



Rijksoverheid

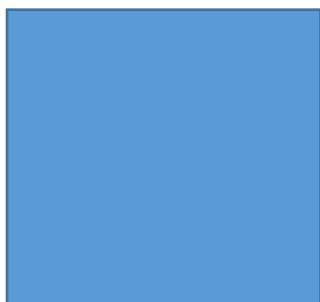


Interprovinciaal Overleg



UNIE VAN
WATERSCHAPPEN

Selectie Inkoop Eisen Cybersecurity Overheid



Ten behoeve van
Bijlage
Bij aanbesteding

Sociale Dienst Drechtsteden
Bijlage J – Inkoop Eisen Cybersecurity bij de Overheid
200057-1SDD Repro- en kantoordrukwerk

Datum

1-9-2021

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 substituut 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	Clouddiensten
Proceseis	ja
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Eisen meenemen die te maken hebben met louter schaalgrootte	ja
Prioriteit	hoog
Aantal geselecteerde eisen	34

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](#)
[Softwarepakketten](#)
[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 inkooppeisen

Wet en Regelgeving

Referentie code norm:	B.01
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan de eisen te voldoen, behoren voor elke cloud dienst en voor de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	Eis: Alleen <u>beleid</u> vaststellen, documenteren en actueel houden, niveau BBN1.

Cloud beveiligingsstrategie

Referentie code norm:	B.02
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort een cloud beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	Eis

Exit strategie

Referentie code norm:	B.03
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de clouddiensten overeenkomst tussen CSP en CSC behoort een exit strategie te zijn opgenomen waarbij zowel een aantal bepalingen aangaande exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.

Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting: Eis

Cloud dienstenbeleid

Referentie code norm: B.04

Referentie brondocument: Thema Clouddiensten

BIO-BBN: 2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud beveiligingsbeleid om de voorzieningen en het gebruik van cloud services te adresseren.

Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Risicomanagement

Referentie code norm: B.06

Referentie brondocument: Thema Clouddiensten

BIO-BBN: 2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagement proces voor de beveiliging van de cloud diensten te hebben opgezet en te onderhouden.

Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting: Eis

IT-functionaliteiten

Referentie code norm: B.07

Referentie brondocument: Thema Clouddiensten

BIO-BBN: 2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: IT functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van CSP naar CSC.

Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Business continuïteit management

Referentie code norm:	B.08
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort haar Business Continuïteit Management (BCM) proces adequaat hebben georganiseerd, waar bij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, business continuity planning, verificatie en updaten, en computercentra.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis, er moet een back-up zijn.

Data- en Privacy

Referentie code norm:	B.09
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Standaarden voor Clouddiensten

Referentie code norm:	U.01
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP past aantoonbaar relevante, nationale en internationale standaarden toe voor de opzet en

exploitatie van de diensten en de interactie met de CSC.

Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis, pas toe of leg uit lijst meesturen.

Risico Assessment

Referentie code norm: U.02
Referentie brondocument: Thema Clouddiensten
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De CSP behoort risico assessment uit te voeren, bestaande uit risico analyse en risico evaluatie en op basis van de criteria en de doelstelling m.b.t. cloud diensten van de CSP.

Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting: Wens

Business Continuity Services

Referentie code norm: U.03
Referentie brondocument: Thema Clouddiensten
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.

Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Herstelfunctie voor data en cloud diensten

Referentie code norm: U.04
Referentie brondocument: Thema Clouddiensten
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De herstelfunctie van data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen behoort te worden gefaciliteerd met infrastructuur

Verificatie methode(n): en IT-diensten, die robuust zijn en periodiek worden getest.
Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting: Eis

Dataprotectie

Referentie code norm: U.05
Referentie brondocument: Thema Clouddiensten
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie: * TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)
Samenvatting eis: Data (op transport, in verwerking en in rust) met classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.
Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting: Eis

Dataretentie en vernietiging van gegevens

Referentie code norm: U.06
Referentie brondocument: Thema Clouddiensten
BIO-BBN: 2
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn technologieonafhankelijk, onveranderbaar, integer en raadpleegbaar te worden opgeslagen en op aanwijzing van de CSC/data eigenaar te kunnen worden vernietigd.
Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting: Eis

Scheiding van data

Referentie code norm: U.07

Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Scheiding van dienstverlening

Referentie code norm:	U.08
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De cloud infrastructuur is zodanig ingericht, dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Malware protectie

Referentie code norm:	U.09
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Toegang tot IT diensten en data

Referentie code norm:	U.10
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Gebruikers behoren alleen toegang te krijgen tot de IT-diensten en data waarvoor zij specifiek bevoegd zijn.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Eis

Cryptoservices

Referentie code norm:

U.11

Referentie brondocument:

Thema Clouddiensten

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

* TLS, HTTPS en HSTS (beveiligde verbinding)

Samenvatting eis:

Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen, tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting:

Eis

Koppelvlakken

Referentie code norm:

U.12

Referentie brondocument:

Thema Clouddiensten

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De onderlinge netwerkconnecties (koppelvlakken) in de keten van CSC naar CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Eis

Interoperabiliteit en Portabiliteit

Referentie code norm:

U.14

Referentie brondocument:

Thema Clouddiensten

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

* TLS, HTTPS en HSTS (beveiligde verbinding)

Cloud services zijn bruikbaar (Interoperabiliteit) op verschillende IT-platforms en kunnen op basis van standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (Portabiliteit) naar andere CSP's.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.
Daarnaast Internet.nl.

Toelichting:

Eis

Logging en Monitoring

Referentie code norm:

U.15

Referentie brondocument:

Thema Clouddiensten

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Eis

Cloud diensten architectuur

Referentie code norm:

U.16

Referentie brondocument:

Thema Clouddiensten

BIO-BBN:

2

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De clouddiensten architectuur specificeert de samenhang en beveiliging van de services en de inter-connectie tussen CSC en CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Wens

Service Managementbeleid en evaluatie richtlijnen

Referentie code norm:	C.01
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP heeft voor de clouddiensten een Service Management beleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Risk control

Referentie code norm:	C.02
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het risico management en het risico assessment proces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis

Compliance en Assurance

Referentie code norm:	C.03
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort regelmatig de naleving van de cloud beveiligingsovereenkomsten op compliance te beoordelen, jaarlijks een assurance verklaring aan de CSC uit te brengen en ervoor te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting: Eis (eventueel afzwakken wens)

Security Monitoring

Referentie code norm:	C.05
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	2
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De performance van de informatiebeveiliging van de cloud omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan de verschillende stakeholders.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	Eis