Selectie Inkoopeisen Cybersecurity Overheid

Samengesteld door <naam>
Organisatie <afdeling, affiliatie>

<vrije tekst>

Datum 12-3-2024

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	Algemeen Ketenpartners, Clouddiensten, Communicatievoorzieningen
Proceseis	ja
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Ook eisen meegeven die alleen te maken hebben met schaalgrootte	ja
Basispakket	ja
Privacy-toevoegingen meenemen	ja
Toon BIO-O maatregelen BBN1	ja
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	190

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

Voldoen aan BIO Hoofdstuk 1

Referentie code norm:	Ketenpartnereis 1
Referentie brondocument:	n.v.t.
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie van de Opdrachtnemer en zijn dienstverlening dienen in opzet, bestaan en werking te voldoen aan hoofdstuk 1 van de Baseline Informatiebeveiliging Overheid (BIO, versie 1.04, te downloaden op www.bio-overheid.nl) en toont dat jaarlijks aan middels onafhankelijke onderzoeken.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

PDCA-cyclus

Referentie code norm:	Ketenpartnereis 2
Referentie brondocument:	n.v.t.
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Informatiebeveiliging en privacy zijn dynamische onderwerpen en de maatregelen dienen vanwege toenemende risico's en bedreigingen via een PDCA-cyclus actueel te worden gehouden.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Recht op audit

Referentie code norm:	Ketenpartnereis 3
Referentie brondocument:	n.v.t.
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De Opdrachtgever heeft het recht om maximaal een maal per jaar een audit te laten uitvoeren. Deze audit wordt in overleg met de Opdrachtnemer ingepland.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Onderaannemers

Referentie code norm:	Ketenpartnereis 4
Referentie brondocument:	n.v.t.
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De eisen van het inkooponderdeel 'Algemeen Ketenpartners' zijn ook van toepassing op onderaannemers van de Opdrachtnemer.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Toeleveringsketen van informatie- en communicatietechnologie

Referentie code norm:	15.1.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Beheer van informatiebeveiligingsincidenten

Referentie code norm:	Ketenpartnereis 5
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Op de inrichting van het beheer van Informatiebeveiligingsincidenten is hoofstuk 16 van de BIO 2019 van toepassing.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.4
Referentie brondocument:	BIO 2019

BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.5
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.6
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.2.7
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rapportage van zwakke plekken in de informatiebeveiliging

Referentie code norm:	16.1.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een Coördinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Referentie code norm:	16.1.4.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Lering uit informatiebeveiligingsincidenten

Referentie code norm:	16.1.6.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Lering uit informatiebeveiligingsincidenten

Referentie code norm:	16.1.6.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Verzamelen van bewijsmateriaal

Referentie code norm:	16.1.7.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Referentie code norm:	Ketenpartnereis 6
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Op het bedrijfscontinuïteitsbeheer zijn de Informatiebeveiligingsaspecten van hoofstuk 17 van de BIO 2019 van toepassing.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Referentie code norm:	17.1.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Referentie code norm:	17.1.3.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Referentie code norm:	17.1.3.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Inrichting van verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	Ketenpartnereis 7

Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Op de inrichting van verantwoordelijkheden bij informatiebeveiliging is paragraaf 6.1. van de BIO 2019 van toepassing
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	

Samenvatting eis:	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Scheiding van taken

Referentie code norm:	6.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Contact met overheidsinstanties

Referentie code norm:	6.1.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is door de organisatie uitgewerkt wie met welke (overheids) instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/ calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.

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

Toelichting:

O-maatregel. Contact met overheidsinstanties

Referentie code norm:	6.1.3.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het contactoverzicht wordt jaarlijks geactualiseerd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Sturen op veilig personeel

Referentie code norm:	Ketenpartnereis 8
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij het sturen op veilig personeel is hoofdstuk 7 van de BIO 2019 van toepassing.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Screening

Referentie code norm:	7.1.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Arbeidsvoorwaarden

Referentie code norm:	7.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Directieverantwoordelijkheden

Referentie code norm:	7.2.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

O-maatregel. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Referentie code norm:	7.2.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Referentie code norm:	7.2.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Referentie code norm:	7.2.2.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Speciale systeemhulpmiddelen gebruiken

Referentie code norm:	9.4.4.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Speciale systeemhulpmiddelen gebruiken

Referentie code norm:	9.4.4.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoekemhulpmiddelen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Transport en verzenden

Referentie code norm:	Ketenpartnereis 10
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Media fysiek overdragen

Referentie code norm:	8.3.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een vastgestelde procedure voor het fysiek transport van media.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Media fysiek overdragen

Referentie code norm:	8.3.3.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Privacybeleid

Referentie code norm:	ALG P.01
Referentie brondocument:	Privacy-supplement Algemeen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Privacy-organisatie

Referentie code norm:	ALG P.02
Referentie brondocument:	Privacy-supplement Algemeen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de organisatie vastgelegd en vastgesteld , inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de

	betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Privacy-bewustzijn

Referentie code norm:	ALG P.03
Referentie brondocument:	Privacy-supplement Algemeen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Formele vastlegging handelen verwerker

Referentie code norm:	ALG P.04
Referentie brondocument:	Privacy-supplement Algemeen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Privacy in de levenscyclus

Referentie code norm:	ALG P.05
Referentie brondocument:	Privacy-supplement Algemeen

BIO-BBN:

Relevante standaard PToLU-lijst Forum Standaardisatie:

Samenvatting eis: Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacyrisico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.

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

Toelichting:

Register van verwerkingsactiviteiten

Referentie code norm: ALG P.06

Referentie brondocument: Privacy-supplement Algemeen

BIO-BBN:

Relevante standaard PToLU-lijst Forum Standaardisatie:

Samenvatting eis: De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.

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

Toelichting:

Datalekken

Referentie code norm: ALG P.07

Referentie brondocument: Privacy-supplement Algemeen

BIO-BBN:

Relevante standaard PToLU-lijst Forum Standaardisatie:

Samenvatting eis: De organisatie heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.

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

Toelichting:

Beleid en procedures voor informatietransport

Referentie code norm:	B.01
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Cryptografiebeleid voor communicatie

Referentie code norm:	B.03
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:	10.1.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor

	cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:	10.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Cryptografische toepassingen voldoen aan passende standaarden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Organisatiestructuur netwerkbeheer

Referentie code norm:	B.04
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In het beleid behoort te zijn vastgesteld dat een centrale organisatiestructuur gebruikt wordt voor het beheren van netwerken (onder andere Local Area Network (LAN) en Virtual Local Area Network (VLAN)) en zo veel mogelijk van de hardware en softwarecomponenten daarvan.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Richtlijnen voor netwerkbeveiliging

Referentie code norm:	U.01
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Beveiligde inlogprocedure

Referentie code norm:	U.02
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	SAML (authenticatie)
Samenvatting eis:	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Beveiligde inlogprocedures

Referentie code norm:	9.4.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Beveiligde inlogprocedures

Referentie code norm:	9.4.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Netwerkbeveiligingsbeheer

Referentie code norm:	U.03
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Vertrouwelijkheids- en of geheimhoudingsovereenkomst

Referentie code norm:	U.04
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Beveiliging van netwerkdiensten

Referentie code norm:	U.05

Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

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

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT,

	bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Zonering en filtering

Referentie code norm:	U.06
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Scheiding in netwerken

Referentie code norm:	13.1.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Elektronische berichten

Referentie code norm:	U.07
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	* STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing)
Samenvatting eis:	Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Elektronische berichten

Referentie code norm:	13.2.3.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen

	phishing en afluisteren op pas-toe-of-leg-uit lijst van het forum standaardisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Elektronische berichten

Referentie code norm:	13.2.3.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pastoe-of-leg-uit lijst, gebruik gemaakt van de actuele versie van Digikoppeling.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Elektronische berichten

Referentie code norm:	13.2.3.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Elektronische berichten

Referentie code norm:	13.2.3.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	

Samenvatting eis:	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Toepassingen via openbare netwerken

Referentie code norm:	U.08
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Gateways en firewalls

Referentie code norm:	U.09
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De filterfuncties van gateways en firewalls behoren zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Virtual Private Networks

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

Relevante standaard PToLU-lijst Forum Standaardisatie:	TLS
Samenvatting eis:	Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de organisatie die de VPN gebruikt.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Cryptografische services

Referentie code norm:	U.11
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)
Samenvatting eis:	Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

O-maatregel. Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Referentie code norm:	18.1.5.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Draadloze toegang

Referentie code norm:	U.12
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	* WPA2 Enterprise (Beveiligde WiFi-netwerken)
Samenvatting eis:	Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Netwerkconnecties

Referentie code norm:	U.13
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Netwerkauthenticatie

Referentie code norm:	U.14
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Netwerkbeheeractiviteiten

Referentie code norm:	U.15
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Logging en monitoring

Referentie code norm:	U.16
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden gemaakt en bewaard en regelmatig te worden beoordeeld (op de ernst van de risico's).
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.5
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Netwerk beveiligingsarchitectuur

Referentie code norm:	U.17
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Naleving richtlijn netwerkbeheer en evaluaties

Referentie code norm:	C.01
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Compliance-toets netwerkbeveiliging

Referentie code norm:	C.02

Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De naleving van een, conform het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliancy-toetsen).
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Evalueren robuustheid netwerkbeveiliging

Referentie code norm:	C.03
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Evalueren netwerkgebeurtenissen (monitoring)

Referentie code norm:	C.04
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Toereikende logging en monitoring behoren te zijn ingericht, om detectie, vastlegging en onderzoek van gebeurtenissen mogelijk te maken van gebeurtenissen, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beheersorganisatie netwerkbeveiliging

Referentie code norm:	C.05
Referentie brondocument:	Thema Communicatievoorzieningen
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.3
Referentie brondocument:	BIO 2019

BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Scheiden binnen communicatievoorzieningen

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

Toelichting:

Verbergen binnen communicatievoorzieningen

Referentie code norm:	CVZ P.02
Referentie brondocument:	Privacy-supplement Communicatievoorzieningen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	

Samenvatting eis:	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt wordt, waarbij het verbergen van verwerkingen het uitgangspunt is.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Logging binnen communicatievoorzieningen

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

Toelichting:

Wet en Regelgeving

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

Toelichting:

Cloudbeveiligingsstrategie

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

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort een cloud-beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Exit-strategie

Referentie code norm:	B.03
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen6 over exit zijn opgenomen, als een aantal condities6 die aanleiding kunnen geven tot een exit.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Clouddienstenbeleid

Referentie code norm:	B.04
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Transparantie

Referentie code norm:	B.05
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Risicomanagement

Referentie code norm:	B.06
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van 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-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Bedrijfscontinuïteitsmanagement

Referentie code norm:	B.08
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Privacy en bescherming persoonsgegevens

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

Toelichting:

Beveiligingsorganisatie

Referentie code norm:	B.10
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging

Referentie code norm:	6.1.1.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Clouddienstenarchitectuur

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

Toelichting:

Standaarden voor clouddiensten

Referentie code norm:	U.01
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe 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-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en

	risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Bedrijfscontinuïteitsservices

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

Toelichting:

Herstelfunctie voor data en clouddiensten

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

Toelichting:

Dataprotectie

Referentie code norm:	U.05
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-

	mailphishing/-spoofing) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)
Samenvatting eis:	Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting:

Dataretentie en gegevensvernietiging

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

Toelichting:

O-maatregel. Beschermen van registraties

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

Toelichting:

Datascheiding

Referentie code norm:	U.07

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

Toelichting:

Scheiding dienstverlening

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

Toelichting:

Malware-protectie

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

Toelichting:

O-maatregel. Beheersmaatregelen tegen malware

Referentie code norm:	12.2.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja

Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beheersmaatregelen tegen malware

Referentie code norm:	12.2.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beheersmaatregelen tegen malware

Referentie code norm:	12.2.1.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beheersmaatregelen tegen malware

Referentie code norm:	12.2.1.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Computers en media worden als voorzorgsmaatregel routinematig gescand. De

	uitgevoerde scan behoort te omvatten: (a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beheersmaatregelen tegen malware

Referentie code norm:	12.2.1.5
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Toegang IT-diensten en data

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

Toelichting:

O-maatregel. Toegang tot netwerken en netwerkdiensten

Referentie code norm:	9.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	

Samenvatting eis:	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Toegang tot netwerken en netwerkdiensten

Referentie code norm:	9.1.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Cryptoservices

Referentie code norm:	U.11
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis:	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting:

O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:	10.1.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer

	cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting:

O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Referentie code norm:	10.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Cryptografische toepassingen voldoen aan passende standaarden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting:

O-maatregel. Sleutelbeheer

Referentie code norm:	10.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Toelichting:

O-maatregel. Sleutelbeheer

Referentie code norm:	10.1.2.2

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

Toelichting:

Koppelvlakken

Referentie code norm:	U.12
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

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

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Beveiliging van netwerkdiensten

Referentie code norm:	13.1.2.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden

	(bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Service-orkestratie

Referentie code norm:	U.13
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Service-orkestratie biedt coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloud-service die aan de CSC wordt geleverd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Interoperabiliteit en portabiliteit

Referentie code norm:	U.14
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis:	Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende ITplatforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere CSP's.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Toelichting:

Logging en monitoring

Referentie code norm:	U.15
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en

	informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	

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

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.4
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

O-maatregel. Gebeurtenissen registreren

Referentie code norm:	12.4.1.5
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Clouddienstenarchitectuur

Referentie code norm:	U.16
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Multi-tenantarchitectuur

Referentie code norm:	U.17
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Servicemanagementbeleid en evaluatierichtlijn

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

Toelichting:

Risico-control

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

Toelichting:

Compliance en assurance

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

Toelichting:

O-maatregel. Beoordeling van het informatiebeveiligingsbeleid

Referentie code norm:	5.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P en C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging

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

Toelichting:

O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging

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

Toelichting:

O-maatregel. Naleving van beveiligingsbeleid en -normen

Referentie code norm:	18.2.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de P en C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Beoordeling van technische naleving

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

Toelichting:

Technische kwetsbaarhedenbeheer

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

Toelichting:

O-maatregel. Beheer van technische kwetsbaarheden

Referentie code norm:	12.6.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.

Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.
Toelichting:	

Security-monitoringsrapportage

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

Beheersorganisatie clouddiensten

Referentie code norm:	C.06
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De CSP heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Testdata

Referentie code norm:	APO P.01
Referentie brondocument:	Privacy-supplement Applicatieontwikkeling Algemeen
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risico-analyse gebruik gemaakt wordt van persoonsgegevens,

	worden passende maatregelen ter bescherming van de persoonsgegevens genomen.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring
Toelichting:	

Privacy by Default binnen applicaties

Referentie code norm:	SSD P.01
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij standaard zo min mogelijk persoonsgegevens worden verwerkt
Verificatie methode(n):	Testen
Toelichting:	

Correcte en gewenste verwerking met applicaties

Referentie code norm:	SSD P.02
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring en testen
Toelichting:	

Informatieverstrekking aan betrokkene met applicaties

Referentie code norm:	SSD P.03
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	

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

Toelichting:

Toegang op taakniveau met applicaties

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

Toelichting:

Logging met applicaties

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

Toelichting:

Dataminimalisatie binnen applicaties

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

BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Generalisatie binnen applicaties

Referentie code norm:	SSD P.07
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie behoort, indien de functionele eisen aan de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Scheiden binnen applicaties

Referentie code norm:	SSD P.08
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Verbergen binnen applicaties

Referentie code norm:	SSD P.09
Referentie brondocument:	Privacy-supplement SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een taak alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

DataminimalisatieDataminimalisatie door serverplatformen

Referentie code norm:	SVP P.01
Referentie brondocument:	Privacy-supplement Serverplatform
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Scheiden door serverplatformen

Referentie code norm:	SVP P.02
Referentie brondocument:	Privacy-supplement Serverplatform
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.

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

Toelichting:

Verbergen door serverplatformen

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

Toelichting:

Scheiden binnen communicatievoorzieningen

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

Toelichting:

Verbergen binnen communicatievoorzieningen

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

Toelichting:

Logging binnen communicatievoorzieningen

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

Toelichting:

Uitvallen van een dienst

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

Toelichting:

Het stelsel van toegangsbeheer

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

	gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoringplaats.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring
Toelichting:	

Doelbinding op rolniveau

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

Toegang op taakniveau

Referentie code norm:	TBV P.03
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring
Toelichting:	

Logging en monitoring uitgeven toegangsrechten

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

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

Toelichting:

Toegang tot fysieke omgevingen

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

Toelichting:

Toegang buiten beveiligde omgevingen

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

Toelichting:

Toegang in het buitenland

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

BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Beëindiging (verwerkers)overeenkomst

Referentie code norm:	TBV P.08
Referentie brondocument:	Privacy-supplement Toegangsbeveiliging
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting: