Document naam	Integrale Beveiliging Rijksvastgoedbedrijf Opdrachten (IBRO)
Auteur	RVB Team Integralebeveiling en Privacy
Versie	1.0
Datum	8-mrt-24
Classificatie	OPENBAAR
Toelichting	De gehele IBRO vermeldt voor alle typen geclassificeerde informatie (openbaar tot en met Staatsgeheim Zeer Geheim) welke maatregelen van toepassing zijn. De "standaard" classificatie van alle informatie is "Intern Vertrouwelijk", tenzij anders nadrukkelijk zichtbaar vermeld. De hier vermelde IBRO-maatregelen zijn vergelijkbaar met de ABDO-maatregelen zoals die door het ministerie van Defensie worden gehanteerd.
Bij tegenstrijdigheden	Bij tegenstrijdigheden geldt de zwaarste maatregel, tenzij het RVB anders besluit.
Eigenaar	Vragen, opmerkingen en toelichten kunnen gericht worden aan: postbus.rvb.informatiebeveiliging@rijksoverheid.nl

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
01	**ORGANISATORISCHE BEHEERSMAATREGELEN**								
01.01.01	Ten behoeve van de opdracht voldoet de opdrachtnemer en al zijn partners, onderaannemers en leveranciers aan de van toepassing zijnde IBRO eisen.		V	V	V	V	V	V	V
01.01.02	Bij beëindiging dient de Opdrachtnemer de door RVB (Opdrachtgever) verstrekte informatie te retourneren tenzij Opdrachtgever, eventueel in overleg met de RVB ondertekenaar van de opdracht, schriftelijk toestemming heeft verleend om de informatie te vernietigen of te behouden.			V	V	V	V	V	V
01.02.01	Op bedrijfsniveau beschikt de opdrachtnemer over een integraal informatiebeveiligingsbeleid (Opdrachtnemer, personeel, fysiek en Technologisch) dat tevens is bekrachtigd door het hoogste bestuursorgaan van de Opdrachtnemer en gecommuniceerd aan medewerkers en relevante externe partijen.				V	V	V	V	V
01.02.02	Ten behoeve van de opdracht beschikt de opdrachtnemer over een informatiebeveiligingsplan conform informatiebeveiligingsbeleid ondertekend door het hoogste bestuursorgaan van de Opdrachtnemer waarin invulling wordt gegeven aan IBRO. Dit informatiebeveiligingsplan is tevens gecommuniceerd aan medewerkers en relevante externe partijen.				V	V	V	V	V
01.02.03	Ten behoeve van de opdracht beschikt de opdrachtnemer over een informatiebeveiligingsplan conform informatiebeveiligingsbeleid, goedgekeurd door de RVB ondertekenaar van de opdracht en ondertekend door het hoogste bestuursorgaan van de Opdrachtnemer waarin invulling wordt gegeven aan IBRO.					V	V	V	V
01.02.04	Opdrachtnemer heeft de in het informatiebeveiligingsplan beschreven maatregelen eenduidig en aantoonbaar geïmplementeerd.				V	V	V	V	V
01.02.05	Opdrachtnemer heeft maatregelen getroffen om binnen 48 uur na verzoek van het RVB de geregistreerde bedrijfsmiddelen op te leveren waarmee RVB-informatie worden verwerkt.					V	V	V	V
01.02.06	Opdrachtnemer heeft een Integrale beveiligingsfunctionaris (IBF) benoemd en zonodig één of meerdere sub-IBF'n.				V	V	V	V	V
01.02.07	De IBF is namens het bestuur van de opdrachtnemer bevoegd en verantwoordelijk tot het nemen van gepaste beveiligingsmaatregelen. Het bestuur van de opdrachtnemer blijft ten alle tijden eindverantwoordelijk.				V	V	V	V	V
01.02.08	Opdrachtnemer heeft, met voorafgaande schriftelijke instemming van de RVB ondertekenaar van de (hoofd)opdracht, een integrale beveiligingsfunctionaris (IBF) benoemd en zonodig één of meerdere sub-IBF'n.				V	V	V	V	V
01.02.09	De IBF beschikt ten minste over: - De Nederlandse nationaliteit en is in dienst van het desbetreffende bedrijf; - Voldoende autonomie, bevoegdheden, slagkracht en senioriteit; - Een Verklaring Omtrent Gedrag (VOG) of een Verklaring van Geen Bezwaar (VGB) op het hoogst geldende classficatieniveau van de informatie met betrekking tot de opdracht; - Rechtstreekse en onafhankelijke toegang tot alle bestuursorganen binnen de Opdrachtnemer.				V	V	V	V	V
01.02.10	Alle organisatorische beveiligingsmaatregelen zijn volgens een schillenstructuur opgebouwd.			V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
01.02.11	Bij het samenstellen van alle organisatorische maatregelen worden de "Need-to-Be" en "Need-to-Know", "Need-to-Have" principes toegepast.				V	V	V	V	V
01.03.01	De IBF is belast met de dagelijkse zorg voor het informatiebeveiligingbeleid, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de Opdrachtnemer.				V	V	V	V	V
01.03.02	De IBF toetst periodiek, doch minimaal eenmaal per jaar, het informatiebeveiligingsplan aan de praktijk. De resultaten hiervan zijn schriftelijk vastgelegd en aan het bestuur, in afschrift aan de RVB ondertekenaar van de opdracht, gerapporteerd. Zonodig wordt het informatiebeveiligingsplan geactualiseerd.				V	V	V	V	V
01.03.03	(Beleids)wijzigingen die impact hebben op het security beleid van het bedrijf zijn aan de RVB ondertekenaar van de opdracht ter beoordeling verstrekt en zijn verwerkt in het informatiebeveiligingsplan.				V	V	V	V	V
01.03.04	Noodzakelijke wijzigingen n.a.v. een verhoogd dreigingsbeeld of een Beveiligingsincident, zijn binnen 3 werkdagen vastgelegd in het informatiebeveiligingsplan.				V	V	V	V	V
01.03.05	De IBF draagt zorg voor volledige medewerking bij controles, audits en onderzoeken bij Opdrachtnemer door of namens het RVB.				V	V	V	V	V
01.03.06	De IBF stelt zich door middel van het onderhouden van contacten met het RVB, ketenpartners, derde partijen, overheidsinstanties, omliggende bedrijven en de politie op de hoogte van zaken die het informatiebeveligingsplan aangaan.				V	V	V	V	V
01.04.01	Opdrachtnemer heeft ten behoeve van de housing en hosting van informatie een Verklaring van Eigendom, Zeggenschap en bedrijfsstructuur opgesteld en ter beschikking gesteld aan de RVB ondertekenaar van de (hoofd)opdracht.				V	V	V	V	V
01.04.02	Opdrachtnemer meldt elke voorgenomen wijziging in zeggenschap/eigendom/aandeelhouderschap van het bedrijf terstond schriftelijk aan de RVB ondertekenaar van de opdracht.				V	V	V	V	V
01.04.03	Opdrachtnemer meldt voorgenomen benoemingen van bestuurders die niet beschikken over de Nederlandse nationaliteit, terstond schriftelijk aan de RVB ondertekenaar van de hoofdopdracht.					V	V	V	V
01.04.04	Opdrachtnemer meldt voorgenomen samenwerking met buitenlandse bedrijven of overheden, terstond schriftelijk aan de RVB ondertekenaar van de (hoofd)opdracht.					V	V	V	V
01.04.05	Opdrachtnemer meldt voorgenomen splitsing, strategische samenwerking of fusie, dreigende gedeeltelijke danwel volledige overname, bedrijfsbeëindiging, surseance van betaling of faillissement terstond schriftelijk aan de RVB ondertekenaar van de (hoofd)opdracht.				V	V	V	V	V
01.04.06	Opdrachtnemer meldt voorgenomen wijziging van bedrijfsactiviteiten, locaties, sourcing, fusies of gedeeltelijke dan wel volledige overname terstond schriftelijk aan de RVB ondertekenaar van de (hoofd)opdracht.				V	V	V	V	V
01.04.07	Opdrachtnemer garandeert dat RVB geclassificeerde informatie op EU grondgebied wordt gegenereerd, bewerkt en opgeslagen.				V				
01.04.08	Opdrachtnemer garandeert dat RVB geclassificeerde informatie op Nederlands grondgebied wordt gegenereerd, bewerkt en opgeslagen.					V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
01.04.09	Opdrachtnemer plaatst enkel medewerkers met de Nederlandse nationaliteit op Vertrouwensfuncties.						V	V	V
01.05.01	Opdrachtnemer voert periodiek een programma uit ter bevordering van het beveiligingsbewustzijn waarbij de deelname verplicht en meetbaar is.				V	V	V	V	V
01.05.02	De IBF geeft ten minste eenmaal per jaar voorlichting aan medewerkers die werken aan de opdracht conform IBRO.				V	V	V	V	V
01.05.03	De IBF geeft waar nodig individueel advies en begeleiding aan medewerkers welke buitenlandse contacten hebben of op reis gaan naar risicolanden.					V	V	V	V
01.06.01	Een door de het RVB ingevulde ClassificatieAanduidingsLijst (CAL) is per hoofdopdracht aanwezig. Deze CAL is de basis voor het classificeren en/of rubriceren van alle informatie die tijdens de opdracht wordt opgesteld en/of gebruikt.		V	V	V	V	V	V	V
01.07.01	Opdrachtnemer meldt voorgenomen uitbesteding van werkzaamheden in het kader van de (hoofd)opdracht aan binnen- of buitenlandse onderaannemers/leveranciers vooraf aan de RVB ondertekenaar van de (hoofd)opdracht.					V	V	V	V
01.07.02	Voor inschakeling van een buitenlands bedrijf is vooraf schrijftelijke toestemming van de RVB ondertekenaar van de (hoofd)opdracht vereist.					V	V	V	V
01.08.01	Zonder uitdrukkelijke voorafgaande toestemming van de RVB ondertekenaar van de (hoofd)opdracht mag op geen enkele wijze publiekelijk bekend worden gemaakt welke (hoofd)opdracht voor het RVB wordt uitgevoerd.					V	V	V	V
01.08.02	Het maken van opnamen van informatie, anders dan noodzakelijk voor de uitvoering van de (hoofd)opdracht, is ongeacht het middel, niet toegestaan zonder voorafgaande schriftelijke goedkeuring van de RVB ondertekenaar van de hoofdopdracht.					V	V	V	V
01.08.03	Contactinformatie en afspraken met het RVB mogen op geen enkele wijze publiekelijk bekend worden gemaakt.					V	V	V	V
01.09.01	Er is een Incident Response Procedure (IRP) opgesteld voor het behandelen van Beveiligingsincidenten.			V	V	V	V	V	V
01.09.02	Beveiligingsincidenten dienen binnen de normstelling genoemd in tabel “Classificatie” met behulp van de IRP aan het RVB te zijn gerapporteerd.		V	V	V	V	V	V	V
01.09.03	Beveiligingsincidenten dienen binnen 1 werkdag na ontdekking aan het RVB te worden gemeld.					V	V	V	V
01.09.04	Informatie t.a.v. toegang tot en inzicht in zijn vastgelegd en worden gedurende de aangegeven periode bewaard om achteraf onderzoek naar vermoede Beveiligingsincidenten mogelijk te maken. Bewaarperiode Stg-ZG: 6 , Stg-G: 6, Stg-C: 3, Dep-V: 3 , IV:3 en IA/OB:3 maanden.			V	V	V	V	V	V
01.09.05	Informatie aangaande vastgestelde Beveiligingsincidenten wordt gedurende de aangegeven periode door de IBF bewaard. Bewaarperiode Stg-ZG: 3 , Stg-G: 3, Stg-C: 3, Dep-V: 2, IV:2, IA:2 en OB:2 jaar.			V	V	V	V	V	V
01.09.06	Werknemers dienen zwakke plekken in de beveiliging direct aan de IBF te rapporteren.		V	V	V	V	V	V	V
01.09.07	Er is een evaluatiemechanisme gedefinieerd waarmee men specifieke lessen (lessons learned) identificeert en deze verwerkt in het beveiligingsbeleid.		V	V	V	V	V	V	V
01.09.08	Er zijn disciplinaire maatregelen mogelijk tegen veroorzakers van Beveiligingsincidenten.		V	V	V	V	V	V	V
02	**PERSONELE BEHEERSMAATREGELEN**								

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
02.01.01	Er is een formele Lijst van Vertrouwensfuncties (LvV) vastgesteld door het RVB.					V	V	V	V
02.01.02	Veiligheidsonderzoeken worden aangevraagd op basis van een formeel vastgestelde LvV.					V	V	V	V
02.01.03	Een geldige VGB voor het vervullen van een Vertrouwensfunctie op A-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar.								V
02.01.04	Een geldige VGB voor het vervullen van een Vertrouwensfunctie op B-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar.							V	
02.01.05	Een geldige VGB voor het vervullen van een Vertrouwensfunctie op C-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar.						V		
02.01.06	Een geldige VOG is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 2 jaar.				V	V	V	V	V
02.01.07	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een VGB op A-niveau.							V	V
02.01.08	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een VGB op minimaal B-niveau.					V	V		
02.01.09	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een VGB op minimaal C-niveau.				V				
02.01.10	De IBF van de Opdrachtnemer vraagt tenminste drie maanden voor het verstrijken van de periode van vijf jaar na de afgifte van de meest recente VGB een hernieuwd Veiligheidsonderzoek aan.					V	V	V	V
02.01.11	Bij tussentijdse aanleiding, bijvoorbeeld bij wijziging persoonlijke omstandigheden, vraagt de IBF een hernieuwd Veiligheidsonderzoek aan.					V	V	V	V
02.01.12	Een overzichtslijst van alle de VGB's, VOG's en door opdrachtnemer verzorgde geheimhoudingsverklaringen is bij de IBF aanwezig. IBF verstrekt deze overzichtslijst minimaal 1 keer per maand aan Opdrachtgever.				V	V	V	V	V
02.02.01	De IBF heeft de medewerker/ vertrouwensfunctionaris gewezen op de verplichtingen die voortvloeien uit het bekleden van een vertrouwensfunctie.					V	V	V	V
02.02.02	Elke medewerker/vertrouwensfunctionaris heeft een door de opdrachtnemer verzorgde geheimhoudingsverklaring getekend.				V	V	V	V	V
02.03.01	Indien de vertrouwensfunctionaris de beveiligingsregels van de opdrachtnemer bewust of onbewust negeert of overtreedt, dient de IBF passende maatregelen te nemen en het RVB hierover te informeren. Grove nalatigheid of bewuste compromitatie van Staatsgeheime of vitale informatie of materieel kan aanleiding zijn tot strafrechtelijke vervolging.						V	V	V
02.03.02	De IBF ziet er op toe dat bij ontheffing uit de vertrouwensfunctie zeker gesteld is dat de medewerker geen informatie in bezit heeft.						V	V	V
02.03.03	De IBF meldt ontheffing uit een vertrouwensfunctie aan AIVD en RVB bij: - Functiewijziging van een vertrouwensfunctionaris; - Ontslag van een vertrouwensfunctionaris; - Overtreding van beveiligingsregels door een vertrouwensfunctionaris.						V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
02.03.04	Na het beëindigen van de opdracht/dienstverband worden bedrijfsmiddelen teruggegeven aan de Opdrachtnemer. Het proces hiervan is beschreven in het informatiebeveiligingsplan. Het inleveren van de bedrijfdmiddelen wordt formeel geregistreerd en opgeslagen.		V	V	V	V	V	V	V
02.04.01	Een Vertrouwensfunctionaris heeft een voorgenomen reis naar het buitenland in het kader van de opdracht onverwijld gemeld aan de IBF.						V	V	V
02.04.02	Een Vertrouwensfunctionaris heeft een voorgenomen reis naar een risicoland onverwijld gemeld aan de IBF.						V	V	V
02.04.03	Indien bij een zakelijke reis een Request for Visit (RfV) benodigd is, dient de Vertrouwensfunctionaris, via de IBF, een RfV ter goedkeuring in bij het RVB. Zonder goedgekeurd RfV kan de reis niet plaatsvinden.						V	V	V
02.04.04	De IBF brieft en debrieft Vertrouwensfunctionarissen die voorgenomen reizen naar risicolanden aan de IBF hebben gemeld. Van de brieving en debrieving worden notulen opsteld.						V	V	V
02.04.05	Een Vertrouwensfunctionaris heeft zakelijk of privéverblijf van een hemzelf/haarzelf of diens Partner in het buitenland langer dan zes aaneengesloten maanden onverwijld gemeld aan de IBF.						V	V	V
02.04.06	De IBF meldt aan het RVB het zakelijk of privéverblijf van een Vertrouwensfunctionaris of diens Partner in het buitenland langer dan zes aaneengesloten maanden.						V	V	V
02.04.07	De IBF meldt aan het RVB de voorgenomen reis van een Vetrouwensfunctionaris naar het buitenland in het kader van de opdracht of omdat het een reis naar een risicoland betreft.						V	V	V
03	**FYSIEKE BEHEERSMAATREGELEN**								
03.01.01	De fysieke beveiligingsmaatregelen zijn volgens een schillenstructuur opgebouwd met toepassing van het "Need-to-Be" principe.			V	V	V	V	V	V
03.01.02	Bij het samenstellen van alle fysieke beheersmaatregelen worden de "Need-to-Be" en "Need-to-Know", "Need-to-Have" principes toegepast.				V	V	V	V	V
03.01.03	Fysieke toegang tot het compartiment met informatie is tot op individueel niveau controleerbaar.				V	V	V	V	V
03.01.04	Fysieke toegang tot informatie of compartiment is alleen door middel van Two-factor Authenticatie verleend.						V	V	V
03.01.05	Alleen een Geautoriseerd persoon kan zelfstandig toegang krijgen tot informatie of tot een compartiment waarin zich informatie bevindt.			V	V	V	V	V	V
03.01.06	De IBF zorgt voor Autorisatie van het personeel betreffende de toegang tot informatie en de daarbij behorende infrastructuur.				V	V	V	V	V
03.01.07	Periodiek, doch minimaal 1x per jaar, wordt het betrokken personeel en bewakingspersoneel getraind in het uitvoeren van beveiligingsmaatregelen.				V	V	V	V	V
03.01.08	Toegang van personen zonder Autorisatie (zoals bezoekers) is vooraf gemeld aan de IBF.				V	V	V	V	V
03.01.09	Personen met een Autorisatie zijn binnen het compartiment herkenbaar door middel van een zichtbaar gedragen pas. Op de pas staan tenminste de naam van de persoon en een pasfoto.						V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
03.01.10	Personen zonder Autorisatie (zoals bezoekers) zijn binnen het compartiment herkenbaar door middel van een zichtbaar gedragen pas. Op de pas staat voor een ieder goed zichtbaar "bezoeker" vermeld.				V	V	V	V	V
03.01.11	Bij toegang van personen zonder Autorisatie is het personeel in een compartiment waar gewerkt wordt met of aan informatie vooraf geïnformeerd. Het personeel neemt hierop maatregelen om Compromitatie te voorkomen.				V	V	V	V	V
03.01.12	In alle compartimenten met informatie wordt personeel zonder Autorisatie (zoals bezoekers) begeleid door personeel met een Autorisatie. Van personen zonder Autorisatie is vooraf de identiteit vastgesteld en geregistreerd. De registratie hiervan wordt minimaal een jaar bewaard.				V	V	V	V	V
03.01.13	Toegang tot een compartiment met informatie door bezoekers zonder Autorisatie die niet beschikken over de Nederlandse nationaliteit is minimaal vijf werkdagen voor het bezoek gemeld via de IBF aan het RVB. Zonder toestemming van het RVB kan het bezoek niet plaatsvinden.							V	V
03.01.14	Er vindt toegangscontrole plaats bij elke fysieke beveiligingsschil.						V	V	V
03.01.15	Aan de buitenzijde van het compartiment met informatie zijn algemene beveiligingsinstructies bevestigd.					V	V	V	V
03.01.16	De uitgifte van sleutels voor toegang tot compartimenten en opbergmiddelen met informatie is geregistreerd. Bij de uitgifte van sleutels is gecontroleerd of men over een Autorisatie beschikt. De registratie hiervan wordt minimaal (NA INLEVERING) een jaar bewaard. Sleutels zijn voor zo min mogelijk personen toegankelijk.				V	V	V	V	V
03.01.17	Er zijn uitsluitend gecertificeerde sleutels gebruikt.				V	V	V	V	V
03.01.18	De IBF beheert certificaten, cijfercombinaties en reservesleutels van opbergmiddelen en compartimenten. Deze dienen opgeborgen/beveiligd te worden overeenkomstig het beveiligingsniveau van het desbetreffende informatie.				V	V	V	V	V
03.01.19	Cijfercombinaties van sloten worden, zonder dat een eerder gebruikte combinatie wordt gekozen, veranderd; - Indien een nieuw opbergmiddel of slot in gebruik wordt genomen - Indien een medewerker die de combinatie kent, wordt overgeplaatst - Indien wordt vermoed of vaststaat dat compromitatie heeft plaatsgevonden - Uiterlijk zes maanden na de laatste wijziging van de combinatie					V	V	V	V
03.01.20	Alvorens informatie buiten het reguliere, in het informtiebeveiligingsplan beschreven, proces te plaatsen, is hier schriftelijke toestemming voor verkregen van het RVB. De beveiliging van de informatie wordt hierbij op hetzelfde niveau gehouden.							V	V
03.01.21	Alvorens informatie buiten het reguliere, in het informtiebeveiligingsplan beschreven, proces te plaatsen, is hier toestemming voor verkregen van de IBF. De beveiliging van de informatie wordt hierbij op hetzelfde niveau gehouden.				V	V	V		
03.01.22	Het "Clear Desk principe" en “clear screen principe” is toegepast in alle compartimenten waar zich informatie bevindt of kan bevinden. informatie wordt niet onbeveiligd achter gelaten.			V	V	V	V	V	V
03.01.23	Beheer- en instandhoudingsmaatregelen zijn getroffen om informtiebeveiligingsmaatregelen blijvend te laten functioneren.		V	V	V	V	V	V	V

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
03.01.24	Het verlies van een authenticatiemiddel, zoals (elektronische) sleutel, dient behandeld te worden als een Beveiligingsincident.	V	V	V	V	V	V	V
03.01.25	Er zijn niet meer compartimenten dan strikt noodzakelijk.	V	V	V	V	V	V	V
03.01.26	Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan een opdracht worden de compartimenten zoveel mogelijk gecentraliseerd.			V	V	V	V	V
03.01.27	Het compartiment met informatie bevindt zich in een zone die met toegangscontrole is afgeschermd van de openbare ruimte of van ruimten die niet onder controle staan.			V	V	V	V	V
03.01.28	Beveiligingspersoneel heeft de beschikking over alarmeringsmiddelen.			V	V	V	V	V
03.01.29	Bij het verlaten van een compartiment met informatie is een sluitronde gemaakt, waarbij de deur van het opbergmiddel, het compartiment en zo mogelijk het gebouw is afgesloten. Ramen en deuren zijn afgesloten en het Indringer Detectie- en Signaleringssysteem (IDSS) is geactiveerd. Tevens is een controle op insluiping en de verzegeling van nooddeuren uitgevoerd.			V	V	V	V	V
03.01.30	Informatie moet worden beveiligd zodat enerzijds Compromitatie wordt voorkomen en anderzijds Compromitatie wordt gedetecteerd/gesignaleerd.	V	V	V	V	V	V	V
03.01.31	Bij afwezigheid van geautoriseerd personeel blijft positief bewakingsrendement gewaarborgd.			V	V	V	V	V
03.02.01	Compartimenten met informatie zijn afsluitbaar.	V	V	V	V	V	V	V
03.02.02	In het informatiebeveiligingsplan is een sluit- en sleutelplan opgenomen. Ramen, deuren en opbergmiddelen zijn afgesloten bij afwezigheid van geautoriseerd personeel. Sleutels worden op hetzelfde niveau beveiligd als informatie waar de sleutel toegang toe geeft. De sleutel is opgeborgen in een sleutelkast met een EN 1300 gecertificeerd slot. Indien het opbergmiddel en/of sleutelkast onder detectie staat/staan, kan de norm van het slot van de sleutelkast (i.c. EN 1300) vervallen.			V	V	V	V	V
03.02.03	Een compartiment waarin informatie zijn opgeborgen is afgesloten met een slot voorzien van een gecertificeerde cilinder en sleutels. Wanneer een slot met een cilinder niet kan worden toegepast, wordt een gelijkwaardig gecertificeerd of getest mechanisme gebruikt, waardoor onbevoegd betreden niet mogelijk is zonder sporen van braak.				V	V	V	V
03.02.04	Wanneer toegangsdeuren met een Elektronisch Toegangsbeheer Systeem (ETS) zijn voorzien dan zijn een deurdranger en een (elektronisch en akoestisch) alarm tegen te lang openstaan aanwezig.				V	V	V	V
03.02.05	Nooddeuren in het compartiment zijn verzegeld en alleen naar buiten toe te openen. Bij openen klinkt een elektronisch of akoestisch signaal.			V	V	V	V	V
03.02.06	Het gebouw waarin zich informatie bevinden, is tegen opklimmen beveiligd. Losse opklimmogelijkheden zijn verwijderd zoals (afval) containers en ladders. Hemelwaterafvoeren, lage muren e.d. zijn van opklimbeveiliging conform NEN 1887 voorzien.			V	V	V	V	V
03.02.07	Gevelopeningen groter dan 15 cm moeten zijn beveiligd conform NEN-EN 5096 en NEN-EN-1627 die geldt voor het compartiment.			V	V	V	V	V
03.02.08	Kelderramen en dergelijke zijn afgeschermd met traliewerk of strekmetaal conform NEN-EN 5096 en NEN-EN-1627 die geldt voor het compartiment.			V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
03.02.09	Lichtkoepels, indien niet slagvast, zijn voorzien van traliewerk of strekmetaal conform NEN-EN 5096 en NEN-EN-1627 die geldt voor het compartiment.			V	V	V	V	V
03.02.10	Het compartiment met informatie of een opbergmiddel met informatie, zijn op alle vlakken van inbraakwerende maatregelen voorzien.				V	V	V	V
03.02.11	Opbergmiddelen tot 1000 kilogram zijn chemisch verankerd.						V	V
03.02.12	Opbergmiddelen tot 1000 kilogram zijn verankerd.				V	V		
03.02.13	Bevestigingspunten van opbergmiddelen die van buitenaf bereikbaar zijn, zijn voorzien van beveiligde schroeven, bouten of moeren.				V	V	V	V
03.02.14	Opbergmiddelen zijn voorzien van Two-factor Authenticatie.					V	V	V
03.02.15	Opbergmiddelen zijn dusdanig afsluitbaar dat braak achteraf kan worden vastgesteld.			V	V	V	V	V
03.02.16	Opbergmiddelen voldoen aan de normering NEN-1143.				V	V	V	V
03.02.17	Rondom het gebouw of terrein met informatie staat een terreinafscheiding met toegangscontrole.				V	V	V	V
03.02.18	Er is beveiligingsverlichting toegepast rondom het gebouw.				V	V	V	V
03.02.19	Bij de aanleg van infrastructuur is rekening gehouden met inbraakpreventie doormiddel van het creëren van een overzichtelijk geheel, zodat de indringer niet ongezien te werk kan gaan.				V	V	V	V
03.02.20	De ramen en glazen wanden in een compartiment met informatie zijn voorzien van inkijk beperkende maatregelen				V	V	V	V
03.02.21	Er zijn voorzieningen getroffen om elektronische apparatuur die niet strikt noodzakelijk zijn voor het uitvoeren van werkzaamheden buiten de compartimenten te houden.					V	V	V
03.03.01	Het compartiment waarin een opbergmiddel met informatie is geplaatst, is voorzien van een IDSS.			V	V	V	V	V
03.03.02	De aanliggende compartimenten van het compartiment met informatie zijn voorzien van IDSS of een opbergmiddel met informatie is zelf voorzien van IDSS.			V	V	V	V	V
03.03.03	Het activeren en deactiveren van een IDSS kan alleen door middel van een Two-factor Authenticatie.					V	V	V
03.03.04	Het IDSS functioneert 24 uur per dag en 7 dagen per week, tenzij Geautoriseerd personeel aanwezig is in het compartiment.			V	V	V	V	V
03.03.05	IDSS-onderdelen zijn zodanig geplaatst dat Compromitatie van informatie of pogingen daartoe worden ontdekt en een alarm genereren.			V	V	V	V	V
03.03.06	De ruimte met informatie is binnen het IDSS als aparte zone opgenomen. Deze zone is actief wanneer er geen Geautoriseerd personeel is in de ruimte.			V	V	V	V	V
03.03.07	Doormelding van een IDSS voldoet aan de NEN 8131 of de vigerende norm geldend op moment van realisatie.			V	V	V	V	V
03.03.08	Een alarm van een IDSS leidt tot een alarmopvolging conform de NEN 8131 of de vigerende norm geldend op moment van realisatie.			V	V	V	V	V
03.03.09	Het IDSS signaleert en registreert uitval van de stroomvoorziening van de IDSS.			V	V	V	V	V
03.03.10	Het IDSS beschikt over een gegarandeerde stroomvoorziening.			V	V	V	V	V
03.03.11	Het IDSS is niet onopgemerkt te saboteren c.q. een Compromitatie wordt opgemerkt. Pogingen hiertoe zijn als een werkelijk alarm te presenteren.			V	V	V	V	V

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
03.03.12	Detectie vindt onder alle (klimatologische) omstandigheden plaats.				V	V	V	V
03.03.13	Bewegingsmelders beschikken over anti-masking maatregelen.				V	V	V	V
03.03.14	Alleen elektronische apparatuur die essentieel is voor het uitvoeren van de opdracht is toegestaan binnen de ruimten van het informatie. De keuze voor apparatuur geschiedt op basis van een risico-analyse. Een lijst van de apparatuur en de bijbehorende risico-analyse is vooraf afgestemd met het RVB en opgenomen in het informatiebeveiligingsplan.					V	V	V
03.03.15	In een ruimte met informatie zijn geen camera's, smartdevices, microfoons of andere apparatuur met een opnamefunctionaliteit aanwezig.					V	V	V
03.03.16	Beveiligingssystemen zijn geïnstalleerd en periodiek onderhouden door een gecertificeerd bedrijf conform NEN-EN 50130. Daarbij zijn de beveiligingssystemen periodiek, doch minimaal 1x per jaar, gecontroleerd.				V	V	V	V
03.03.17	Een beveiligingscamera met zicht op de toegang van een compartiment is buiten het compartiment aangebracht.				V	V	V	V
03.03.18	De bewaartermijn voor camerabeelden is 3 maanden. Camerabeelden met incidentdata dienen 1 jaar bewaard te zijn.				V	V	V	V
03.03.19	Er is een ETS voor gecontroleerde toegang tot het compartiment geïnstalleerd en in werking.				V	V	V	V
03.03.20	Als gebruik is gemaakt van elektronische sloten, zijn maatregelen getroffen om te detecteren dat toegang "onder dwang" is verleend.					V	V	V
03.03.21	Een ETS is uitgerust met een Anti Pass Back (APB) systeem.				V	V	V	V
03.03.22	Een ETS is voorzien van Logging, waarbij de logs tenminste een jaar worden bewaard.				V	V	V	V
03.03.23	Een ETS is zodanig uitgevoerd dat, wanneer het systeem uitschakelt of uitvalt, alle toegangen tot het compartiment mechanisch worden afgesloten of elektronisch afgesloten blijven.					V	V	V
03.03.24	Een ETS is dusdanig uitgevoerd dat een noodknopbediening of mechanische paniekontgrendeling binnen het compartiment op zodanige wijze is aangebracht dat bij calamiteiten het Object snel in het kader van veiligheid kan worden verlaten.					V	V	V
03.03.25	De noodknopbediening of mechanische paniekontgrendeling is van buitenaf niet bereikbaar. Na gebruik van de noodknopbediening of mechanische paniekontgrendeling dienen adequate veiligheidsmaatregelen te worden getroffen ter bescherming van de informatie.					V	V	V
03.03.26	Wanneer een beveiligingssysteem (ETS of IDSS) gekoppeld is aan een gebouwbeheersysteem, gelden de beveiligingsmaatregelen van het beveiligingssysteem ook voor het gebouwbeheersysteem.					V	V	V
03.03.27	Voorafgaand aan de ingebruikname van een compartiment en bij toevoeging of wijziging van middelen in het compartiment dient er, in overleg met het RVB, een elektronisch veiligheidsonderzoek (EVO), geluidsdempingsmeting en zoneringsmeting uitgevoerd te zijn. Eventuele maatregelen zijn afgestemd met het RVB.						V	V
03.04.01	Meldingen uit het IDSS en het ETS moeten leiden tot tijdige Interventie.	V	V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
03.04.02	Interventie vindt plaats door daartoe aangewezen en opgeleid personeel binnen de gestelde Interventietijd.		V	V	V	V	V	V	V
03.04.03	Als alleen een alarm afgaat in een compartiment en niet bij de daaromheen liggende beveiligingsschillen is te handelen alsof de omliggende alarmen ook zijn afgegaan.				V	V	V	V	V
03.04.04	Beveiligingspersoneel informeert bij een geconstateerde Compromitatie terstond de IBF.				V	V	V	V	V
03.04.05	Reactie op (technische) storingen moet leiden tot het herstellen van het gewenste beveiligingsrendement			V	V	V	V	V	V
03.04.06	Na een alarm vindt controle van het compartiment plaats door de IBF of diens gemandateerde.			V	V	V	V	V	V
03.04.07	Alarmverificatie vindt aan de buitenzijde van het compartiment met informatie plaats. Hierbij zijn alle toegangen, gevelopeningen, daken e.d. gecontroleerd.			V	V	V	V	V	V
03.04.08	Personeel dat alarmverificatie uitvoert, heeft ten tijde van de alarmverificatie niet de beschikking over sleutels of codes die toegang geven tot de informatie.			V	V	V	V	V	V
03.04.09	Een Particuliere Alarm Centrale beschikt over een justitiële erkenning en voldoet aan de NEN-EN 50518 norm.			V	V	V	V	V	V
03.05.01	informatie wordt uitsluitend buiten de fysieke ruimte gebracht als dit voor de voortgang van de werkzaamheden absoluut noodzakelijk is.					V	V	V	V
03.05.02	De IBF stelt voorschriften op voor het fysiek en/of digitaal transporteren en verzenden van informatie en zorgt dat deze worden toegepast.				V	V	V	V	V
03.05.03	informatie mag nooit mee naar huis worden genomen.					V	V	V	V
03.05.04	Transport van informatie is vooraf gemeld aan het RVB.						V	V	V
03.05.05	Transport van informatie vindt uitsluitend plaats met door Nationaal Bureau voor Verbindingsbeveiliging (NBV) goedgekeurde ICT middelen én na schriftelijke goedkeuring van het transportplan door het RVB.						V	V	V
03.06.01	Fysieke informatie is uitsluitend mee te nemen in een door Nationaal Bureau voor Verbindingsbeveiliging (NBV) goedgekeurd afsluitbaar transportmiddel.						V	V	V
03.06.02	Fysieke informatie is uitsluitend mee te nemen in een afsluitbaar transportmiddel.				V	V			
03.06.03	Transport van informatie vindt plaats: - Handcarried, al dan niet met eigen vervoer, door 1 geautoriseerde medewerker, of - Met inschakeling van een ministerieel goedgekeurd transport-/koeriersbedrijf.						V	V	
03.06.04	Transport van informatie vindt plaats: - Handcarried, al dan niet met eigen vervoer, door 1 geautoriseerde medewerker, of - Met inschakeling van een door RVB goedgekeurd transport-/koeriersbedrijf, of - Met inschakeling van een transport-/koeriersbedrijf.					V			
03.06.05	Het transport-/koeriersbedrijf waaraan de informatie zonder toezicht of begeleiding door een vertrouwensfunctionaris wordt toevertrouwd, is als onderaannemer aangemeld bij het RVB.					V	V	V	
03.06.06	Transport van informatie gaat via de kortst mogelijke weg zonder onderbrekingen. De informatie blijft onder toezicht, voertuigen worden niet onbeheerd gestald.						V	V	
03.06.07	Verzenden van informatie per post is niet toegestaan.								V

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
03.06.08	Verzending van fysieke informatie per post is uitsluitend toegestaan binnen Nederland wanneer dit aangetekend met een track en trace nummer wordt verstuurd in dubbele verpakking met een onmiddellijke ontvangstbevestiging.					V	V	
03.06.09	Verzending van informatie per post is uitsluitend binnen Nederland toegestaan wanneer dit in dubbele verpakking wordt verstuurd.				V			
03.07.01	Informatie mag zonder toestemming van het RVB niet worden meegenomen naar het buitenland.			V	V	V	V	V
03.07.02	Transport van fysieke informatie via de post naar het buitenland vindt plaats met door RVB goedgekeurde middelen, partijen en na schriftelijke goedkeuring van het transportplan door het RVB.			V	V	V	V	V
03.07.03	Transport van digitale informatie naar het buitenland vindt uitsluitend plaats met door NBV goedgekeurde middelen en na schriftelijke goedkeuring van het het RVB.			V	V	V	V	V
03.08.01	De IBF of een daartoe aangewezen en geautoriseerd persoon dient een actueel overzicht te hebben van alle RVB opdrachten en RVB informatie binnen het bedrijf.			V	V	V	V	V
03.08.02	Geregistreerd is wie informatie onder zijn berusting heeft en waar					V	V	V
03.08.03	Geregistreerd is wie werkzaamheden aan informatie heeft uitgevoerd en/of informatie heeft ingezien.						V	V
03.08.04	Informatie geproduceerd door de opdrachtnemer (of diens onderaannemers), waarbij de steller vermoedt dat bij Compromitatie voor de Staat schade kan ontstaan, is gerubriceerd. De Rubricering is door de IBF vastgesteld en geregistreerd op basis van de door RVB beschikbaargestelde CAL.				V	V	V	V
03.08.05	informatie is geregistreerd en van een rubricering voorzien.				V	V	V	V
03.08.06	informatie is geregistreerd en van een uniek exemplaarnummer voorzien.						V	V
03.08.07	Classificatie, rubriceringen en merkingen zijn conform de documenten 'Richtlijn classificeren van informatie' en 'Rubricerings categorieen' en CAL aangebracht.	V	V	V	V	V	V	V
03.08.08	De reproductie van Informatie geschiedt alleen met toestemming van degene die de Rubricering heeft vastgesteld.					V	V	V
03.08.09	Gemaakte reproducties zijn geregistreerd.					V	V	V
03.08.10	Het maken van reproducties is voorbehouden aan daartoe aangewezen geautoriseerd personeel dat ook zorgdraagt voor de registratie hiervan.					V	V	V
03.08.11	Reproducties kennen dezelfde Classificatie en rubricering als het origineel, ook als slechts delen van het origineel is gebruikt.	V	V	V	V	V	V	V
03.08.12	Er zijn niet meer reproducties gemaakt dan strikt noodzakelijk is.		V	V	V	V	V	V
03.08.13	Reproducties maken, is alleen toegestaan met door het RVB toegestane middelen.					V	V	V
03.08.14	Reproductiemiddelen worden beschouwd als een Informatiesysteem en worden minimaal op hetzelfde niveau beveiligd als de verwerkte informatie.		V	V	V	V	V	V
03.08.15	In geval van vernietiging wordt door de IBF of een aangewezen medewerker met de juiste Autorisatie een proces-verbaal van vernietiging opgemaakt.					V	V	V
03.08.16	Vernietigen van Informatie geschiedt uitsluitend conform de aanwijzingen van het RVB.				V	V	V	V
04	**CYBER BEHEERSMAATREGELEN**							

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.01.01	Er is conform de eisen een informatiebeveiligingsbeleid opgesteld in lijn met deze IBRO eisen.		V	V	V	V	V	V	V
04.01.02	Het beleid wordt periodiek beoordeeld en daar waar nodig via de continue verbeter cyclus bijgesteld.		V	V	V	V	V	V	V
04.01.03	Alle technologische beheersmaatregelen zijn volgens een schillenstructuur opgebouwd.			V	V	V	V	V	V
04.01.04	Bij het samenstellen van alle technologische beheersmaatregelen worden de "Need-to-Be", "Need-to-Know", "Need-to-Have" principes toegepast.				V	V	V	V	V
04.01.05	De IBF verstrekt, jaarlijks en op verzoek van de RVB ondertekenaar van de hoofdopdracht, de aan de Opdrachtnemer toebehorende externe IP adressen, haar Internet Service Provider(s), domeinnamen en de door de Opdrachtnemer, ten behoeve van de gerubriceerde opdracht, gebruikte hard-/software aan het RVB.					V	V	V	V
04.01.06	De IBF houdt door middel van een registratie toezicht op de locatie, uitgifte, inname en herkomst van alle door de Opdrachtnemer in ontvangst of beheer genomen digitale informatie.				V	V	V	V	V
04.01.07	De rechten van een gebruiker omvatten niet meer dan de hoogst noodzakelijke rechten voor de uitoefening van zijn/haar taak. De "Need-to-Be", "Need-to-Know", "Need-to-Have" principes moeten worden toegepast.				V	V	V	V	V
04.01.08	Er is een scheiding tussen IT-beheertaken en gebruikerstaken.				V	V	V	V	V
04.01.09	Voorafgaand aan een systeemverandering die de Integriteit van informatiesystemen kunnen aantasten is de systeemverandering door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie is een log bijgehouden.				V	V	V	V	V
04.01.10	Implementeer Role-Based Access Control (RBAC) voor IT-beheer.		V	V	V	V	V	V	V
04.01.11	Er is door de opdrachtnemer beleid voor het gebruik van mobiele apparatuur vastgesteld		V	V	V	V	V	V	V
04.01.12	Het opslaan van informatie op (mobiele) apparatuur is alleen toegestaan met producten die positief zijn geevalueerd door het Nationaal Bureau voor Verbindingsbeveiliging (NBV).				V	V	V	V	V
04.01.13	Voor het gebruik van (mobiele) apparatuur gebruikersinstructies opgesteld en verstrekt.				V	V	V	V	V
04.01.14	Een (mobiel) apparaat bevat geen kenmerken die direct herleidbaar zijn tot het RVB.				V	V	V	V	V
04.01.15	Er zijn voorzieningen om de actualiteit van anti-Malware programmatuur op (mobiele) apparaten te garanderen.			V	V	V	V	V	V
04.01.16	Na melding van verlies of diefstal is direct de communicatiemogelijkheid met de centrale applicaties afgesloten.			V	V	V	V	V	V
04.01.17	Apparatuur in het kader van BYOD of CYOD is toegestaan.		V	V	V				
04.01.18	Apparatuur in het kader van BYOD of CYOD is alleen toegestaan na goedkeuring van het bestuur van opdrachtnemer en na goedkeuring van de RVB ondertekenaar van de hoofdopdracht.					V			
04.01.19	Er is door de opdrachtnemer beleid voor telewerken vastgesteld			V	V	V			
04.01.20	Telewerken is niet toegestaan.						V	V	V
04.01.21	Mobiele apparatuur/ telewerken op basis van een terminal server verbinding zijn zo ingericht dat op de werkplek geen bedrijfsinformatie is opgeslagen (“zero footprint”) en mogelijke Malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen.		V	V	V	V			

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
04.01.22	Indien toegang tot informatie via een remote inlogvoorziening mogelijk is, is een procedure hiervoor in het Informatiebeveiligingsplan opgenomen.	V	V	V	V			
04.01.23	Voor remote toegang is gebruik gemaakt van producten die positief zijn geëvalueerd door het Nationaal Bureau voor Verbindingsbeveiliging (NBV).				V			
04.01.24	Bij gebruik van telewerken moet al het verkeer van en naar de mobiele apparatuur via cryptografie versleuteld zijn.	V	V	V	V			
04.01.25	Bij mobiele apparatuur welke zich in openbare ruimtes bevinden, zijn inkijkbeperkende maatregelen toegepast (bijv. screenfilters).	V	V	V	V			
04.03.01	Het personeel dat betrokken is bij de behandeling van informatie voortvloeiend uit de opdracht doorloopt binnen 3 maanden na aanvang en vervolgens jaarlijks, met goed gevolg, een Cyber security-awareness training.				V	V	V	V
04.03.02	De IBF, IT-beheer en het overige personeel dat betrokken is bij de behandeling informatie bezitten de benodigde ervaring, competenties en kennis door relevante opleiding en training.				V	V	V	V
04.03.03	Er is een procedure vastgesteld voor verandering/beëindiging van functie/dienstverband, contract/project of overeenkomst waarin minimaal aandacht besteed is aan het intrekken/wijzigen van toegangsrechten, innemen van ICT-bedrijfsmiddelen en fysieke informatie en de verplichtingen die ook na beëindiging van het dienstverband blijven gelden.		V	V	V	V	V	V
04.03.04	Er is een formele en gecommuniceerde disciplinaire procedure waarmee tegen medewerkers kan worden opgetreden die een inbreuk hebben gepleegd op de informatiebeveiliging.	V	V	V	V	V	V	V
04.03.05	Er is een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.	V	V	V	V	V	V	V
04.04.01	Er is een actuele registratie van ICT-bedrijfsmiddelen.		V	V	V	V	V	V
04.04.02	Er is een actuele beschrijving van de ICT-infrastructuur beschikbaar.	V	V	V	V	V	V	V
04.04.03	Alle apparatuur en systemen worden in een actuele netwerk- of configuratietekening bijgehouden. Hierin wordt duidelijk de locatie en de functie van de componenten aangegeven.	V	V	V	V	V	V	V
04.04.04	Voor elk bedrijfsproces, applicatie, informatieverzameling en overige ICT-bedrijfsmiddelen is een verantwoordelijke lijnmanager/eigenaar benoemd.	V	V	V	V	V	V	V
04.04.05	Er zijn regels vastgesteld en gedocumenteerd voor gebruik van ICT-bedrijfsmiddelen en deze zijn ter kennis gesteld aan én getekend door de gebruikers. De regels zijn als bijlage opgenomen in het informatiebeveiligingsplan.	V	V	V	V	V	V	V
04.04.06	Alleen applicaties die door IT-Beheer op een systeem geplaatst zijn, zijn gebruikt.				V	V	V	V
04.04.07	De opdrachtgever (RVB) heeft op basis van een expliciete risicoafweging een ClassificatieAanduidingsLijst (CAL) opgesteld waarmee de opdrachtnemer alle informatie moet classificeren en/of rubriceren.	V	V	V	V	V	V	V
04.04.08	De opsteller van informatie doet (op basis van de CAL) een voorstel tot Classificatie, rubricering en/of Merking en brengt deze, conform de regels, aan op de informatie. De IBF stelt de classificatie, rubricering en/of merking van de informatie vast.	V	V	V	V	V	V	V

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
04.04.09	De opsteller van de informatie zet de vastgestelde classificatie/rubricering conform de instructie aan op de informatie.	V	V	V	V	V	V	V
04.04.10	De hoogste classificatie, rubricering en/of merking van informatie is vermeld op verwijderbare en/of mobiele informatiedragers.	V	V	V	V	V	V	V
04.04.11	Beleid en procedures voor het behandelen van bedrijfsmiddelen zijn opgesteld en geimplementeerd in overeenstemming met de CAL lijst welke is vastgesteld door het RVB.	V	V	V	V	V	V	V
04.04.12	Systeemdocumentatie, wanneer deze specifieke informatie bevat over beveiligingsmaatregelen van informatie welke zich op het systeem bevinden, is op het zelfde niveau beveiligd als informatie.	V	V	V	V	V	V	V
04.04.13	Er is systeemdocumentatie aanwezig die een implementatie van een systeem beschrijft om beheer te kunnen uitvoeren.	V	V	V	V	V	V	V
04.04.14	Er zijn procedures vastgesteld en in werking gesteld voor verwijderen van informatie en de vernietiging hiervan.	V	V	V	V	V	V	V
04.04.15	Na beëindigen van de opdracht of bij het afvoeren zijn de informatiedragers fysiek vernietigd. Een proces-verbaal van vernietiging is opgesteld.					V	V	V
04.04.16	Alle digitale informatiedragers in een compartiment waar informatie op staat, zijn vercijferd. Voor ingebruikname is, in overleg met het RVB, goedkeuring verkregen over de voorgestelde oplossing.					V	V	V
04.04.17	Verwijderbare informatiedragers zijn niet onbeheerd achtergelaten.	V	V	V	V	V	V	V
04.04.18	In het geval dat informatiedragers een kortere verwachte levensduur hebben dan de informatie die ze bevatten, zijn de informatie gekopieerd wanneer 75% van de levensduur van de informatiedrager is verstreken.			V	V	V	V	V
04.05.01	Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van de RVB informatiebeveiligingseisen.		V	V	V	V	V	V
04.05.02	Alleen geautoriseerde gebruikers hebben toegang.		V	V	V	V	V	V
04.05.03	Het systeem voorkomt ongeautoriseerde toegang.		V	V	V	V	V	V
04.05.04	Toegang door derden uit hoofde van toezicht, inspectie en of audit is goedgekeurd door het RVB.						V	V
04.05.05	In het informatiebeveiligingsplan is beschreven op welke wijze gebruikers toegang hebben.			V	V	V	V	V
04.05.06	Er is één basisadministratie van authenticatieinformatie van gebruikers, op basis waarvan de gebruikers vooraf zijn geïdentificeerd en geautoriseerd.		V	V	V	V	V	V
04.05.07	Beheer op afstand is niet toegestaan.					V	V	V
04.05.08	Er is een procedure vastgesteld waarbij onderhoud op afstand alleen toegankelijk is als het strikt noodzakelijk is en een verbinding uitsluitend geactiveerd kan worden door een bevoegd functionaris (conform Beveiligingsplan).			V	V			
04.05.09	De toegang voor onderhoud op afstand door een Leverancier is alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.	V	V	V	V			
04.05.10	Beheer op afstand van apparatuur is alleen toegestaan indien gebruik is gemaakt van door het RVB goedgekeurde verbindingsmiddelen.			V	V			

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.05.11	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding is toegepast en welke toegangsrechten zijn gegeven. De risicoafweging, resultaten en maatregelen zijn weergegeven in het informatiebeveiligingsplan.			V	V	V	V	V
04.05.12	Het accountmechanisme garandeert dat handelingen uitgevoerd door een natuurlijk persoon te herleiden zijn naar zijn/haar account			V	V	V	V	V
04.05.13	Het accountmechanisme garandeert dat handelingen uitgevoerd door een Systeem account te herleiden zijn het unieke systeemaccount.			V	V	V	V	V
04.05.14	Een account mag geen indicatie geven van het privilegeniveau van de gebruiker.			V	V	V	V	V
04.05.15	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.		V	V	V	V	V	V
04.05.16	Bij uitgifte van authenticatiemiddelen is de identiteit van de gebruiker vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.		V	V	V	V	V	V
04.05.17	Gebruikers hebben alleen bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is ("Need-to-know", "need-to-use").			V	V	V	V	V
04.05.18	Gebruikers hebben alleen toegang tot een voor de functie noodzakelijk geachte set van applicaties en commando's.	V	V	V	V	V	V	V
04.05.19	Systeemprocessen draaien onder een eigen gebruikersnaam, voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.			V	V	V	V	V
04.05.20	Autorisaties en gebruikersrollen zijn per gebruiker verstrekt conform een vaste autorisatieprocedure.	V	V	V	V	V	V	V
04.05.21	Er is een noodprocedure zodat in noodgevallen een beheerdersaccount met bijbehorend wachtwoord toegankelijk is. Hierin moet beschreven zijn wie er toestemming geeft voor gebruik van dit account.	V	V	V	V	V	V	V
04.05.22	Op het wachtwoord voor een beheerdersaccount zijn de volgende eisen van toepassing: Één classificatie/rubriceringsniveau hoger dan het systeem dat er mee beheerd wordt, met als hoogste rubriceringsniveau STG. ZEER GEHEIM.	V	V	V	V	V	V	V
04.05.23	Er zijn maatregelen getroffen om het ongeautoriseerde gebruik van i/o-poorten (zoals de parallelle, seriële, USB en firewire poorten) op de werkplek(sessie) tegen te gaan.	V	V	V	V	V	V	V
04.05.24	Indien een gebruiker ingelogd is op een werkplek(sessie), dan vindt het overnemen van de werkplek(sessie) alleen plaats na toestemming van de gebruiker. Er moet een mogelijkheid zijn om overname van de werkplek(sessie) zelf te beëindigen of er moet een melding komen dat de werkplek(sessie) is beëindigd.	V	V	V	V	V	V	V
04.05.25	Administrator- of rootrechten zijn aan een beperkte groep IT-beheerders toegekend. Van deze IT-beheerders is een register bijgehouden.	V	V	V	V	V	V	V
04.05.26	De IT-beheerders administreren het gebruik van de beheerdersaccounts.	V	V	V	V	V	V	V
04.05.27	Het systeem geeft aan welke autorisaties zijn verleend aan personen en/of systemen.	V	V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.05.28	Ten aanzien van wachtwoorden geldt: - Wachtwoorden zijn op een veilige manier uitgegeven (controle identiteit van de gebruiker evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel); -Tijdelijke wachtwoorden zijn bij eerste gebruik vervangen door een ander wachtwoord; - Wachtwoorden mogen niet tegelijkertijd met het gebruikersaccount zijn verstrekt; - Wachtwoorden die standaard in software zijn meegegeven, zijn bij installatie gewijzigd.		V	V	V	V	V	V	V
04.05.29	Op het wachtwoord voor een gebruikersaccount zijn de eisen van toepassing die gelijk zijn aan het classificatie/rubriceringsniveau van het systeem waartoe toegang is verkregen.		V	V	V	V	V	V	V
04.05.30	Toegangsrechten van gebruikers zijn periodiek, minimaal halfjaarlijks, geëvalueerd. Het interval is beschreven in het informatiebeveiligingsplan.			V	V				
04.05.31	Toegangsrechten van gebruikers zijn periodiek, minimaal driemaandelijks, geëvalueerd. Het interval is beschreven in het informatiebeveiligingsplan					V	V	V	
04.05.32	Toegangsrechten van gebruikers zijn periodiek, minimaal maandelijks, geëvalueerd. Het interval is beschreven in het informatiebeveiligingsplan.								V
04.05.33	Accounts die meer dan 60 dagen niet zijn gebruikt, zijn geblokkeerd.			V	V	V	V	V	V
04.05.34	Een geblokkeerd account kan alleen worden vrijgegeven door tussenkomst van de IBF.				V	V	V	V	V
04.05.35	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: - Wachtwoorden zijn niet opgeschreven - Gebruikers delen hun wachtwoord nooit met anderen - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde - Wachtwoorden zijn niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro)			V	V	V	V	V	V
04.05.36	De minimale lengte van wachtwoorden is voor (informatie1:12, informatie2, 3:10, informatie4:9, IV:9, IA:6) karakters.			V	V	V	V	V	V
04.05.37	Wachtwoorden zijn elke (informatie1:60, informatie2:90, informatie3:90, informatie4:90, IV:90, IA:90) dagen gewijzigd. Daarbij zijn de laatste 10 gebruikte wachtwoorden niet hergebruikt.			V	V	V	V	V	V
04.05.38	Authenticatie van gebruikers is op basis van wachtwoorden.			V	V	V	V	V	V
04.05.39	Two-factor Authenticatie is gebruikt, waarbij één van de factoren een wachtwoord (weten) is en de andere factor iets hebben is.					V	V	V	V
04.05.40	Two-factor Authenticatie, waarbij één van de factoren een wachtwoord (weten) is en de andere factor vrij te kiezen, is gebruikt bij het toepassen van externe toegang.			V	V				
04.05.41	Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount draaien.		V	V	V	V	V	V	V
04.05.42	Indien tokens of biometrische toepassingen zijn gebruikt, is het niet mogelijk deze toepassingen eenvoudig buiten werking te stellen			V	V	V	V	V	V
04.05.43	Wachtwoorden bestaan uit tenminste drie van de volgende elementen: hoofd- en kleine letters, leestekens en cijfers.			V	V	V	V	V	V
04.05.44	Bij het toekennen van autorisaties is tenminste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.		V	V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.05.45	Hardware van een informatie-systeem is fysiek vast toegewezen aan dat systeem.						V	V	V
04.05.46	Voorafgaand aan het aanmelden is aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de Opdrachtnemer vastgestelde doeleinden.					V	V	V	V
04.05.47	Het aantal actieve sessies (werkplekken) per gebruiker is beperkt tot twee.			V	V				
04.05.48	Het aantal actieve sessies (werkplekken) per gebruiker is beperkt tot één.					V	V	V	V
04.05.49	Nadat voor een gebruikersaccount vijf maal een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockoutperiode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.			V	V	V			
04.05.50	Nadat voor een gebruikersaccount drie maal een verkeerd wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten. De IBF verleent daartoe toestemming.						V		
04.05.51	Nadat voor een gebruikersaccount drie maal een verkeerd wachtwoord gegeven is, wordt het account geblokkeerd totdat de gebruiker verzoekt de lockout op te heffen of het wachtwoord te resetten. De IBF verleent daartoe toestemming.							V	V
04.05.52	Nadat voor een beheeraccount vijf maal een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockoutperiode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.		V	V	V				
04.05.53	Nadat voor een beheerdersaccount drie maal een verkeerd wachtwoord gegeven is, wordt het account geblokkeerd totdat de IT-beheerder verzoekt de lockout op te heffen of het wachtwoord te resetten. De IBF verleent daartoe toestemming.					V	V	V	V
04.05.54	Het is niet toegestaan om gebruik te maken van groepsaccounts om informatie te wijzigen in bedrijfskritieke applicaties die zelf geen Identificatie-, Authenticatie- en authorisatiemechanisme hebben.		V	V					
04.05.55	Het is niet toegestaan om gebruik te maken van groepsaccounts.				V	V	V	V	V
04.05.56	Systeemaccounts zijn toegestaan onder de volgende voorwaarden: - Het is niet toegestaan om via externe toegang gebruik te maken van een systeemaccount - Het is niet toegestaan om toegang te hebben tot externe systemen (bijvoorbeeld het internet) met behulp van een systeemaccount - Het is niet toegestaan om persoonlijke of niet-werkgerelateerde informatie te verwerken met behulp van een systeemaccount			V	V	V	V	V	V
04.05.57	Er wordt automatisch gecontroleerd op het voldoen aan de wachtwoordpolicy.			V	V	V	V	V	V
04.05.58	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatieinformatie.			V	V	V	V	V	V
04.05.59	Wachtwoorden die gereset zijn en initiële wachtwoorden zijn uniek en niet hergebruikt.			V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.05.60	Gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende: - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd - Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure			V	V	V	V	V	V
04.05.61	Wachtwoorden worden NIET in originele vorm (plaintext) opgeslagen of verstuurd.			V	V	V	V	V	V
04.05.62	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het besturingssysteem.					V	V	V	V
04.05.63	Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst, zijn afgesloten.				V	V	V	V	V
04.05.64	Alle onnodige programmatuur, services, protocollen en accounts zijn uitgeschakeld, evenals alle onnodige functionaliteiten zoals scripts, drivers, bestandssystemen en systeemhulpmiddelen.			V	V	V	V	V	V
04.05.65	De door de fabrikant van de gebruikte apparatuur minimaal voorgeschreven en aangeraden beveiligingsmaatregelen zijn uitgevoerd (Hardening).			V	V	V	V	V	V
04.05.66	De toegang tot Broncode is beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.			V	V	V	V	V	V
04.06.01	Voor de Beveiliging van informatie zijn door het RVB goedgekeurde cryptografische beveiligingsvoorzieningen, componenten en procedures gebruikt.				V	V	V	V	V
04.06.02	Er is een IBF die aangesteld is voor het beheer van cryptografie.				V	V	V	V	V
04.06.03	Er is vastgesteld aan welke voorwaarden, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Dit is vastgelegd in het informatiebeveiligingsplan.				V	V	V	V	V
04.06.04	In het cryptografische sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.				V	V	V	V	V
04.06.05	De geldigheidsduur van cryptografische sleutels is bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid als onderdeel van het informatiebeveiligingsplan.				V	V	V	V	V
04.06.06	De Vertrouwelijkheid van cryptografische sleutels is gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.				V	V	V	V	V
04.06.07	Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromiteerde sleutels.				V	V	V	V	V
04.07.01	Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.				V	V	V	V	V
04.07.02	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.				V	V	V	V	V
04.07.03	Apparatuur en bekabeling is zo geplaatst en beschermd dat risico's van schade en storing van buitenaf is geminimaliseerd.				V	V	V	V	V

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
04.07.04	Ter voorkoming van compromiterende emissies zijn TEMPEST maatregelen genomen. De maatregelen zijn vooraf afgestemd met het RVB.					V	V	V
04.07.05	Ter voorkoming van emissie dienen niet gebruikte spannings-/databekabeling of losse metaalgeleiders te worden verwijderd.					V	V	V
04.07.06	Alle apparatuur gerelateerd aan het opslaan, verwerken en transporteren van de informatie is uitgerust met een voedingsfilter.					V	V	V
04.07.07	Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	V	V	V	V	V	V	V
04.07.08	Apparatuur, software en informatiedragers is geïnstalleerd, gebruikt en onderhouden volgens de voorschriften van de fabrikant voor zover dit past binnen het gebruik en onderhoudsplan van de Opdrachtnemer.	V	V	V	V	V	V	V
04.07.09	Onderhoud vindt op locatie plaats en zijn uitsluitend toegestaan met toepassing van door de RVB goedgekeurde procedures.					V	V	V
04.07.10	Apparatuur, informatie en programmatuur van de Opdrachtnemer is niet zonder vooraf schriftelijke toestemming van de IBF van de locatie meegenomen.			V	V	V	V	V
04.07.11	Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de Opdrachtnemer.	V	V	V	V	V	V	V
04.07.12	Hergebruik van ICT-bedrijfsmiddelen is toegestaan mits het dezelfde informatie betreft en is gewist door gebruik te maken van de door het RVB goedgekeurde middelen. Een proces-verbaal van vernietiging (wissen) is opgesteld.					V	V	V
04.07.13	Bij het verlaten van de werkplek vergrendelt de gebruiker de werkplek (clear screen).		V	V	V	V	V	V
04.07.14	In het "clear-desk" beleid staat minimaal dat de gebruiker informatie opbergt op de daartoe bestemde plaats indien men de Informatie niet gebruikt. Deze informatie is altijd opgeborgen in een afsluitbare opbergmogelijkheid van het juiste classificatie/rubriceringsniveau.		V	V	V	V	V	V
04.07.15	Bij het afdrukken van een informatie op een printer in een andere ruimte dan het werkstation is gebruik gemaakt van de functie "beveiligd afdrukken" (bijvoorbeeld pincode verificatie).		V	V	V	V	V	V
04.07.16	Een werkplek (sessie) is voor (informatie1 en 2 na:5, informatie3 na:10,informatie4, IV en IA na:15) minuten van inactiviteit automatisch geblokkeerd.		V	V	V	V	V	V
04.07.17	Toegangsbeveiligingslock is automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).			V	V	V	V	V
04.07.18	Voor het uitzetten/uitstellen van de schermbeveiliging op een bepaalde werkplek (sessie) gelden de volgende voorwaarden: - De schermbeveiliging is alleen uitgezet of uitgesteld als er een grote operationele noodzaak is - Voordat een schermbeveiliging wordt uitgezet of uitgesteld moet hiervoor toestemming verleend worden door de IBF - De IBF onderhoudt een registratie van werkplek (sessie) en de noodzaak waarom ontheffing is gegeven.			V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.08.01	Bedieningsprocedures bevatten actuele en accurate informatie over opstarten, afsluiten, back-uppen en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures, speciale maatregelen voor Beveiliging en zijn beschikbaar gesteld aan alle gebruikers die deze nodig hebben.			V	V	V	V	V	V
04.08.02	Er zijn procedures voor de behandeling van informatiedragers die ingaan op ontvangst, opslag, classificatie, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.			V	V	V	V	V	V
04.08.03	Systeemcomponenten - zoals Firewall, router, switches, servers - zijn in de basis ingericht volgens een standaard configuratie. Deze configuratie is vastgelegd en regelmatig gecheckt op actualiteit.		V	V	V	V	V	V	V
04.08.04	De verantwoordelijkheden en procedures voor het adequaat beheer en juist gebruik van de IT-voorzieningen waarin informatie wordt verwerkt, zijn vastgesteld.			V	V	V	V	V	V
04.08.05	Voor alle systemen is een proces van wijzigingenbeheer ingesteld. Dit proces behelst minimaal: - Het administreren van significante wijzigingen, activiteiten zijn tot de natuurlijke persoon te herleiden - Impactanalyse van mogelijke gevolgen van de wijzigingen - Goedkeuringsprocedure voor wijzigingen. De IBF is daarin opgenomen.		V	V	V	V	V	V	V
04.08.06	Instellingen van informatiebeveiligingsfuncties (b.v. securitysoftware) op het koppelvlak tussen vertrouwde en onbetrouwbare netwerken, worden automatisch op wijzigingen gecontroleerd.			V	V	V	V	V	V
04.08.07	Op basis van een risicoanalyse is bepaald wat de beschikbaarheidseis van een ICT voorziening is en wat de impact bij uitval is. Afhankelijk daarvan zijn maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen, op te vangen. De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van Beschikbaarheid. Er zijn voorzieningen geïmplementeerd om de Beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik is actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.		V	V	V	V	V	V	V
04.08.08	Er zijn beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de Beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.		V	V	V	V	V	V	V
04.08.09	In koppelpunten met externe of onbetrouwbare segmenten zijn maatregelen getroffen om onder andere DOS/DDOS ((Distributed) Denial of Service attacks) aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is .		V	V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.08.10	Er zijn gescheiden omgevingen voor Ontwikkeling, Test, Acceptatie en Productie (OTAP). De systemen en applicaties in deze omgevingen beïnvloeden systemen en applicaties in andere omgevingen niet.		V	V	V	V	V	V	V
04.08.11	Er is een fysieke scheiding aanwezig tussen de ontwikkel- en testomgeving (OT-omgeving) enerzijds en acceptatie- en de productieomgeving (AP-omgeving) anderzijds.			V	V	V	V	V	V
04.08.12	Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test, Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.		V	V	V	V	V	V	V
04.08.13	Indien er een experimenteer- of laboratorium omgeving is, is deze fysiek gescheiden van de andere omgevingen.		V	V	V	V	V	V	V
04.08.14	De scheiding tussen Ontwikkel-, Test-, Acceptatie- en Productiesystemen (OTAPsystemen) is ondersteund door formele overdrachtsprocedures.		V	V	V	V	V	V	V
04.08.15	informatie uit de productieomgeving mag alleen in de Acceptatieomgeving worden gebruikt wanneer deze op dezelfde wijze beveiligd is als in de productieomgeving. Deze informatie zijn niet in een Ontwikkel- of Testomgeving gebruikt.			V	V	V	V	V	V
04.08.16	Bij het openen van bestanden zijn deze geautomatiseerd gecontroleerd op Malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, plaats. Malware wordt in quarantaine geplaatst.		V	V	V	V	V	V	V
04.08.17	Inkomende en uitgaande e-mails zijn gecontroleerd op Malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, plaats. Malware wordt in quarantaine geplaatst.		V	V	V	V	V	V	V
04.08.18	Bestanden op een bestandssysteem, zowel server- als hostbased zijn automatisch gescand op Malware. Bij het aantreffen van Malware zijn deze in quarantaine geplaatst.		V	V	V	V	V	V	V
04.08.19	In verschillende schakels van een keten binnen de infrastructuur van een Opdrachtnemer is anti-Malware programmatuur van verschillende leveranciers toegepast.		V	V	V	V	V	V	V
04.08.20	Er zijn maatregelen getroffen om verspreiding van Malware tegen te gaan en daarmee schade te beperken (bijv. quarantaine en Compartimentering).		V	V	V	V	V	V	V
04.08.21	Er zijn continuïteitsplannen voor herstel na aanvallen met Malware waarin minimaal maatregelen voor back-ups en herstel van informatie en programmatuur zijn beschreven.		V	V	V	V	V	V	V
04.08.22	Gebruikers controleren alle van externen verkregen of door externen gebruikte digitale informatiedragers met speciaal voor dit doel ingerichte Scrubber-functionaliteiten.						V	V	V
04.08.23	Afwijkingen van het normbeeld (anomalies) met betrekking tot sessies door perimeter devices zijn onderzocht op dreigingen zoals "covert channels". Monitoring op ongebruikelijke creaties, aanwezigheid en/of beëindiging van processen teneinde infiltratie te onderkennen, vindt continu plaats.					V	V	V	V
04.08.24	Er zijn geteste procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.		V	V	V	V	V	V	V
04.08.25	Back-upstrategieën zijn vastgesteld op basis van het soort informatie (bestanden, databases, enz.), de maximaal toegestane periode waarover informatie verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.		V	V	V	V	V	V	V
04.08.26	Van back-upactiviteiten en de verblijfplaats van informatiedragers is een registratie bijgehouden.			V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.08.27	Back-ups zijn bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.		V	V	V	V	V	V	V
04.08.28	De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.		V	V	V	V	V	V	V
04.08.29	Back-ups zijn beveiligd conform de hoogste classificatie/rubricering van de informatie.		V	V	V	V	V	V	V
04.08.30	Back-ups zijn minimaal één jaar en maximaal voor de duur van de opdracht opgeslagen tenzij anders overeengekomen.		V	V	V	V	V	V	V
04.08.31	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.		V	V	V	V	V	V	V
04.08.32	Per systeem zijn gebeurtenissen vastgelegd in de Logging. Op basis van risicoanalyse is vastgesteld welke Logging noodzakelijk is. Deze Logging kan context-specifiek zijn. In het informatiebeveiligingsplan zijn de resultaten van de analyse verwerkt/vastgelegd.		V	V	V	V	V	V	V
04.08.33	Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen zijn gegenereerd.		V	V	V	V	V	V	V
04.08.34	Controle op opslag van Logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens is gelogd en leidt tot automatische alarmering van IT-beheer. Dit geldt ook als het bewaren van loginformatie niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).		V	V	V	V	V	V	V
04.08.35	Het (automatisch) overschrijven of verwijderen van logbestanden is gelogd in de nieuw aangelegde log.		V	V	V	V	V	V	V
04.08.36	Het raadplegen van logbestanden is voorbehouden aan IT-beheerders. Hierbij is de toegang beperkt tot leesrechten.		V	V	V	V	V	V	V
04.08.37	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.		V	V	V	V	V	V	V
04.08.38	Logbestanden zijn zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.		V	V	V	V	V	V	V
04.08.39	De instellingen van logmechanismen zijn zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden is het vier-ogen principe toegepast.		V	V	V	V	V	V	V
04.08.40	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden.		V	V	V	V	V	V	V
04.08.41	Loginformatie over een (vermoed) incident zijn gedurende vijf jaar bewaard.		V	V	V	V	V	V	V
04.08.42	Loginformatie dragen minimaal de classificatie/rubricering van de informatie waarop zij betrekking hebben.		V	V	V	V	V	V	V
04.08.43	Systeemklokken zijn zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.		V	V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.08.44	Alleen geautoriseerd IT-beheer kan functies en software installeren of activeren.		V	V	V	V	V	V	V
04.08.45	Programmatuur is pas geïnstalleerd op een productieomgeving nadat een formele test en acceptatie procedure is doorlopen.		V	V	V	V	V	V	V
04.08.46	Er is alleen door de Leverancier onderhouden (versies van) software gebruikt.		V	V	V	V	V	V	V
04.08.47	Er is een rollbackstrategie.		V	V	V	V	V	V	V
04.08.48	Er is een integriteitcontrolemechanisme om ervoor te zorgen dat de Integriteit van programmatuur en systeembestanden behouden blijft.		V	V	V	V	V	V	V
04.08.49	Ongeautoriseerde programmatuur is gedetecteerd.		V	V	V	V	V	V	V
04.08.50	Er is een proces ingericht voor het onderkennen en Mitigeren van technische kwetsbaarheden; dit omvat minimaal penetratietests, risicoanalyses van kwetsbaarheden en patching.		V	V	V	V	V	V	V
04.08.51	Van softwarematige voorzieningen van de Technische Infrastructuur is gecontroleerd of de laatste updates (patches) zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de Leverancier.		V	V	V	V	V	V	V
04.08.52	Kritische (security)updates en (security)patches zijn zo spoedig mogelijk doorgevoerd.		V	V	V	V	V	V	V
04.08.53	Het is niet toegestaan om een TOR (The Onion Router)/Darknet webbrowser te gebruiken.		V	V	V	V	V	V	V
04.09.01	Netwerken zijn voorzien van beheersmaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.		V	V	V	V	V	V	V
04.09.02	Er zijn technische maatregelen getroffen om te voorkomen dat interne netwerkadressen naar buiten toe routeren.		V	V	V	V	V	V	V
04.09.03	Het gebruik van draadloze communicatie is niet toegestaan.						V	V	V
04.09.04	Het gebruik van draadloze communicatie is toegestaan met toepassing van door het RVB goedgekeurde procedures en middelen.					V			
04.09.05	In geval van een externe koppeling is een "Demilitarized Zone" (DMZ) toegepast. In de DMZ zijn Monitoring systems ingericht die tenminste Packet Headers informatie en bij voorkeur full packet header en payload van het data verkeer monitoren en loggen.				V	V			
04.09.06	Alleen geïdentificeerde en geauthenticeerde apparatuur is aangesloten. De borging hiervan is beschreven in het informatiebeveiligingsplan.			V	V	V	V	V	V
04.09.07	Blokkeer al het TOR (The Onion Router)/Darknet verkeer		V	V	V	V	V	V	V
04.09.08	Beperk op basis van een risicoanalyse het interne en externe dataverkeer tot de noodzakelijke protocollen en sessies.		V	V	V	V	V	V	V
04.09.09	Het netwerk is gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de Betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.		V	V	V	V	V	V	V
04.09.10	Netwerken zijn gecontroleerd op ongeautoriseerde koppelingen.		V	V	V	V	V	V	V
04.09.11	Indien van toepassing is op aanwijzing van het RVB is medewerking verleend aan: - Het plaatsen van monitoringboxen - Het monitoren van netwerkverkeer en hosts door gebruik van monitoringboxen.					V	V	V	V
04.09.12	In geval van een externe koppeling is netwerkbased IDS of IPS toegepast.		V	V	V	V			
04.09.13	Een netwerkbased IDS of IPS is voorzien van actuele Signatures.		V	V	V	V			
04.09.14	Er is een filter geïnstalleerd voor uitgaand dataverkeer.		V	V	V	V			

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.09.15	Voor in- en uitgaand dataverkeer van en naar een onbeveiligde omgeving, zowel intern als extern, is in een DMZ een Proxy-server en/of sandbox toegepast.		V	V	V	V			
04.09.16	Een netwerk waarop informatie is opgeslagen, heeft geen verbinding met een ander netwerk, tenzij door het RVB goedgekeurde procedures en middelen zijn toegepast.						V	V	V
04.09.17	De Technische Infrastructuur is ingedeeld in segmenten. Van systemen is bijgehouden in welk segment ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in het optimale segment zit of verplaatst moet worden.		V	V	V	V	V	V	V
04.09.18	Werkstations zijn zo ingericht dat routeren van verkeer tussen verschillende segmenten of netwerken niet mogelijk is.		V	V	V	V	V	V	V
04.09.19	Informatie die wordt overgedragen tussen netwerken en systemen kan Malware bevatten en is potentieel onveilig. Maatregelen zijn genomen om besmetting te voorkomen.		V	V	V	V	V	V	V
04.09.20	Elk segment heeft een gedefinieerd beveiligingsniveau. Bij overgang van segment vindt controle plaats op protocol, inhoud en richting van de communicatie.		V	V	V	V	V	V	V
04.09.21	Beheer en audit van segmenten vindt plaats vanuit een minimaal logisch gescheiden, separaat segment.		V	V	V	V	V	V	V
04.09.22	Segmentering is ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke.		V	V	V	V	V	V	V
04.09.23	Het netwerk is gesegmenteerd (Compartimentering) op basis van "Need-to-be", "Need-to-know" en "least privilege" principes.		V	V	V	V	V	V	V
04.09.24	Alle informatie die zich niet binnen het daarvoor bestemde fysieke compartiment bevindt is versleuteld met moderne cryptografische technieken.			V	V				
04.09.25	Alle informatie die zich niet binnen het daarvoor bestemde fysieke compartiment bevindt is versleuteld met moderne cryptografische technieken.vercijferd. De toe te passen cryptografie is goedgekeurd door het RVB.					V	V	V	V
04.09.26	Informatie wordt alleen verzonden over een onbeveiligde verbinding met gebruik making van cryptografische versleuteling met moderne technieken.			V	V				
04.09.27	Informatie wordt alleen verzonden over een onbeveiligde verbinding wanneer door het RVB goedgekeurde cryptografische versleuteling is toegepast.					V	V	V	V
04.09.28	Binnenkomende programmatuur (zowel op fysieke media als gedownload) is gecontroleerd op ongeautoriseerde wijzigingen (integriteitscontrole) aan de hand van een door de Leverancier via een gescheiden kanaal geleverde checksum of certificaat.		V	V	V	V	V	V	V
04.09.29	Ontsluiting van informatie op een netwerk tussen verschillende bedrijfslocaties (WAN) is niet toegestaan.								V
04.09.30	Ontsluiting van informatie op een netwerk tussen verschillende bedrijfslocaties (WAN) is alleen toegestaan indien de verbinding tussen de locaties van een door de RVB goedgekeurde Vercijfering is voorzien.				V				
04.09.31	Ontsluiting van informatie op een netwerk tussen verschillende bedrijfslocaties (WAN) is alleen toegestaan indien de verbinding tussen de locaties van een door het RVB goedgekeurde Vercijfering is voorzien.					V	V	V	
04.09.32	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.		V	V	V	V	V	V	V

	RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.09.33	Het gebruik van clouddiensten (computing, opslag, transport) is niet toegestaan.				V	V	V	V
04.09.34	Het gebruik van Clouddienst (computing, opslag, transport) is wel toegestaan.	V	V	V				
04.09.35	Cloud-dienst (computing, opslag, transport) vindt plaats op EU-grondgebied.	V	V	V				
04.09.36	Bij toepassing van Virtualisatie is een risicoanalyse uitgevoerd. De volgende voorwaarden zijn hierbij van toepassing: - Securityfuncties draaien op fysiek gescheiden virtualisatieplatformen - Er zijn alleen systeemcomponenten gecombineerd die hetzelfde beveiligingsniveau hebben - Het ontwerp en implementatie is goedgekeurd door het RVB.					V	V	V
04.09.37	Het toepassen van VLAN's is alleen toegestaan in netwerken met een gelijk beveiligingsniveau. Het ontwerp en implementatie is goedgekeurd door het RVB.					V	V	V
04.10.01	In projecten zijn beveiligingsrisicoanalyses en maatregelbepalingen opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen in het ontwerp zijn de beveiligingsconsequenties meegenomen. Deze zijn bij Wijziging en jaarlijks gecontroleerd op actualiteit.	V	V	V	V	V	V	V
04.10.02	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.	V	V	V	V	V	V	V
04.10.03	Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	V	V	V	V	V	V	V
04.10.04	Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de Opdrachtnemer te worden toegepast.	V	V	V	V	V	V	V
04.10.05	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	V	V	V	V	V	V	V
04.10.06	Opdrachtnemers behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	V	V	V	V	V	V	V
04.10.07	Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de Opdrachtnemer	V	V	V	V	V	V	V
04.10.08	Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	V	V	V	V	V	V	V
04.10.09	Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de Opdrachtnemer.	V	V	V	V	V	V	V
04.10.10	De samenhang tussen de ICT-bedrijfsmiddelen is in kaart gebracht in een netwerktekening.	V	V	V	V	V	V	V
04.10.11	Er worden controles uitgevoerd op de invoer van informatie. Daarbij is minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige informatie, informatie die niet aan het juiste format voldoen en inconsistentie van informatie.	V	V	V	V	V	V	V

	RVB Classificatieniveau	**OB**	**IA**	**IV**	**DEP-V (TBB4)**	**STG-C (TBB3)**	**STG-G (TBB2)**	**STG-ZG (TBB1)**
04.10.12	Het Informatiesysteem bevat functies waarmee vastgesteld kan worden dat informatie correct verwerkt is. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.	V	V	V	V	V	V	V
04.10.13	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de informatie te kunnen vaststellen.	V	V	V	V	V	V	V
04.10.14	Van acceptatietesten is een log bijgehouden.	V	V	V	V	V	V	V
04.10.15	Er zijn acceptatiecriteria vastgesteld voor het testen van de Beveiliging.	V	V	V	V	V	V	V
04.10.16	Voordat systemen en/of componenten in productie genomen zijn, zijn testinformatie en testaccounts verwijderd.	V	V	V	V	V	V	V
04.10.17	Acceptatie van systemen/software vindt plaats nadat vastgesteld is dat de IBRO beveiligingsmaatregelen daadwerkelijk zijn geïmplementeerd.	V	V	V	V	V	V	V
04.10.18	Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	V	V	V	V	V	V	V
04.11.01	Indien een externe partij betrokken is bij het beheer van een omgeving, dan is daarvoor vooraf schriftelijke goedkeuring nodig van het RVB.			V	V	V	V	V
04.11.02	Indien dataopslag van informatie door een externe partij wordt gefaciliteerd, dan is daavoor vooraf schriftelijke goedkeuring nodig van het RVB.			V	V	V	V	V
04.11.03	Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot ITinfrastructuurelementen ten behoeve van de informatie van de Opdrachtnemer, of deze verwerkt, opslaat, communiceert of biedt.			V	V	V	V	V
04.11.04	Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.			V	V	V	V	V
04.11.05	Opdrachtnemers behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.			V	V	V	V	V
04.11.06	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.			V	V	V	V	V
04.12.01	De Opdrachtnemer behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, minimaal als volgt in het richten. • Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. • Maximaal dataverlies 24 uur. • Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (twee dagen van 8 uur).	V	V	V	V	V	V	V

		RVB Classificatieniveau	OB	IA	IV	DEP-V (TBB4)	STG-C (TBB3)	STG-G (TBB2)	STG-ZG (TBB1)
04.12.02	De Opdrachtnemer behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.		V	V	V	V	V	V	V
04.12.03	De Opdrachtnemer behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.		V	V	V	V	V	V	V
04.12.04	Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.		V	V	V	V	V	V	V
04.13.01	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de Opdrachtnemer om aan deze eisen te voldoen behoren voor elk informatiesysteem en de Opdrachtnemer expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.		V	V	V	V	V	V	V
04.13.02	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.		V	V	V	V	V	V	V
04.13.03	Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.		V	V	V	V	V	V	V
04.13.04	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		V	V	V	V	V	V	V
04.13.05	Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.		V	V	V	V	V	V	V
04.13.06	De aanpak van de Opdrachtnemer ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.		V	V	V	V	V	V	V
04.13.07	De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.		V	V	V	V	V	V	V
04.13.08	Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de Opdrachtnemer voor informatiebeveiliging.		V	V	V	V	V	V	V