



Rijksoverheid



Vereniging van
Nederlandse Gemeenten

Interprovinciaal Overleg



UNIE VAN
WATERSCHAPPEN

Selectie Inkoop Eisen Cybersecurity Overheid (ICO report)



Samengesteld door
Organisatie

R.W. Vollenberg/R. van Dick
Staf en Informatiebeheer

Datum

22-9-2022

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.

Selectiecriteria

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

Inkooponderdelen	Clouddiensten
Proceseis	nee
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Eisen meenemen die te maken hebben met louter schaalgrootte	nee
Basispakket	ja
Privacy-supplement	nee
Aantal geselecteerde eisen	17

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](#)

[Privacy-supplementen](#)

Geselecteerde inkoop-eisen

Transparantie

Referentie code norm:

[B.05](#)

Referentie brondocument:

[Thema Clouddiensten](#)

O-Maatregel:

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

De CSP¹ voorziet de CSC² in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

IT-functionaliiteit

Referentie code norm:

[B.07](#)

Referentie brondocument:

[Thema Clouddiensten](#)

O-Maatregel:

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

¹ CSP: (Cloud Service Provider)

² CSC:(Cloud Service Consumer)

Privacy en bescherming persoonsgegevens

Referentie code norm:	B.09
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	
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:	

Clouddienstenarchitectuur

Referentie code norm:	B.11
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Bedrijfscontinuïteitsservices

Referentie code norm:	U.03
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Herstelfunctie voor data en clouddiensten

Referentie code norm:	U.04
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Dataproductie

Referentie code norm:	U.05
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	
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 de 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:	

Dataretentie en gegevensvernietiging

Referentie code norm: [U.06](#)

Referentie brondocument: [Thema Clouddiensten](#)

O-Maatregel:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer 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:

Datascheiding

Referentie code norm: [U.07](#)

Referentie brondocument: [Thema Clouddiensten](#)

O-Maatregel:

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:

Scheiding dienstverlening

Referentie code norm: [U.08](#)

Referentie brondocument: [Thema Clouddiensten](#)

O-Maatregel:

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:

Malware-protectie

Referentie code norm:	U.09
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	Ja
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:	

Toegang IT-diensten en data

Referentie code norm:	U.10
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Cryptoservices

Referentie code norm:	U.11
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	Ja
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:	

Koppelvlakken

Referentie code norm:	U.12
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de 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:	

Interoperabiliteit en portabiliteit

Referentie code norm:	U.14
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis:	Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende ITplatforms en kunnen met 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:	

Logging en monitoring

Referentie code norm:	U.15
Referentie brondocument:	Thema Clouddiensten
O-Maatregel:	Ja
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:	

Multi-tenantarchitectuur

Referentie code norm:

[U.17](#)

Referentie brondocument:

[Thema Clouddiensten](#)

O-Maatregel:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting: