Borgen van Sessie Authenticiteit

Referentie code norm:	SSD-14
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	SAML (authenticatie)
Samenvatting eis:	De applicatie hanteert voor sessie-identifiers onvoorspelbare tekenreeksen en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.
Verificatie methode(n):	Testen. Daarnaast Internet.nl.

Toelichting:

Scheiding van presentatie, applicatie en gegevens

Referentie code norm:	SSD-15
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De architectuur van een applicatie is gebaseerd op een gelaagde structuur door de presentatie-laag, de applicatielaag en de gegevens te scheiden, zodat de lagen beschermd kunnen worden binnen de netwerkzones.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Gescheiden beheerinterface

Referentie code norm:	SSD-17
Referentie brondocument:	SSD
BIO-BBN:	2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Beheeractiviteiten vinden plaats via een van de
standaard gebruikersinterface gescheiden
beheerinterface.

Verificatie methode(n):

Testen.

Toelichting:

Invoer-normalisatie

Referentie code norm:

SSD-19

Referentie brondocument:

SSD

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De applicatie voorkomt manipulatie door alle
ontvangen invoer te normaliseren alvorens die te
valideren. De richtlijnen voor invoerbehandeling
zijn van toepassing voor alle invoer die van
buiten de applicatie komt. Dus niet alleen
(eind)gebruikers, maar ook externe systemen en
applicaties.

Verificatie methode(n):

Testen.

Toelichting:

Uitvoer-schoning

Referentie code norm:

SSD-20

Referentie brondocument:

SSD

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De applicatie beperkt de uitvoer tot waarden die
(veilig) verwerkt kunnen worden door deze te
normaliseren naar de juiste context.

Verificatie methode(n):

Testen.

Toelichting:

Geparametriseerde queries Beperkte commando/query-toegang

Referentie code norm:

SSD-21

Referentie brondocument:

SSD

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De applicatie legt beperkingen aan queries en commando's op daar waar met achterliggende systemen wordt gecommuniceerd en deze communicatie wordt alleen ingericht indien strikt noodzakelijk.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Invoervalidatie

Referentie code norm: SSD-22

Referentie brondocument: SSD

BIO-BBN: 2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De applicatie controleert invoer (bijvoorbeeld een HTTP-request) door deze te valideren alvorens die te gebruiken.

Verificatie methode(n): Testen.

Toelichting:

Beperkte file Includes

Referentie code norm: SSD-23

Referentie brondocument: SSD

BIO-BBN: 2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De applicatie voorkomt de mogelijkheid van dynamische file includes.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Beperking van te versturen HTTP-headers

Referentie code norm: SSD-24

Referentie brondocument: SSD

BIO-BBN: 2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De webserver stuurt bij een antwoord aan een gebruiker alleen die informatie in de HTTP-headers mee die van belang is voor het functioneren van HTTP.

Verificatie methode(n): Testen.

Toelichting:

Beperkte HTTP-methoden

Referentie code norm: SSD-26
Referentie brondocument: SSD
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie: TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis: De webserver faciliteert alleen de HTTP-functionaliteiten die nodig zijn voor het functioneren van de applicatie.
Verificatie methode(n): Overleg bewijsstukken en Internet.nl.

Toelichting:

Discrete foutmeldinge

Referentie code norm: SSD-27
Referentie brondocument: SSD
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De applicatie neemt in een foutmelding geen inhoudelijke foutinformatie op die misbruikt kan worden.
Verificatie methode(n): Testen.

Toelichting:

Discreet commentaar

Referentie code norm: SSD-28
Referentie brondocument: SSD
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De aan de gebruiker aangeboden scripts / code bevat geen commentaar dat tot misbruik kan leiden.
Verificatie methode(n): Testen.

Toelichting:

Voorkom directory listing

Referentie code norm:	SSD-29
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De aan de gebruiker getoonde informatie bevat geen directory listings, zodat die niet kunnen worden misbruikt.
Verificatie methode(n):	Testen.

Toelichting:

Applicatie logging

Referentie code norm:	SSD-30
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Standaard stack

Referentie code norm:	SSD-31
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De (web-)applicatie(-omgeving) maakt gebruik van systeemcomponenten en voorzieningen die onderdeel zijn van een formeel gespecificeerde stack.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Bescherming tegen XML externe entiteit

Referentie code norm:	SSD-32
-----------------------	--------

Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie beperkt de mogelijkheid tot manipulatie door alle externe XML invoer te beschermen tegen entiteit injectie.
Verificatie methode(n):	Testen.

Toelichting:

Veilige HTTP response headers

Referentie code norm:	SSD-33
Referentie brondocument:	SSD
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie maakt gebruik van veilige response headers.
Verificatie methode(n):	Testen.

Toelichting:

Referenties

SSD normen V3.0 (cip-overheid.nl)
 ICT-beveiligingsrichtlijnen voor webapplicaties | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)