



Rijksoverheid



Inter provinciaal Overleg



UNIE VAN
WATERSCHAPPEN

Selectie Inkoop Eisen Cybersecurity Overheid



Samengesteld door Organisatie	<naam> <afdeling, affiliatie> <vrije tekst>
Datum	28-1-2022

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.

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, Huisvesting IV, Serverplatform, Softwarepakketten, Toegangsbeveiliging
Proceseis	ja
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Eisen meenemen die te maken hebben met louter schaalgrootte	ja
Basispakket	ja
Privacy-supplement	ja
Aantal geselecteerde eisen	163

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.

Bij de eisen is tevens aangegeven of er specifieke overheidsmaatregelen van toepassing zijn. Deze eisen zullen - ongeacht risicoafwegingen - altijd moeten worden gesteld.

[Applicatieontwikkeling algemeen](#)

[Clouddiensten](#)

[Communicatievoorzieningen](#)

[DIGID Applicaties](#)

[Huisvesting IV](#)

[Maatwerk of maatwerkpakket](#)

[Mobiele Applicaties](#)

[Server-platform](#)

[Softwarepakketten](#)

[Toegangsbeveiliging](#)

[Privacy-supplementen](#)

[CSIR 3.4](#)

Per 1 oktober 2021 zijn in de Wizard privacy-supplementen toegevoegd. Deze kunnen naar keuze wel of niet mee-geselecteerd worden. De uitwerkingen kunnen direct worden gedownload met de link in het hierboven genoemde document van dezelfde naam.

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

Informatiebeveiligingsbeleid voor leveranciersrelaties

Referentie code norm:	B.02
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Met de leverancier behoren de informatiebeveiligingseisen en een periodieke actualisering daarvan te worden overeengekomen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Exit-strategie

Referentie code norm:	B.03
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de overeenkomst tussen de klant en leverancier behoort een exit-strategie te zijn opgenomen, waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Bedrijfs- en beveiligingsfuncties

Referentie code norm:	B.04
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Cryptografie

Referentie code norm:	B.05
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ter bescherming van de communicatie en opslag van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Levenscyclusmanagement softwarepakket

Referentie code norm:	U.01
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De leverancier behoort de klant te adviseren met marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over strategische ontwikkeling en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Beperkingen wijziging softwarepakket

Referentie code norm:	U.02
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Bedrijfscontinuïteit

Referentie code norm:	U.03
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.
Verificatie methode(n):	Testen.

Toelichting:

Input-/output-validatie

Referentie code norm:	U.04
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het softwarepakket behoort mechanismen te bevatten voor normalisatie en validatie van invoer en voor schoning van de uitvoer.
Verificatie methode(n):	Testen.

Toelichting:

Sessiebeheer

Referentie code norm:	U.05
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	SAML (authenticatie)
Samenvatting eis:	Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit.
Verificatie methode(n):	Testen.

Toelichting:

Gegevensopslag

Referentie code norm:	U.06
-----------------------	------

Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	Ja
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:

Communicatie

Referentie code norm:	U.07
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)
Samenvatting eis:	Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop.
Verificatie methode(n):	Testen.

Toelichting:

Authenticatie

Referentie code norm:	U.08
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Softwarepakketten behoren de identiteiten van gebruikers vast te stellen met een mechanisme voor identificatie en authenticatie.
Verificatie methode(n):	Testen.

Toelichting:

Toegangsautorisatie

Referentie code norm:	U.09
Referentie brondocument:	Thema Softwarepakketten
BIO-O-maatregel van toepassing?	Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Het softwarepakket behoort een
autorisatiemechanisme te bieden.

Verificatie methode(n):

Testen.

Toelichting:

Autorisatiebeheer

Referentie code norm:

U.10

Referentie brondocument:

Thema Softwarepakketten

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De rechten die gebruikers hebben binnen een
softwarepakket (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:

Logging

Referentie code norm:

U.11

Referentie brondocument:

Thema Softwarepakketten

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Het softwarepakket biedt signaleringsfuncties
voor registratie en detectie die beveiligd zijn
ingericht.

Verificatie methode(n):

Testen.

Toelichting:

Application Programming Interface (API)

Referentie code norm:

U.12

Referentie brondocument:

Thema Softwarepakketten

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.

Verificatie methode(n): Testen.

Toelichting:

Gegevensimport

Referentie code norm: U.13

Referentie brondocument: Thema Softwarepakketten

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis: Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.

Verificatie methode(n): Testen.

Toelichting:

Versiebeheer

Referentie code norm: C.02

Referentie brondocument: Thema Softwarepakketten

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis: Wijzigingen aan het softwarepakket binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.

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

Toelichting:

Patchmanagement

Referentie code norm: C.03

Referentie brondocument: Thema Softwarepakketten

BIO-O-maatregel van toepassing? Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis: Patchmanagement behoort procesmatig en procedureel uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code, zodat zo snel mogelijk de

laatste (beveiligings-)patches kunnen worden geïnstalleerd.

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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:

Beleid voor beveiligde inrichting en onderhoud

Referentie code norm:	B.01
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het beveiligd inrichten en onderhouden van het serverplatform behoren regels te worden vastgesteld en binnen de organisatie te worden toegepast.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Inrichtingsprincipes voor serverplatform

Referentie code norm:	B.02
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Principes voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Serverplatform-architectuur

Referentie code norm:	B.03
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een architectuurdokument vastgelegd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Bedieningsprocedure

Referentie code norm:	U.01
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Standaarden voor serverconfiguratie

Referentie code norm:	U.02
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Het serverplatform is geconfigureerd volgens gedocumenteerde standaarden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Malwareprotectie

Referentie code norm:	U.03
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Ter bescherming tegen malware behoren beheersmaatregelen voor preventie, detectie en herstel te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Technische kwetsbaarhedenbeheer

Referentie code norm:	U.04
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

STIX en TAXII (uitwisseling van
cyberdreigingsinformatie)

Informatie over technische
serverkwetsbaarheden[1] behoort tijdig te
worden verkregen, de blootstelling van de
organisatie aan dergelijke kwetsbaarheden dient
te worden geëvalueerd en passende maatregelen
moeten worden genomen om het risico dat ermee
samenhangt aan te pakken.

Verificatie methode(n):

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

Toelichting:

Patchmanagement

Referentie code norm:

U.05

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Patchmanagement is procesmatig en procedureel
opgezet en wordt ondersteund door richtlijnen
zodat het zodanig kan worden uitgevoerd dat op
de servers de laatste (beveiligings)patches tijdig
zijn geïnstalleerd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beheer op afstand

Referentie code norm:

U.06

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Richtlijnen en ondersteunende
beveiligingsmaatregelen behoren te worden
geïmplementeerd ter beveiliging van beheer op
afstand van servers.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of
Verklaring.

Toelichting:

Server-onderhoud

Referentie code norm:	U.07
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Servers behoren correct te worden onderhouden om de continue beschikbaarheid en integriteit te waarborgen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Verwijderen of hergebruiken serverapparatuur

Referentie code norm:	U.08
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle onderdelen van servers die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Hardenen server

Referentie code norm:	U.09
Referentie brondocument:	Thema Serverplatform
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het beveiligen van een server worden overbodige functies en ongeoorloofde toegang uitgeschakeld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Serverconfiguratie

Referentie code norm:	U.10
Referentie brondocument:	Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Serverplatforms behoren zo geconfigureerd te zijn, dat zij functioneren zoals het vereist is en zijn beschermd tegen ongeautoriseerd en incorrecte updates.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Virtualisatie serverplatform

Referentie code norm:

U.11

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Virtuele servers behoren goedgekeurd te zijn en toegepast te worden op robuuste en veilige fysieke servers (bestaande uit hypervisors en virtuele servers) en behoren zodanig te zijn geconfigureerd dat gevoelige informatie in voldoende mate is beveiligd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beperking van software- installatie

Referentie code norm:

U.12

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Voor het door gebruikers (beheerders) installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Kloksynchronisatie

Referentie code norm:

U.13

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De klokken van alle relevante
informatieverwerkende systemen binnen een
organisatie of beveiligingsdomein behoren te
worden gedocumenteerd en gesynchroniseerd
met één referentietijdbron.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Ontwerpdocument

Referentie code norm:

U.14

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Het ontwerp van een serverplatform behoort te
zijn gedocumenteerd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Evaluatierichtlijn servers en serverplatforms

Referentie code norm:

C.01

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Richtlijnen behoren te worden vastgesteld om de
implementatie en beveiliging van servers en
besturingssystemen te controleren waarbij de
bevindingen tijdig aan het management worden
gerapporteerd.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of
Verklaring.

Toelichting:

Beoordeling technische serveromgeving

Referentie code norm:

C.02

Referentie brondocument:

Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Technische serveromgevingen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.

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

Toelichting:

Logbestanden beheerders

Referentie code norm: C.03

Referentie brondocument: Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis: Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.

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

Toelichting:

Logging

Referentie code norm: C.04

Referentie brondocument: Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

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

Toelichting:

Monitoring

Referentie code norm: C.05

Referentie brondocument: Thema Serverplatform

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis: De organisatie reviewt/analyseert regelmatig de logbestanden om onjuist gebruik en verdachte

activiteiten op servers en besturingssystemen vast te stellen en bevindingen aan het management te rapporteren.

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

Toelichting:

Beheerorganisatie servers en serverplatforms

Referentie code norm: C.06
Referentie brondocument: Thema Serverplatform
BIO-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Binnen de beheerorganisatie is een beveiligingsfunctionaris benoemd die de organisatie ondersteunt in de vorm van het bewaken van beveiligingsbeleid en die inzicht verschaft in de inrichting van de servers en het serverplatform.

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

Toelichting:

Dataminimalisatie door serverplatformen

Referentie code norm: SVP P.01
Referentie brondocument: Privacy-supplement Serverplatform
BIO-O-maatregel van toepassing?
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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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:

Huisvesting IV-Beleid

Referentie code norm:

B.01

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Ten behoeve van het huisvesting IV-beleid behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Wet- en regelgeving

Referentie code norm:

B.02

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de huisvesting IV-organisatie om aan deze eisen te voldoen behoren voor elke huisvestingsdienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Eigenaarschap

Referentie code norm:

B.03

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Huisvesting IV-bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Certificering

Referentie code norm:

B.04

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Huisvesting IV van de leverancier behoort gecertificeerd te zijn conform de gangbare standaarden.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Service Level Management

Referentie code norm:

B.06

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Het management van huisvesting IV behoort diensten te leveren conform een dienstenniveau-overeenkomst (Service Level Agreement).

Verificatie methode(n):

Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

In- en externe bedreigingen

Referentie code norm:

B.07

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Training en bewustwording

Referentie code norm:

B.08

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Organisatiestructuur huisvesting IV

Referentie code norm:

B.09

Referentie brondocument:

Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De huisvesting IV-organisatie behoort voor de te realiseren huisvesting IV een adequate organisatiestructuur in te richten en de aan functionarissen toe te wijzen taken, verantwoordelijkheden en bevoegdheden vast te stellen.

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

Toelichting:

Richtlijn gebieden en ruimten

Referentie code norm: U.01

Referentie brondocument: Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Voor het werken in beveiligde gebieden behoren richtlijnen te worden ontwikkeld en toegepast.

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

Toelichting:

Bedrijfsmiddelen-inventaris

Referentie code norm: U.02

Referentie brondocument: Thema Huisvesting-IV

BIO-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Bedrijfsmiddelen die samenhangen met informatie en informatie-verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden

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

Toelichting:

Fysieke zonering

Referentie code norm: U.03

Referentie brondocument: Thema Huisvesting-IV

BIO-O-maatregel van toepassing? Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:	Fysieke beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beveiligingsfaciliteiten

Referentie code norm:	U.04
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het beveiligen van ruimten behoren faciliteiten te worden ontworpen en toegepast.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Nutsvoorziening

Referentie code norm:	U.05
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Apparatuur-positionering

Referentie code norm:	U.06
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Apparatuur behoort zo te worden geplaatst en beschermd, dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.

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

Toelichting:

Apparatuur-onderhoud

Referentie code norm: U.07
Referentie brondocument: Thema Huisvesting-IV
BIO-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Apparatuur behoort op een correcte wijze te worden onderhouden.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Apparatuur-verwijdering

Referentie code norm: U.08
Referentie brondocument: Thema Huisvesting-IV
BIO-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Bedrijfsmiddelenverwijdering

Referentie code norm: U.09
Referentie brondocument: Thema Huisvesting-IV
BIO-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Informatieverwerkende bedrijfsmiddelen, uitgezonderd daarvoor bestemde mobiele apparatuur, behoren niet van de locatie te worden verwijderd zonder voorafgaande goedkeuring.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Laad- en loslocatie

Referentie code norm:	U.10
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van IT-voorzieningen
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Bekabeling

Referentie code norm:	U.11
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Huisvesting IV-architectuur

Referentie code norm:	U.12
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het implementeren en onderhouden van huisvestingsvoorzieningen behoren architectuurvoorschriften en benodigde documentatie beschikbaar te zijn.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Controle-richtlijn huisvesting IV

Referentie code norm:	C.01
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bedrijfsmiddelen behoren periodiek te worden gecontroleerd met formeel vastgestelde richtlijnen en geconstateerde bevindingen dienen tijdig aan het management te worden gerapporteerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Onderhoudsplan

Referentie code norm:	C.02
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor iedere locatie van huisvesting IV behoort een onderhoudsplan te zijn opgesteld met een risicoafweging en onderhoudsbepalingen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Continuïteitbeheer

Referentie code norm:	C.03
Referentie brondocument:	Thema Huisvesting-IV
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Continuïteitbeheer behoort procesmatig voor de gehele organisatie te zijn ingericht, zodat na het plaatsvinden van een calamiteit de hosting services zo snel mogelijk worden hersteld en voortgezet.
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-O-maatregel van toepassing?	
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, 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:

Toegangbeveiligingsbeleid

Referentie code norm:	B.01
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Eigenaarschap

Referentie code norm:	B.02
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen behoort te zijn vastgelegd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Beveiligingsfunctie

Referentie code norm:	B.03
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een gespecialiseerde beveiligingsfunctie dient te zijn vastgesteld die verantwoordelijk is voor het bevorderen van toegangsbeveiliging binnen de gehele organisatie.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Cryptografie

Referentie code norm:	B.04
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Beveiligingsorganisatie

Referentie code norm:	B.05
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.

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

Toelichting:

Toegangsbeveiligingsarchitectuur

Referentie code norm: B.06
Referentie brondocument: Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De organisatie behoort met organisatorische eisen en wensen de technische inrichting beschreven te hebben en behoort in een toegangsbeveiligingsarchitectuur te zijn vastgelegd.

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

Toelichting:

Registratieprocedure

Referentie code norm: U.01
Referentie brondocument: Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

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

Toelichting:

Toegangsverleningsprocedure

Referentie code norm: U.02
Referentie brondocument: Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing? Ja
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

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

Toelichting:

Inlogprocedure

Referentie code norm:	U.03
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Autorisatieproces

Referentie code norm:	U.04
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een formeel autorisatieproces dient geïmplementeerd te zijn voor het beheersen van de toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Wachtwoordenbeheer

Referentie code norm:	U.05
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Speciale toegangsrechtenbeheer

Referentie code norm:	U.06
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Functiescheiding

Referentie code norm:	U.07
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigingen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Geheime authenticatie-informatie

Referentie code norm:	U.08
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het toewijzen van geheime authenticatie- informatie behoort te worden beheerst via een formeel beheersproces.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Autorisatie

Referentie code norm:	U.09
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Autorisatievoorzieningen

Referentie code norm:	U.10
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ter ondersteuning van autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten, beschikbaar zijn.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Fysieke toegangsbeveiliging

Referentie code norm:	U.11
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Beoordelingsprocedure

Referentie code norm:	C.01
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er procedures te zijn vastgesteld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Logging en monitoring

Referentie code norm:	C.03
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-O-maatregel van toepassing?	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Het stelsel van toegangsbeheer

Referentie code norm:	TBV P.01
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging
BIO-O-maatregel van toepassing?	
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 verstrekt. Aanvullend vindt logging en monitoring plaats.

Verificatie methode(n):

Overleg bewijsstukken en/of verklaring

Toelichting:

Doelbinding op rolniveau

Referentie code norm:

TBV P.02

Referentie brondocument:

Privacy-supplement Toegangsbeveiliging

BIO-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke

Verificatie methode(n): persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
Overleg bewijsstukken en/of verklaring

Toelichting:

Toegang tot fysieke omgevingen

Referentie code norm: TBV P.05
Referentie brondocument: Privacy-supplement Toegangsbeveiliging
BIO-O-maatregel van toepassing?
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-O-maatregel van toepassing?
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-O-maatregel van toepassing?
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-O-maatregel van toepassing?	
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:

Wet en Regelgeving

Referentie code norm:	B.01
Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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 clouddiensten te adresseren.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Transparantie

Referentie code norm:	B.05
-----------------------	------

Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

IT-functionaliteit

Referentie code norm:	B.07
Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP past aantoonbaar relevante, nationale standaarden 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:	

Risico-assessment

Referentie code norm:	U.02
Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	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-O-maatregel van toepassing?	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-O-maatregel van toepassing?	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
BIO-O-maatregel van toepassing?	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:

Service-orkestratie

Referentie code norm:	U.13
Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	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:

Clouddienstenarchitectuur

Referentie code norm:	U.16
Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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:

Technische kwetsbaarhedenbeheer

Referentie code norm:	C.04
Referentie brondocument:	Thema Clouddiensten
BIO-O-maatregel van toepassing?	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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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:	

Dataminimalisatie door serverplatformen

Referentie code norm:	SVP P.01
Referentie brondocument:	Privacy-supplement Serverplatform
BIO-O-maatregel van toepassing?	
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

Verificatie methode(n): persoonsgegevens wordt verwerkt en
verwijdering van persoonsgegevens mogelijk is.
Overleg bewijsstukken en/of verklaring

Toelichting:

Scheiden door serverplatformen

Referentie code norm: SVP P.02
Referentie brondocument: Privacy-supplement Serverplatform
BIO-O-maatregel van toepassing?
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-O-maatregel van toepassing?
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-O-maatregel van toepassing?
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De organisatie heeft een proces ingericht, zodat
bij de configuratie van (onderdelen van) het

Verificatie methode(n): netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is.
Overleg bewijsstukken en/of verklaring

Toelichting:

Verbergen binnen communicatievoorzieningen

Referentie code norm: CVZ P.02
Referentie brondocument: Privacy-supplement Communicatievoorzieningen
BIO-O-maatregel van toepassing?
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-O-maatregel van toepassing?
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-O-maatregel van toepassing?
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

Verificatie methode(n): betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
Overleg bewijsstukken en/of verklaring

Toelichting:

Het stelsel van toegangsbeheer

Referentie code norm: TBV P.01
Referentie brondocument: Privacy-supplement Toegangsbeveiliging
BIO-O-maatregel van toepassing?
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 verstrekt. Aanvullend vindt logging en monitoring plaats.
Verificatie methode(n): Overleg bewijsstukken en/of verklaring

Toelichting:

Doelbinding op rolniveau

Referentie code norm: TBV P.02
Referentie brondocument: Privacy-supplement Toegangsbeveiliging
BIO-O-maatregel van toepassing?
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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?

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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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-O-maatregel van toepassing?	
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:	

Referenties

Thema Applicatie ontwikkeling <referentie + link>

<lijst van andere brondocumenten waarnaar wordt verwezen in de eisen>