



Rijksoverheid



Bijlage 1a – Informatiebeveiligingseisen Selectie Inkoopseisen Cybersecurity Overheid



Domeinen Roerende Zaken
Ministerie van Financiën

Behorende bij: Voertuigentransport met Kenmerk: IUC23-711

Samengesteld door Eelco Kums
Organisatie BV/BIK (Information Security Officer)

Datum 06-11-2024

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.

Selectiecriteria

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

Inkooponderdelen	Algemeen Ketenpartners, Toegangsbeveiliging
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	59

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

Voldoen aan BIO Hoofdstuk 1

Referentie code norm:	Ketenpartnereis 1
Referentie brondocument:	n.v.t.
BIO-BBN:	
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:	
Samenvatting eis:	Informatiebeveiliging en privacy zijn dynamische onderwerpen. Opdrachtnemer dient de maatregelen vanwege toenemende risico's en bedreigingen via een PDCA-cyclus actueel te houden.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Recht op audit

Referentie code norm:	Ketenpartnereis 3
Referentie brondocument:	n.v.t.
BIO-BBN:	
Samenvatting eis:	De opdrachtgever heeft het recht om maximaal een maal per jaar een audit te laten uitvoeren op de eisen in dit document. 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

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

Samenvatting eis: Opdrachtnemer moet zijn keten van toeleveranciers op verzoek van opdrachtgever bekendmaken en transparant zijn over de maatregelen die opdrachtnemer genomen heeft om de aan hen opgelegde eisen ook door te vertalen naar zijn 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

Samenvatting eis: Op de inrichting van het beheer van Informatiebeveiligingsincidenten is hoofdstuk 16 van de BIO 2019 van toepassing.

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

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
Samenvatting eis:	Beveiligingsincidenten worden door opdrachtnemer geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.
Verificatie methode(n):	Overleg bewijsstukken en/of verklaring

Toelichting:

Referentie code norm:	16.1.6.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Samenvatting eis:	De analyses van de beveiligingsincidenten worden door opdrachtnemer 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
Samenvatting eis:	Beveiligingsincidenten worden door opdrachtnemer 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
Samenvatting eis:	Op het bedrijfscontinuïteitsbeheer zijn de Informatiebeveiligingsaspecten van hoofdstuk 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

Samenvatting eis: Continuïteitsplannen van opdrachtnemer worden jaarlijks getest op geldigheid en bruikbaarheid.

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

Toelichting:

Referentie code norm: [17.1.3.2](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Door het uitvoeren van een expliciete risicoafweging door opdrachtnemer worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.

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

Toelichting:

Referentie code norm: [17.1.3.3](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week door opdrachtnemer 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

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. Contact met overheidsinstanties

Referentie code norm: [6.1.3.1](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Er is door opdrachtnemer 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:

Referentie code norm: [6.1.3.2](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Het contactoverzicht zoals hierboven vermeld (referentie code norm: 6.1.3.2) wordt jaarlijks door opdrachtnemer 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

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. Speciale systeemhulpmiddelen gebruiken

Referentie code norm: [9.4.4.2](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Het gebruik van systeemhulpmiddelen wordt door opdrachtnemer gelogd. De logging is een halfjaar beschikbaar voor onderzoekshulpmiddelen.

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

Toelichting:

Transport en verzenden

Referentie code norm: Ketenpartnereis 10

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Media van opdrachtnemer 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

Samenvatting eis: Opdrachtnemer heeft een vastgestelde procedure voor het fysiek transport van media.

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

Toelichting:

Referentie code norm: [8.3.3.2](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie door opdrachtnemer voldoet aan vooraf opgestelde betrouwbaarheidseisen.

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

Toelichting:

Toegangbeveiligingsbeleid

Referentie code norm: [B.01](#)

Referentie brondocument: [Thema Toegangsbeveiliging](#)

BIO-BBN:

Samenvatting eis:	Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld door opdrachtnemer op basis van bedrijfseisen en informatiebeveiligingseisen.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Eigenaarschap

Referentie code norm:	B.02
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	
Samenvatting eis:	Het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen behoren te zijn vastgelegd door opdrachtnemer.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Beveiligingsfunctie

Referentie code norm:	B.03
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	
Samenvatting eis:	Een gespecialiseerde beveiligingsfunctie dient te zijn vastgesteld die verantwoordelijk is voor het bevorderen van toegangsbeveiliging binnen de gehele organisatie van opdrachtnemer.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Cryptografie

Referentie code norm:	B.04
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	Ja
Samenvatting eis:	Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd door opdrachtnemer.
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
Samenvatting eis:	In het cryptografiebeleid van opdrachtnemer 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:

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

Toelichting:

Beveiligingsorganisatie

Referentie code norm:	B.05
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	
Samenvatting eis:	De van opdrachtnemer moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Toegangsbeveiligingsarchitectuur

Referentie code norm:	B.06
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	

Samenvatting eis: De opdrachtnemer behoort met organisatorische eisen en wensen de technische inrichting beschreven te hebben en behoort in een toegangsbeveiligingsarchitectuur te zijn vastgelegd.

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

Toelichting:

Registratieprocedure

Referentie code norm: [U.01](#)

Referentie brondocument: [Thema Toegangsbeveiliging](#)

BIO-BBN: Ja

Samenvatting eis: Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd door opdrachtnemer om toewijzing van toegangsrechten mogelijk te maken.

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

Toelichting:

Toegangsverleningsprocedure

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

Referentie brondocument: [Thema Toegangsbeveiliging](#)

BIO-BBN: Ja

Samenvatting eis: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd door opdrachtnemer om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

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

Toelichting:

O-maatregel. Gebruikers toegang verlenen

Referentie code norm: [9.2.2.3](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen van opdrachtnemer bevoegdheden hebben voor het verlenen van toegangsrechten.

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

Toelichting:

Inlogprocedure



Referentie code norm:	U.03
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	Ja
Samenvatting eis:	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure door opdrachtnemer.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

O-maatregel. Beveiligde inlogprocedures

Referentie code norm:	9.4.2.2
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Samenvatting eis:	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt door opdrachtnemer. 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 Testen.

Toelichting:

Autorisatieproces

Referentie code norm:	U.04
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	
Samenvatting eis:	Een formeel autorisatieproces dient geïmplementeerd te zijn door opdrachtnemer voor het beheersen van de toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Wachtwoordenbeheer

Referentie code norm:	U.05
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	Ja
Samenvatting eis:	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door opdrachtnemer, door middel van een beheerproces waarvan het adviseren van het personeel over de

juiste manier van omgaan met authenticatie-informatie deel uitmaakt.

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

Toelichting:

O-maatregel. Geheime authenticatie-informatie gebruiken

Referentie code norm: [9.3.1.1](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Medewerkers van opdrachtnemer worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.

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

Toelichting:

O-maatregel. Systeem voor wachtwoordbeheer

Referentie code norm: [9.4.3.2](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.) door (medewerkers van) opdrachtnemer.

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

Toelichting:

Referentie code norm: [9.4.3.3](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen door opdrachtnemer.

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

Toelichting:

Referentie code norm: [9.4.3.4](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd door opdrachtnemer.

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

Toelichting:

Referentie code norm: [9.4.3.5](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.

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

Toelichting:

Speciale toegangsrechtenbeheer

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

Referentie brondocument: [Thema Toegangsbeveiliging](#)

BIO-BBN: Ja

Samenvatting eis: Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst door opdrachtnemer.

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

Toelichting:

O-maatregel. Beheren van speciale toegangsrechten

Referentie code norm: [9.2.3.1](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld door opdrachtnemer.

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

Toelichting:

O-maatregel. Beperking toegang tot informatie

Referentie code norm: [9.4.1.1](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Er zijn maatregelen genomen door opdrachtnemer die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.

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

Toelichting:

Referentie code norm: [9.4.1.2](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

Samenvatting eis: Medewerkers van opdrachtnemer kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.

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

Toelichting:

Functiescheiding

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

Referentie brondocument: [Thema Toegangsbeveiliging](#)

BIO-BBN: Ja

Samenvatting eis: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden door opdrachtnemer om de kans op onbevoegd of onbedoeld wijzigen of misbruiken van bedrijfsmiddelen te verminderen.

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

Toelichting:

Geheime authenticatie-informatie

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

Referentie brondocument: [Thema Toegangsbeveiliging](#)

BIO-BBN:

Samenvatting eis: Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces door opdrachtnemer.

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

Toelichting:

Autorisatie

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

Referentie brondocument: [Thema Toegangsbeveiliging](#)
BIO-BBN: Ja
Samenvatting eis: Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt door opdrachtnemer in overeenstemming met het toegangsbeveiligingsbeleid.
Verificatie methode(n): Overleg bewijsstukken en/of Testen.

Toelichting:

O-maatregel. Beperking toegang tot informatie

Referentie code norm: [9.4.1.1](#)
Referentie brondocument: [BIO 2019](#)
BIO-BBN: Ja
Samenvatting eis: Er zijn maatregelen genomen door opdrachtnemer die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.
Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Referentie code norm: [9.4.1.2](#)
Referentie brondocument: [BIO 2019](#)
BIO-BBN: Ja
Samenvatting eis: Medewerkers van opdrachtnemer kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
Verificatie methode(n): Overleg bewijsstukken en/of Testen.

Toelichting:

Autorisatievoorzieningen

Referentie code norm: [U.10](#)
Referentie brondocument: [Thema Toegangsbeveiliging](#)
BIO-BBN:
Samenvatting eis: Voor autorisatiebeheer van opdrachtnemer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen beschikbaar zijn, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten.
Verificatie methode(n): Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Fysieke toegangsbeveiliging

Referentie code norm:	U.11
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	Ja
Samenvatting eis:	Opdrachtnemer dient beveiligde gebieden te wbeschermen door passende toegangsbeveiliging.
Verificatie methode(n):	Overleg bewijsstukken en/of Testen.

Toelichting:

Referentie code norm:	11.1.2.1
Referentie brondocument:	BIO 2019
BIO-BBN:	Ja
Samenvatting eis:	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, door opdrachtnemer verzonden aan opdrachtgever,
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Beoordelingsprocedure

Referentie code norm:	C.01
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	
Samenvatting eis:	Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er procedures te zijn vastgesteld door opdrachtnemer.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:

Logging en monitoring

Referentie code norm:	C.03
Referentie brondocument:	Thema Toegangsbeveiliging
BIO-BBN:	Ja
Samenvatting eis:	Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld door opdrachtnemer.
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

Samenvatting eis: De informatieverwerkende omgeving van opdrachtnemer wordt gemonitord door een SIEM en/of SOC middels detectievoorzieningen, 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:

Referentie code norm: [12.4.1.4](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

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:

Referentie code norm: [12.4.1.5](#)

Referentie brondocument: [BIO 2019](#)

BIO-BBN: Ja

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

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

Toelichting: