Selectie Inkoopeisen 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. 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 verzwaard. Dit blijkt uit de eventueel bij de eisen gemaakt opmerkingen.

Selectiecriteria

De volgende criteria zijn van toepassing voor de selectie van inkoopeisen.

Inkooponderdelen	Clouddiensten
Proceseis	nee
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Ook eisen meegeven die alleen te maken hebben met schaalgrootte	nee
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	24

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

Disclaimer:
De inkoopeisen 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 om 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 inkoopeisen

Transparantie, IT-functionaliteit, Clouddienstenarchitectuur

Referentie code norm:	B.05, B.07, B.11
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. IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC. 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:

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/labelen, eigenaarschap en locatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beveiligde inlogprocedure

Referentie code norm:	U.02
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	SAML

Samenvatting eis:	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure, middels SSO, Entra ID (authenticatie).
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Bedrijfscontinuïteitsservices, Herstelfunctie voor data en clouddiensten

Referentie code norm:	U.03, U.04
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. 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. De verwerkende faciliteiten hebben tijdens openingstijden van CSC een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Back-up van informatie

Referentie code norm:	12.3.1.3, 12.3.1.4, 12.3.1.5
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In het back-upbeleid staan minimaal de volgende eisen: (a) Dataverlies bedraagt maximaal 24 uur. (b) Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen. Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere. De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging

	om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Dataprotectie, Dataretentie en gegevensvernietiging, Cryptoservices

Referentie code norm:	U.05, U.06, U.11
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. 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. 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:

Patchmanagement en onderhoud

Referentie code norm:	U.05
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Servers en de applicatie behoren correct te worden onderhouden om de continue beschikbaarheid en integriteit te waarborgen. Patchmanagement is procesmatig en procedureel opgezet en wordt ondersteund door richtlijnen zodat het zodanig kan worden uitgevoerd dat op

	de servers en de applicatie de laatste (beveiligings)patches tijdig zijn geïnstalleerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Datascheiding, Scheiding dienstverlening, Toegang IT-diensten en data

Referentie code norm:	U.07, U.08, U.10
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. De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden. Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
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:

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:	

Interoperabiliteit en portabiliteit

Referentie code norm:	U.14 / BIO 10.1.1.1
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:	

Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:	10.1.1.1 / 10.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	'Pas toe leg uit' standaarden (verplicht) | Forum Standaardisatie
Samenvatting eis:	Cryptografische toepassingen voldoen aan passende standaarden. In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Op welke wijze 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:

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:

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:

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 detectie-voorzieningen. Bij ontdekte nieuwe dreigingen (aanvallen of ernstige kwetsbaarheden) worden deze binnen geldende juridische kaders verplicht gedeeld met CSC
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Privacy eisen

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:

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:

Scheiden binnen applicaties en communicatievoorzieningen

Referentie code norm:	SSD P.08, CVZ P.01
Referentie brondocument:	Privacy-supplement SSD, Privacy-supplement Communicatievoorzieningen
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, communicatievoorzieningen en serverplatformen

Referentie code norm:	SSD P.09, SVP P.03, CVZ P.02
Referentie brondocument:	Privacy-supplement SSD, Privacy-supplement Communicatievoorzieningen
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. 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 en 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:

Dataminimalisatie door serverplatformen

Referentie code norm:	SVP P.01, SVP P.02
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. 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:

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:

Het stelsel van toegangsbeheer, Toegang op taakniveau

Referentie code norm:	TBV P.01, TBV P.02, TBV P.03, TBV P.04
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. 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 verstrekt. 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 Aanvullend vindt logging en monitoringplaats op verwerkers/persoonsniveau.
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: