



Rijksoverheid



Selectie Inkoop Eisen Cybersecurity Overheid

Samengesteld door
Datum

Dienst Justitiële Inrichtingen, Direct Informatievoorziening
10-10-2024

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 substituuut voor eigen risicoafweging.

Op basis van risicoafwegingen van de behoeftesteller kunnen eisen worden geschrapt, verzacht of verzaamd. Dit blijkt uit de eventueel bij de eisen gemaakt opmerkingen.

Selectiecriteria

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

Inkooponderdelen	Applicatieontwikkeling algemeen, Maatwerk of maatwerkpakket, Softwarepakketten
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	nee
Toon BIO-O maatregelen BBN1	nee
Toon BIO-O maatregelen BBN2	ja
Toon ABDO-eisen TBB4	nee
Toon ABDO-eisen TBB3	nee
Toon ABDO-eisen TBB2	nee
Toon ABDO-eisen TBB1	nee
Aantal geselecteerde eisen	85

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 inkoop-eisen op de navolgende pagina's zijn samengesteld op basis van de bovenaan deze pagina ingevoerde criteria. De eisen en selecties die toegepast zijn, steunen op een proces van intensieve en brede, interbestuurlijke samenwerking. Het kan echter voorkomen dat er toch sprake is van omissies of onjuistheden. Het is de verantwoordelijkheid van de gebruiker zelf 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 inkoop Eisen

Beleid voor (beveiligd) ontwikkelen

Referentie code norm:	B.01
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Systeem-ontwikkelmethode

Referentie code norm:	B.02
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Ontwikkelactiviteiten behoren te zijn gebaseerd op een gedocumenteerde systeem-ontwikkelmethode, waarin onder andere standaarden en procedures voor de applicatieontwikkeling, het toepassen van beleid en wet- en regelgeving en een projectmatige aanpak zijn geadresseerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Engineeringprincipes voor beveiligde systemen

Referentie code norm:	B.04
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.

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

Toelichting:

Privacy en bescherming persoonsgegevens

Referentie code norm: [B.06](#)
Referentie brondocument: [Thema Applicatieontwikkeling](#)
BIO-BBN: Ja
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Bij het ontwikkelen van applicaties behoren privacy en bescherming van persoonsgegevens, voor zover van toepassing, te worden gewaarborgd volgens relevante wet- en regelgeving.
Verificatie methode(n): Interne controle.

Toelichting:

O-maatregel. Privacy en bescherming van persoonsgegevens

Referentie code norm: [18.1.4.2](#)
Referentie brondocument: [BIO 2019](#)
BIO-BBN: Ja
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Kwaliteitsmanagementsysteem

Referentie code norm: [B.07](#)
Referentie brondocument: [Thema Applicatieontwikkeling](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: De doelorganisatie behoort volgens een uitgestippeld ontwikkel- en onderhoudsbeleid een kwaliteitsmanagementsysteem in te richten, dat

Verificatie methode(n): ervoor zorgt dat applicatieontwikkeling en - onderhoud wordt uitgevoerd en beheerst.
Overleg bewijsstukken en/of Verklaring.

Toelichting:

Toegangsbeveiliging op programmacode

Referentie code norm: [B.08](#)
Referentie brondocument: [Thema Applicatieontwikkeling](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoren op passende wijze te worden beheerd.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Projectorganisatie

Referentie code norm: [B.09](#)
Referentie brondocument: [Thema Applicatieontwikkeling](#)
BIO-BBN:
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: I Binnen de (project-)organisatie behoort een beveiligingsfunctionaris te zijn benoemd die het systeem-ontwikkeltraject ondersteunt in de vorm van het bewaken van beveiligingsvoorschriften en die inzicht verschaft in de samenstelling van het applicatielandschap.
Verificatie methode(n): Overleg bewijsstukken en/of Verklaring.

Toelichting:

Wijzigingsbeheerprocedures voor applicaties en systemen

Referentie code norm: [U.01](#)
Referentie brondocument: [Thema Applicatieontwikkeling](#)
BIO-BBN: Ja
Relevante standaard PToLU-lijst Forum
Standaardisatie:
Samenvatting eis: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beperking software-installatie

Referentie code norm:

[U.02](#)

Referentie brondocument:

[Thema Applicatieontwikkeling](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op beveiligde wijze te beheren.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Beperkingen voor het installeren van software

Referentie code norm:

[12.6.2.1](#)

Referentie brondocument:

[BIO 2019](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Richtlijnen programmacode

Referentie code norm:

[U.03](#)

Referentie brondocument:

[Thema Applicatieontwikkeling](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis:

Voor het ontwikkelen van de (programma)code zijn specifieke regels van toepassing en behoort gebruik te zijn gemaakt van specifieke best practices

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Applicatiefunctionaliteit

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

Referentie brondocument: [Thema Applicatieontwikkeling](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Informatiesystemen behoren zo te worden ontworpen, dat de invoerfuncties, verwerkingsfuncties en uitvoerfuncties van gegevens (op het juiste moment) in het proces worden gevalideerd op juistheid, tijdigheid en volledigheid om het bedrijfsproces optimaal te kunnen ondersteunen.

Verificatie methode(n): Testen.

Toelichting:

Applicatiebouw

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

Referentie brondocument: [Thema Applicatieontwikkeling](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De bouw van applicaties inclusief programmacode behoort te worden uitgevoerd met (industrie) good practice en door individuen die beschikken over de juiste vaardigheden en tools en behoort te worden gereviewd.

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

Toelichting:

Testen systeembeveiliging

Referentie code norm: [U.09](#)

Referentie brondocument: [Thema Applicatieontwikkeling](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Tijdens ontwikkelactiviteiten behoren zowel de bedrijfsfunctionaliteiten als de beveiligingsfunctionaliteiten te worden getest.

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

Toelichting:

Beschermen testgegevens

Referentie code norm:	U.11
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

Beveiligde ontwikkelomgeving

Referentie code norm:	U.12
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie en die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Scheiding van ontwikkel-, test- en productieomgevingen

Referentie code norm:	12.1.4.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toelichting:

O-maatregel. Scheiding van ontwikkel-, test- en productieomgevingen

Referentie code norm:	12.1.4.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Applicatiekoppeling

Referentie code norm:	U.13
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De koppelingen tussen applicaties behoren te worden uitgevoerd volgens geaccordeerde koppelingsrichtlijnen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Logging en monitoring

Referentie code norm:	U.14
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Applicaties behoren faciliteiten te bieden voor logging en monitoring om ongeoorloofde en/of onjuiste activiteiten van medewerkers en storings binnen de applicatie tijdig te detecteren en vast te leggen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Applicatie-architectuur

Referentie code norm:	U.15
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De functionele en beveiligingseisen behoren in een applicatiearchitectuur, volgens architectuurvoorschriften, in samenhang te zijn vastgelegd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Tooling ontwikkelmethode

Referentie code norm:	U.16
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De ontwikkelmethode moet worden ondersteund door een tool dat de noodzakelijke faciliteiten biedt voor het effectief uitvoeren van de ontwikkelcyclus.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Richtlijnen evaluatie-ontwikkelactiviteiten

Referentie code norm:	C.01
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De projectorganisatie behoort richtlijnen voor de controle-activiteiten en rapportages te hebben geformuleerd, gericht op de evaluaties van ontwikkelactiviteiten, zoals requirements, specificaties en programmacode.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Versiebeheer

Referentie code norm:	C.02
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De projectorganisatie behoort in het systeem-ontwikkeltraject versiebeheer procesmatig en efficiënt ingericht te hebben.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Patchmanagement

Referentie code norm:	C.03
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Patchmanagement behoort procesmatig en procedureel zodanig uitgevoerd te worden, dat van de gebruikte code tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden, zodat tijdig de laatste (beveiligings)patches kunnen worden geïnstalleerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

(Software)configuratiebeheer

Referentie code norm:	C.04
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De inrichting van het configuratiebeheer behoort waarborgen te bieden dat de vastgelegde gegevens van softwareconfiguratie-items in de configuratie-administratie (CMDB) juist en volledig zijn en blijven.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Quality assurance

Referentie code norm:	C.05
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De projectorganisatie behoort een quality assurance-proces te hebben ingericht, waarmee zij de betrouwbare werking van het ontwikkel- en onderhoudsproces voor de applicatieontwikkeling kan vaststellen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Compliance-management

Referentie code norm:	C.06
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De projectorganisatie behoort een compliance-managementproces ingericht te hebben, waarmee zij de implicaties uit wet- en regelgeving en verplichtingen voortvloeiend uit overeenkomsten en beleid kan vaststellen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Technische beoordeling informatiesystemen

Referentie code norm:	C.07
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Bij veranderingen van besturingsplatforms behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact ontstaat op de activiteiten of de beveiliging van de organisatie.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Beheersorganisatie applicatieontwikkeling

Referentie code norm:	C.08
Referentie brondocument:	Thema Applicatieontwikkeling
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De projectverantwoordelijke behoort voor de software-ontwikkelpojecten een beheersorganisatie te hebben ingericht waarin de structuur van de beheersprocessen en van de betrokken functionarissen de taken, verantwoordelijkheden en bevoegdheden zijn vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Hardening van technische componenten

Referentie code norm:	SSD-1
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie voldoet aan het hardeningbeleid. De software en het platform zijn daartoe geconfigureerd volgens de bijbehorende hardeningrichtlijn. Het configureren is procesmatig en procedureel ingericht.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Veilige gegevensopslag

Referentie code norm:	SSD-2
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.
Verificatie methode(n):	Testen.
Toelichting:	

Veilige externe componenten

Referentie code norm:	SSD-3
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Applicaties maken gebruik van veilige en actief onderhouden externe componenten.
Verificatie methode(n):	Testen.

Toelichting:

Veilige communicatie

Referentie code norm:	SSD-4
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)
Samenvatting eis:	De applicatie past versleuteling toe op de communicatie van gegevens die passend is bij het classificatieniveau van de gegevens, zowel over interne als externe netwerken en controleert hierop. Van te beschermen gegevens worden alleen de noodzakelijke gecommuniceerd.
Verificatie methode(n):	Testen. Daarnaast Internet.nl.

Toelichting:

Authenticatie van gebruikers en systemen

Referentie code norm:	SSD-5
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Applicaties stellen de identiteit van gebruikers en systemen vast op basis van een mechanisme voor identificatie en authenticatie, waarbij de authenticatiegegevens in een centrale authenticatievoorziening worden beheerd.
Verificatie methode(n):	Testen.

Toelichting:

Gebruikersrechtenbeheer

Referentie code norm:	SSD-7
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De rechten die gebruikers hebben binnen een applicatie (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.
Verificatie methode(n):	Testen.

Toelichting:

Autoriseer toegang

Referentie code norm:	SSD-8
Referentie brondocument:	SSD
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie dwingt de door de opdrachtgever voorgeschreven beperkende set van rechten en privileges af met alleen de voor de gebruiker en systemen noodzakelijke toegang.
Verificatie methode(n):	Testen.

Toelichting:

O-maatregel. Beperking toegang tot informatie

Referentie code norm:	9.4.1.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.
Verificatie methode(n):	Testen.

Toelichting:

O-maatregel. Beperking toegang tot informatie

Referentie code norm:	9.4.1.2
Referentie brondocument:	BIO 2019

BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
Verificatie methode(n):	Testen.
Toelichting:	

Registreren van inlogpogingen

Referentie code norm:	SSD-9
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie registreert gelukke en mislukte login-pogingen.
Verificatie methode(n):	Testen.
Toelichting:	

Sessie-beëindiging

Referentie code norm:	SSD-12
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	SAML (authenticatie)
Samenvatting eis:	De applicatie beëindigt een sessie na een vooringestelde periode van inactiviteit van de gebruiker via automatische sessie-beëindiging,.
Verificatie methode(n):	Testen. Daarnaast Internet.nl.
Toelichting:	

Onweerlegbaarheid

Referentie code norm:	SSD-13
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie ondersteunt de onweerlegbaarheid voor daartoe aangewezen transacties via cryptografische technieken.

Verificatie methode(n): Testen.

Toelichting:

Borgen van Sessie Authenticiteit

Referentie code norm: SSD-14

Referentie brondocument: [SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie: SAML (authenticatie)

Samenvatting eis: De applicatie hanteert voor sessie-identifiers onvoorspelbare tekenreeksen en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.

Verificatie methode(n): Testen. Daarnaast Internet.nl.

Toelichting:

Scheiding van presentatie, applicatie en gegevens

Referentie code norm: SSD-15

Referentie brondocument: [SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De architectuur van een applicatie is gebaseerd op een gelaagde structuur door de presentatie-laag, de applicatielaag en de gegevens te scheiden, zodat de lagen beschermd kunnen worden binnen de netwerkzones.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Gescheiden beheerinterface

Referentie code norm: SSD-17

Referentie brondocument: [SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Beheeractiviteiten vinden plaats via een van de standaard gebruikersinterface gescheiden beheerinterface.

Verificatie methode(n): Testen.

Toelichting:

Invoer-normalisatie

Referentie code norm:	SSD-19
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie voorkomt manipulatie door alle ontvangen invoer te normaliseren alvorens die te valideren. De richtlijnen voor invoerbehandeling zijn van toepassing voor alle invoer die van buiten de applicatie komt. Dus niet alleen (eind)gebruikers, maar ook externe systemen en applicaties.
Verificatie methode(n):	Testen.

Toelichting:

Uitvoer-schoning

Referentie code norm:	SSD-20
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren naar de juiste context.
Verificatie methode(n):	Testen.

Toelichting:

Geparametriseerde queries Beperkte commando/query-toegang

Referentie code norm:	SSD-21
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie legt beperkingen aan queries en commando's op daar waar met achterliggende systemen wordt gecommuniceerd en deze communicatie wordt alleen ingericht indien strikt noodzakelijk.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Invoervalidatie

Referentie code norm:	SSD-22
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie controleert invoer (bijvoorbeeld een HTTP-request) door deze te valideren alvorens die te gebruiken.
Verificatie methode(n):	Testen.

Toelichting:

Beperkte file Includes

Referentie code norm:	SSD-23
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie voorkomt de mogelijkheid van dynamische file includes.
Verificatie methode(n):	Overleg bewijsstukken.

Toelichting:

Beperking van te versturen HTTP-headers

Referentie code norm:	SSD-24
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De webserver stuurt bij een antwoord aan een gebruiker alleen die informatie in de HTTP-headers mee die van belang is voor het functioneren van HTTP.
Verificatie methode(n):	Testen.

Toelichting:

Beperkte HTTP-methoden

Referentie code norm:	SSD-26
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis:	De webserver faciliteert alleen de HTTP- functionaliteiten die nodig zijn voor het functioneren van de applicatie.
Verificatie methode(n):	Overleg bewijsstukken en Internet.nl.

Toelichting:

Discrete foutmeldingen

Referentie code norm:	SSD-27
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De applicatie neemt in een foutmelding geen inhoudelijke foutinformatie op die misbruikt kan worden.
Verificatie methode(n):	Testen.

Toelichting:

Discreet commentaar

Referentie code norm:	SSD-28
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	De aan de gebruiker aangeboden scripts / code bevat geen commentaar dat tot misbruik kan leiden.
Verificatie methode(n):	Testen.

Toelichting:

Voorkom directory listing

Referentie code norm:	SSD-29
Referentie brondocument:	SSD
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	

Samenvatting eis: De aan de gebruiker getoonde informatie bevat geen directory listings, zodat die niet kunnen worden misbruikt.

Verificatie methode(n): Testen.

Toelichting:

Applicatie logging

Referentie code norm: SSD-30

Referentie brondocument: [SSD](#)

BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: In de applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

O-maatregel. Beschermen van informatie in logbestanden

Referentie code norm: [12.4.2.3](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

O-maatregel. Beschermen van informatie in logbestanden

Referentie code norm: [12.4.2.4](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Standaard stack

Referentie code norm: SSD-31

Referentie brondocument: [SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De (web-)applicatie(-omgeving) maakt gebruik van systeemcomponenten en voorzieningen die onderdeel zijn van een formeel gespecificeerde stack.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Bescherming tegen XML externe entiteit

Referentie code norm: SSD-32

Referentie brondocument: [SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De applicatie beperkt de mogelijkheid tot manipulatie door alle externe XML invoer te beschermen tegen entiteit injectie.

Verificatie methode(n): Testen.

Toelichting:

Veilige HTTP response headers

Referentie code norm: SSD-33

Referentie brondocument: [SSD](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De applicatie maakt gebruik van veilige response headers.

Verificatie methode(n): Testen.

Toelichting:

Informatiebeveiligingsbeleid voor leveranciersrelaties

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

O-maatregel. Informatiebeveiligingsbeleid voor leveranciersrelaties

Referentie code norm:	15.1.1.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

O-maatregel. Informatiebeveiligingsbeleid voor leveranciersrelaties

Referentie code norm:	15.1.1.3
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.
Toelichting:	

Exit-strategie

Referentie code norm:

[B.03](#)

Referentie brondocument:

[Thema Softwarepakketten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

In de overeenkomst tussen de klant en leverancier behoort een exit-strategie te zijn opgenomen, waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Bedrijfs- en beveiligingsfuncties

Referentie code norm:

[B.04](#)

Referentie brondocument:

[Thema Softwarepakketten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

Cryptografie

Referentie code norm:

[B.05](#)

Referentie brondocument:

[Thema Softwarepakketten](#)

BIO-BBN:

Ja

Relevante standaard PToLU-lijst Forum

Standaardisatie:

Samenvatting eis:

Ter bescherming van de communicatie en opslag van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

Verificatie methode(n):

Overleg bewijsstukken en/of Verklaring.

Toelichting:

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):	Overleg bewijsstukken en/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):	Overleg bewijsstukken.

Toelichting:

Levenscyclusmanagement softwarepakket

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

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Beperkingen wijziging softwarepakket

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

Referentie brondocument: [Thema Softwarepakketten](#)

BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.

Verificatie methode(n): Overleg bewijsstukken.

Toelichting:

Bedrijfscontinuïteit

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

Referentie brondocument: [Thema Softwarepakketten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.

Verificatie methode(n): Testen.

Toelichting:

Input-/output-validatie

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

Referentie brondocument: [Thema Softwarepakketten](#)

BIO-BBN:

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Het softwarepakket behoort mechanismen te bevatten voor normalisatie en validatie van invoer en voor schoning van de uitvoer.

Verificatie methode(n): Testen.

Toelichting:

Sessiebeheer

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

Toelichting:

Gegevensopslag

Referentie code norm:	U.06
Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.
Verificatie methode(n):	Testen.

Toelichting:

Communicatie

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

Toelichting:

Authenticatie

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

Toegangsautorisatie

Referentie code norm:	U.09
Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Het softwarepakket behoort een autorisatiemechanisme te bieden.
Verificatie methode(n):	Testen.
Toelichting:	

Autorisatiebeheer

Referentie code norm:	U.10
Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	De rechten die gebruikers hebben binnen een softwarepakket (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.
Verificatie methode(n):	Testen.
Toelichting:	

Logging

Referentie code norm:	U.11
-----------------------	----------------------

Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.
Verificatie methode(n):	Testen.
Toelichting:	

Application Programming Interface (API)

Referentie code norm:	U.12
Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.
Verificatie methode(n):	Testen.
Toelichting:	

Gegevensimport

Referentie code norm:	U.13
Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	
Samenvatting eis:	Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.
Verificatie methode(n):	Testen.
Toelichting:	

Versiebeheer

Referentie code norm:	C.02
Referentie brondocument:	Thema Softwarepakketten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum	
Standaardisatie:	

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

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

Toelichting:

Patchmanagement

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

Referentie brondocument: [Thema Softwarepakketten](#)

BIO-BBN: Ja

Relevante standaard PToLU-lijst Forum
Standaardisatie:

Samenvatting eis: Patchmanagement behoort procesmatig en procedureel uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code, zodat zo snel mogelijk de laatste (beveiligings-)patches kunnen worden geïnstalleerd.

Verificatie methode(n): Interne controle.

Toelichting: