

Bijlage 12 Inkooppeisen Cybersecurity Overheid



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.

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
Ook eisen meegeven die alleen te maken hebben met schaalgrootte	ja
Basispakket	ja
Privacy-toevoegingen meenemen	ja
Toon BIO-O maatregelen BBN1	nee
Toon BIO-O maatregelen BBN2	ja
Toon ABDO-eisen TBB4	nee
Toon ABDO-eisen TBB3	nee
Toon ABDO-eisen TBB2	nee
Toon ABDO-eisen TBB1	nee
Aantal geselecteerde eisen	73

De eisen op de volgende pagina's zijn gebaseerd op de BIO en onderliggende uitwerkingen. Afhankelijk van de gemaakte selecties komt u ook eisen tegen die gebaseerd zijn op andere normenkaders, zoals CSIR, de ABDO en Privacy supplementen. Bij de eisen is aangegeven uit welk brondocument die afkomstig zijn en onder welke codes ze daarin voorkomen. In deze brondocumenten is per eis een nadere specificatie opgenomen. Voor zover mogelijk zijn ook hyperlinks aangebracht waarmee direct de achterliggende informatie kan worden opgevraagd.

Hieronder staan de links naar de vindplaatsen van alle brondocumenten.

[ABDO](#)
[Applicatieontwikkeling algemeen](#)
[Clouddiensten](#)
[Communicatievoorzieningen](#)
[CSIR](#)
[DIGID Applicaties](#)
[Huisvesting IV](#)
[Maatwerk of maatwerkpakket](#)
[Middleware](#)
[Mobiele Applicaties](#)
[Privacy-supplementen](#)
[Server-platform](#)
[Softwarepakketten](#)
[Toegangsbeveiliging](#)

Geselecteerde inkoop-eisen

Wet en Regelgeving

Referentie code norm:	B.01
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Cloudbeveiligingsstrategie

Referentie code norm:	B.02
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
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:

Exit-strategie

Referentie code norm:	B.03
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen ⁶ over exit zijn opgenomen, als een aantal condities ⁶ die aanleiding kunnen geven tot een exit.

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

Toelichting:

Clouddienstenbeleid

Referentie code norm: [B.04](#)

Referentie brondocument: [Thema Clouddiensten](#)

BIO-BBN:

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 cloudservices te adresseren.

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

Toelichting:

Transparantie

Referentie code norm: [B.05](#)

Referentie brondocument: [Thema Clouddiensten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De CSP voorziet de CSC 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:

Risicomanagement

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

Referentie brondocument: [Thema Clouddiensten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van

Verificatie methode(n): clouddiensten te hebben opgezet en onderhouden.
Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

IT-functionality

Referentie code norm: [B.07](#)
Referentie brondocument: [Thema Clouddiensten](#)
BIO-BBN:
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:

Bedrijfscontinuïteitsmanagement

Referentie code norm: [B.08](#)
Referentie brondocument: [Thema Clouddiensten](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Privacy en bescherming persoonsgegevens

Referentie code norm: [B.09](#)
Referentie brondocument: [Thema Clouddiensten](#)
BIO-BBN:
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/labels, eigenaarschap en locatie.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beveiligingsorganisatie

Referentie code norm:

[B.10](#)

Referentie brondocument:

[Thema Clouddiensten](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Clouddienstenarchitectuur

Referentie code norm:

[B.11](#)

Referentie brondocument:

[Thema Clouddiensten](#)

BIO-BBN:

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:

Standaarden voor clouddiensten

Referentie code norm:

[U.01](#)

Referentie brondocument:

[Thema Clouddiensten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe

Verificatie methode(n): voor de opzet en exploitatie van de diensten en de interactie met de CSC.
Overleg bewijsstukken en/of Verklaring.

Toelichting:

Risico-assessment

Referentie code norm: [U.02](#)

Referentie brondocument: [Thema Clouddiensten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.

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

Toelichting:

Bedrijfscontinuïteitsservices

Referentie code norm: [U.03](#)

Referentie brondocument: [Thema Clouddiensten](#)

BIO-BBN:

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](#)

BIO-BBN:

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

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

Toelichting:

Dataproductie

Referentie code norm: [U.05](#)
Referentie brondocument: [Thema Clouddiensten](#)
BIO-BBN:
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](#)
BIO-BBN: Ja
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:

O-maatregel. Beschermen van registraties

Referentie code norm: [18.1.3.1](#)
Referentie brondocument: [BIO 2019](#)
BIO-BBN: Ja
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.
Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Datascheiding

Referentie code norm: [U.07](#)
Referentie brondocument: [Thema Clouddiensten](#)
BIO-BBN:
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](#)
BIO-BBN:
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](#)
BIO-BBN: 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](#)

BIO-BBN:

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](#)

BIO-BBN:

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:

O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:

[10.1.1.1](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.

Verificatie methode(n):

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

Toelichting:

O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:

[10.1.1.2](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Cryptografische toepassingen voldoen aan passende standaarden.

Verificatie methode(n):

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

Toelichting:

O-maatregel. Sleutelbeheer

Referentie code norm:

[10.1.2.1](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.

Verificatie methode(n):

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

Toelichting:

O-maatregel. Sleutelbeheer

Referentie code norm:	10.1.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
Toelichting:	

Koppelvlakken

Referentie code norm:	U.12
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	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:	

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard

Verificatie methode(n): van de te beschermen gegevens en informatiesystemen.
Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm: [13.1.2.2](#)
Referentie brondocument: [BIO 2019](#)
BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).

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

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm: [13.1.2.3](#)
Referentie brondocument: [BIO 2019](#)
BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.

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

Toelichting:

Service-orkestratie

Referentie code norm: [U.13](#)
Referentie brondocument: [Thema Clouddiensten](#)
BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Service-orkestratie biedt coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloud-service die aan de CSC wordt geleverd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Interoperabiliteit en portabiliteit

Referentie code norm:

[U.14](#)

Referentie brondocument:

[Thema Clouddiensten](#)

BIO-BBN:

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](#)

BIO-BBN:

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:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:

[12.4.1.3](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:

[12.4.1.4](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:

[12.4.1.5](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Clouddienstenarchitectuur

Referentie code norm:	U.16
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de 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:

Multi-tenantarchitectuur

Referentie code norm:	U.17
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
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:

Servicemanagementbeleid en evaluatierichtlijn

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

Toelichting:

Risico-control

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

Toelichting:

Compliance en assurance

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

Toelichting:

O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging

Referentie code norm:	18.2.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging

Referentie code norm:	18.2.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

O-maatregel. Beoordeling van technische naleving

Referentie code norm:	18.2.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Technische kwetsbaarhedenbeheer

Referentie code norm:	C.04
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	STIX en TAXII (Uitwisseling van cyberdreigingsinformatie)
Samenvatting eis:	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Security-monitoringsrapportage

Referentie code norm:

[C.05](#)

Referentie brondocument:

[Thema Clouddiensten](#)

BIO-BBN:

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 verschillende stakeholders.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beheersorganisatie clouddiensten

Referentie code norm:

[C.06](#)

Referentie brondocument:

[Thema Clouddiensten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De CSP heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Testdata

Referentie code norm:

APO P.01

Referentie brondocument:

[Privacy-supplement Applicatieontwikkeling Algemeen](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risico-analyse gebruik gemaakt wordt van persoonsgegevens, worden passende maatregelen ter bescherming van de persoonsgegevens genomen.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Privacy by Default binnen applicaties

Referentie code norm:

SSD P.01

Referentie brondocument:

[Privacy-supplement SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij standaard zo min mogelijk persoonsgegevens worden verwerkt

Verificatie methode(n):

Testen

Toelichting:

Correcte en gewenste verwerking met applicaties

Referentie code norm:

SSD P.02

Referentie brondocument:

[Privacy-supplement SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring en testen

Toelichting:

Informatieverstrekking aan betrokkene met applicaties

Referentie code norm:

SSD P.03

Referentie brondocument:

[Privacy-supplement SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:	Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring en testen
Toelichting:	

Toegang op taakniveau met applicaties

Referentie code norm:	SSD P.04
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring
Toelichting:	

Logging met applicaties

Referentie code norm:	SSD P.05
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring
Toelichting:	

Dataminimalisatie binnen applicaties

Referentie code norm:	SSD P.06
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Generalisatie binnen applicaties

Referentie code norm:

SSD P.07

Referentie brondocument:

[Privacy-supplement SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De applicatie behoort, indien de functionele eisen aan de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Scheiden binnen applicaties

Referentie code norm:

SSD P.08

Referentie brondocument:

[Privacy-supplement SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Verbergen binnen applicaties

Referentie code norm:

SSD P.09

Referentie brondocument:

[Privacy-supplement SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een taak alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

DataminimalisatieDataminimalisatie door serverplatformen

Referentie code norm:

SVP P.01

Referentie brondocument:

[Privacy-supplement Serverplatform](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Scheiden door serverplatformen

Referentie code norm:

SVP P.02

Referentie brondocument:

[Privacy-supplement Serverplatform](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Verbergen door serverplatformen

Referentie code norm:	SVP P.03
Referentie brondocument:	Privacy-supplement Serverplatform
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Scheiden binnen communicatievoorzieningen

Referentie code norm:	CVZ P.01
Referentie brondocument:	Privacy-supplement Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Verbergen binnen communicatievoorzieningen

Referentie code norm:	CVZ P.02
Referentie brondocument:	Privacy-supplement Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij het verbergen van verwerkingen het uitgangspunt is.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Logging binnen communicatievoorzieningen

Referentie code norm:	CVZ P.03
Referentie brondocument:	Privacy-supplement Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Uitvallen van een dienst

Referentie code norm:	HVI P.01
Referentie brondocument:	Privacy-supplement Huisvesting-IV
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De organisatie heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Het stelsel van toegangsbeheer

Referentie code norm:	TBV P.01
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt

Verificatie methode(n):

verstrekt. Aanvullend vindt logging en monitoring plaats.
Overleg bewijsstukken en/of verklaring

Toelichting:

Doelbinding op rolniveau

Referentie code norm: TBV P.02
Referentie brondocument: [Privacy-supplement Toegangsbeveiliging](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.

Verificatie methode(n): Overleg bewijsstukken en/of verklaring

Toelichting:

Toegang op taakniveau

Referentie code norm: TBV P.03
Referentie brondocument: [Privacy-supplement Toegangsbeveiliging](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.

Verificatie methode(n): Overleg bewijsstukken en/of verklaring

Toelichting:

Logging en monitoring uitgeven toegangsrechten

Referentie code norm: TBV P.04
Referentie brondocument: [Privacy-supplement Toegangsbeveiliging](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:	De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Toegang tot fysieke omgevingen

Referentie code norm:	TBV P.05
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Toegang buiten beveiligde omgevingen

Referentie code norm:	TBV P.06
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door minimalisatie de omvang van een datalek wordt beperkt.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Toegang in het buitenland

Referentie code norm:	TBV P.07
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging

BIO-BBN:

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Beëindiging (verwerkers)overeenkomst

Referentie code norm:

TBV P.08

Referentie brondocument:

[Privacy-supplement Toegangsbeveiliging](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting: