Rijksoverheid

ABRO 2026
Beveiligingseisen

Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO)

VOORWOORD

Geopolitieke ontwikkelingen en gebeurtenissen zoals sabotageacties in Europa en spionage door statelijke actoren onderstrepen de noodzaak van het beschermen van nationale veiligheidsbelangen. De kabinetsbrede aanpak van economische veiligheid heeft deze aandacht verder versterkt. Wanneer de Rijksoverheid en politie producten en/of diensten inkopen bij een leverancier, kunnen risico's voor de nationale veiligheid ontstaan. Om deze risico's te beperken, zijn de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO) 2026 opgesteld.

De Rijksoverheid en politie beschikken over informatie, systemen, materieel en objecten, ook wel Te Beschermen Belangen. In veel gevallen zijn deze van belang voor onze nationale veiligheid en moet te allen tijde worden voorkomen dat kwaadwillenden toegang krijgen of hiervan kennis kunnen nemen. U kunt als leverancier van een opdracht voor de Rijksoverheid of politie toegang krijgen tot een Te Beschermen Belang dat raakt aan de nationale veiligheid. Dan is het belangrijk dat er voldoende waarborgen zijn om het beveiligingsniveau van het Te Beschermen Belang te garanderen. In deze gevallen zult u als leverancier moeten voldoen aan de ABRO 2026.

De ABRO 2026 is een doorontwikkeling van de ABDO 2019, de Algemene Beveiligingseisen voor Defensieopdrachten. Met het in werking treden van de ABRO 2026 gebruiken de gehele Rijksoverheid en de politie dezelfde beveiligingseisen als leveranciers worden ingeschakeld bij opdrachten waarbij Te Beschermen Belangen zijn betrokken. Voor bestaande contracten van Defensie waarop de ABDO van toepassing zijn, blijven de ABDO gelden voor de looptijd van het contract.

Vastgesteld ter invulling van artikel 2 van het Kaderbesluit ABRO rijksdienst, zoals gepubliceerd in de Staatscourant, te Den Haag op 3 december 2025.

De minister van Defensie	De minister van Binnenlandse Zaken en Koninkrijksrelaties
Ruben Brekelmans	Frank Rijkaart

INHOUDSOPGAVE

ALGEMEEN

1. Introductie

De *Rijksoverheid* en de politie zijn voor bepaalde processen, diensten en producten afhankelijk van het bedrijfsleven. Wanneer leveringen, diensten en werken worden ingekocht, acteert de *Rijksoverheid* en/of de politie als *Opdrachtgever*. Wanneer een leverancier, hierna *Opdrachtnemer*, direct of indirect betrokken is bij Rijksoverheidsopdrachten die raken aan de nationale veiligheid kunnen de *Algemene Beveiligingseisen voor Rijksoverheidsopdrachten* (ABRO) 2026 van toepassing zijn. ABRO 2026 stelt eisen aan de *Betrouwbaarheid* van een *Opdrachtnemer* om de *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid* (ook wel Exclusiviteit) van *Te Beschermen Belangen* in het kader van de nationale veiligheid te waarborgen. Indien het voor een goede uitvoering van een inkoopopdracht noodzakelijk is dat een *Opdrachtnemer* toegang krijgt tot of in aanraking komt met een *Te Beschermen Belang* (TBB) is er sprake van een *Bijzondere Opdracht*. Voor werkzaamheden aan een *Bijzondere Opdracht* is een *ABRO-Verklaring* vereist. Het *Nationaal Bureau Industrieveiligheid (NBIV)* is hiervoor het aanspreekpunt en ziet toe op de *ABRO-Verklaring*.

2. Te Beschermen Belang

Alle informatie, *Systemen,* materieel, goederen en objecten die een zekere mate van bescherming behoeven, worden aangemerkt als een *Te Beschermen Belang*. Er is een viertal *Te Beschermen Belang* categorieën, TBB 1 tot en met TBB 4, waarbij TBB 1 de zwaarst te beveiligen categorie is. Wanneer een *Te Beschermen Belang* informatie betreft of bevat, wordt ook gewerkt met *Rubriceringen* of *Merkingen,* zie ook paragraaf 3 en 4.

Te Beschermen Belangen staan voortdurend bloot aan dreigingen zoals criminaliteit, extremisme, sabotage, terrorisme en spionage. De eisen die zijn voorgeschreven voor de verschillende TBB-categorieën en *Rubriceringsniveaus* dragen bij aan de weerstand tegen deze dreigingen. Het niveau van de beveiligingsmaatregelen hangt af van de aard van het *Te Beschermen Belang* in relatie tot de specifieke dreiging. Voorafgaand aan een inkoopproces stelt de *Opdrachtgever* vast of er sprake is van een *Te Beschermen Belang* en welk beveiligingsniveau vereist is.

3. Bijzondere Informatie

Informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries wordt *Bijzondere Informatie* genoemd. *Bijzondere Informatie* wordt voorzien van een *Rubriceringsniveau* dat wordt onderscheiden in *Staatsgeheime* en niet-*Staatsgeheime Bijzondere Informatie*. Er is sprake van *Staatsgeheime Bijzondere Informatie* wanneer *Vitale* belangen van de Staat of zijn bondgenoten in het geding zijn, en indien kennisname door niet-gerechtigden kan leiden tot (zeer ernstige) schade aan deze belangen. Er is sprake van niet-*Staatsgeheime Bijzondere Informatie* indien kennisname door niet-gerechtigden kan leiden tot nadeel voor het belang van één of meer ministeries. Zie ook de samenvatting in de onderstaande tabel.

Een *Opdrachtnemer* kan in het kader van een *Bijzondere Opdracht* ook in aanraking komen met *Bijzondere Informatie* met een Politie- of internationale *Rubricering*. Een overzicht van de met nationale *Rubricering* overeenkomstige Politie-, *NAVO*- en *EU-Rubriceringen*, alsmede de meest voorkomende buitenlandse nationale *Rubriceringen* is te vinden op de website.

Bijzondere Informatie valt, afhankelijk van het *Rubriceringsniveau*, in een *TBB*-categorie. Opgemerkt wordt dat, in tegenstelling tot *Bijzondere Informatie*, een *Te Beschermen Belang* niet hoeft te zijn gerubriceerd. *Bijzondere Informatie* is altijd een *Te Beschermen Belang*, maar een *Te Beschermen Belang* is niet altijd gerubriceerd.

Onderstreept wordt dat de *ABRO* 2026 van toepassing is op een opdracht met *Rubriceringsniveau* Departementaal VERTROUWELIJK wanneer door *Opdrachtgever* is vastgesteld dat de betreffende opdracht raakt aan de nationale veiligheid, én het betreffende *Te Beschermen Belang* bij de *Opdrachtnemer* terecht kan komen.

Te Beschermen Belang*	Nederlandse Rubricering	Van toepassing wanneer:
TBB 4	Departementaal VERTROUWELIJK	Kennisname door niet-gerechtigden kan nadeel toebrengen aan het belang van één of meer ministeries.
TBB 3	Staatsgeheim CONFIDENTIEEL	Kennisname door niet-gerechtigden kan schade toebrengen aan het belang van de Staat of zijn bondgenoten.
TBB 2	Staatsgeheim GEHEIM	Kennisname door niet-gerechtigden kan ernstige schade toebrengen aan het belang van de Staat en zijn bondgenoten.
TBB 1	Staatsgeheim ZEER GEHEIM	Kennisname door niet-gerechtigden kan zeer ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.

**Bijzondere Informatie* is altijd een *Te Beschermen Belang*, maar een *Te Beschermen Belang* is niet altijd gerubriceerd.

4. Informatie voorzien van een Merking

Informatie kan ook voorzien zijn van een *Merking* (al dan niet in combinatie met een *Rubricering*). Een *Merking* heeft als doel de kring van kennisname door gerechtigden te beperken tot een specifieke groep. Ook kan een *Merking* een specifieke behandeling en beveiliging tot doel hebben. Indien informatie enkel van een *Merking* is voorzien, kan dit aanleiding zijn om informatie op het niveau van Departementaal VERTROUWELIJK te beveiligen.

5. Bijzondere Opdracht

Indien het voor een goede uitvoering van een opdracht noodzakelijk is dat een *Opdrachtnemer* toegang krijgt tot of in aanraking komt met een *Te Beschermen Belang*, is er sprake van een *Bijzondere Opdracht*. Afhankelijk van de aard van de *Bijzondere Opdracht* zijn verschillende hoofdstukken of onderdelen van *ABRO* 2026 van toepassing. Dit wordt vooraf door *NBIV* vastgesteld. Zie ook een aantal voorbeelden in onderstaande tabel.

Toepassing van TBB	Toelichting	H1	H2	H3	H4	H5
Access-to-site	Werkzaamheden voor de *Bijzondere Opdracht* vinden enkel plaats op locatie van *Opdrachtgever*	●	●			
Fysieke opslag	Fysiek opslag en verwerking van *Te Beschermen Belang* op locatie van *Opdrachtnemer*	●	●	●		
Digitale opslag	Digitale opslag en verwerking van *Bijzondere Informatie* in de digitale omgeving van *Opdrachtnemer*	●	●	●	●	
Clouddienst	Gebruik van publieke *Cloudoplossingen*	●	●	○	○	●

Bij een *Bijzondere Opdracht* wordt de *Opdrachtnemer* contractueel verplicht om maatregelen te treffen in lijn met de beveiligingseisen zoals beschreven in *ABRO 2026* voor de betreffende *TBB*-categorie. Aangezien niet alle situaties van tevoren volledig zijn in te schatten kan het in uitzonderlijke gevallen noodzakelijk zijn om op een andere manier invulling te geven aan bepaalde beveiligingseisen. In afstemming met *NBIV* en *Opdrachtgever* wordt in zo'n geval gezocht naar alternatieve of aanvullende beveiligingsmaatregelen die er gezamenlijk toe leiden dat het benodigde beveiligingsniveau wordt gerealiseerd.

6. Internationale opdrachten

Bedrijven kunnen ook in aanmerking komen voor een *Bijzondere Opdracht* van de *NAVO*, *EU, ESA* of een buitenlandse overheid. Naast nationale *Te Beschermen Belangen* kan derhalve sprake zijn van een *NAVO*-, *EU*-, *ESA*- of buitenlands *Te Beschermen Belang*. Hierbij kan de betreffende *Opdrachtgever* afwijkende of aanvullende eisen stellen. De *ABRO-Verklaring* betreft dan een *Facility Security Clearance (FSC)* en dient in dit document als zodanig te worden geïnterpreteerd. *NBIV* treedt naar het betrokken bedrijf op als tussenpersoon namens deze organisaties en landen. Vaak is het een voorwaarde dat afspraken zijn vastgelegd in een *Beveiligingsverdrag* of een *Memorandum of Understanding* (*MoU*).

7. Rollen en verantwoordelijkheden binnen de keten

De beveiliging van een *Te Beschermen Belang* vereist de borging van beveiliging binnen de keten van de betrokken partijen. Dit start bij de dienstverlening van *Opdrachtnemer* aan *Opdrachtgever*, maar betreft ook eventuele *(Toe)leveranciers* van *Opdrachtnemer*. Afhankelijk van de manier waarop een *(Toe)leverancier* betrokken is, kan deze worden aangemerkt als *Onderaannemer* en is *ABRO 2026* ook van toepassing op deze partij. *Onderaannemers* moeten dan ook beschikken over een *ABRO-Verklaring* voor het leveren van diensten of goederen in het kader van een *Bijzondere Opdracht.*

Bij de toepassing van *ABRO 2026* op een *Onderaannemer* gelden de volgende uitgangpunten:

- *Opdrachtgever* blijft te allen tijde verantwoordelijk voor een *Te Beschermen Belang* en de bijbehorende beveiligingsrisico's;
- *Opdrachtgever* is de enige partij die goedkeuring kan geven waar 'goedkeuring van *Opdrachtgever*' is voorgeschreven in een eis;
- *Opdrachtgever* is de enige partij die eventuele restrisico's ten aanzien van een *Te Beschermen Belang* mag accepteren;

- Voor overige eisen waarbij het beoogde beveiligingsdoel betrekking heeft op de samenwerking tussen *Opdrachtnemer* en *Onderaannemer* in het kader van de *Bijzondere Opdracht* geldt dat:
  - Voor de term *Opdrachtgever* de *Opdrachtnemer* wordt verondersteld;
  - Voor de term *Opdrachtnemer* de *Onderaannemer* wordt verondersteld.

Het verkrijgen van goedkeuring van, en communicatie richting, *Opdrachtgever* in het kader van *ABRO 2026* verloopt te allen tijde via *NBIV*.

8. Tussentijdse wijziging van het beveiligingsniveau

Het kan voorkomen dat (eventueel op aanwijzing van *NBIV*) naar aanleiding van een gewijzigd dreigingsbeeld of een *Beveiligingsincident* het beveiligingsniveau tijdens de uitvoering van het contract moet worden bijgesteld en nadere beveiligingsmaatregelen moeten worden geïmplementeerd. Over de eventuele gevolgen daarvan worden in nader overleg tussen *Opdrachtnemer, Opdrachtgever* en *NBIV* afspraken gemaakt.

9. Verklaring van Geen Bezwaar en equivalenten

Indien een medewerker van *Opdrachtnemer* in het kader van de *Bijzondere Opdracht* toegang heeft tot of in aanraking komt met een *Te Beschermen Belang,* heeft een medewerker in de meeste gevallen een *Verklaring van Geen Bezwaar (VGB)* nodig. In geval van een internationale opdracht, bijvoorbeeld verstrekt door *NAVO*, *EU* of *ESA,* kan een *Personnel Security Clearance (PSC)* nodig zijn. In beide gevallen wordt door de Unit Veiligheidsonderzoeken van de *AIVD* en *MIVD* een *Veiligheidsonderzoek* uitgevoerd. Waar in *ABRO 2026* wordt gerefereerd aan een *VGB*, kan ook de (internationale) equivalenten worden gelezen.

Voor sommige *Bijzondere Opdrachten*, bijvoorbeeld wanneer er enkel gewerkt wordt met TBB 4 of Departementaal VERTROUWELIJK, kan worden volstaan met een *Verklaring Omtrent het Gedrag (VOG)*. Deze wordt aangevraagd bij en afgegeven door Justis van het ministerie van Justitie en Veiligheid.

10. ABRO-Verklaring

Voordat *Opdrachtnemer* begint aan de *Bijzondere Opdracht*, dient een *Opdrachtnemer* te beschikken over een *ABRO-Verklaring* op het vereiste niveau. Deze kan door *NBIV* worden afgegeven wanneer *Opdrachtnemer* voldoet aan alle *ABRO*-eisen op het vereiste niveau. Het betreft hier expliciet een *ABRO-Verklaring* in het kader van een *Bijzondere Opdracht* en geen *Certificering*. Het is voor *Opdrachtnemer* niet toegestaan om publiekelijk kenbaar te maken dat het beschikt over een *ABRO-Verklaring*.

Bij het onderzoek voor de *ABRO-Verklaring*, ook wel het *NBIV*-Onderzoek, controleert *NBIV* of *Opdrachtnemer* voldoet aan de *ABRO*-eisen. Het onderzoek richt zich op de beveiliging van de bedrijfsvoering van betreffende *Opdrachtnemer* in het kader van de *Bijzondere Opdracht*. De *ABRO*-eisen en het *NBIV*-Onderzoek zien niet op de kwaliteit of beveiliging van het product of de dienst die gedurende de *Bijzondere Opdracht* wordt geleverd.

Een *ABRO-Verklaring* wordt afgegeven voor één *Bijzondere Opdracht*. Het kan voorkomen dat een *Opdrachtnemer* werkt aan meerdere *Bijzondere Opdrachten* en daarom meerdere *ABRO-Verklaringen* heeft. Afhankelijk van de aard van de *Bijzondere Opdracht*, kunnen verschillende *ABRO 2026* hoofdstukken van toepassing zijn. Daarom kan een *ABRO-Verklaring,* afgegeven voor een *Bijzondere Opdracht,* niet zomaar worden overgenomen voor een andere *Bijzondere Opdracht.*

ABRO 2026 vormt een integraal onderdeel van het contract tussen *Opdrachtgever* en *Opdrachtnemer*. Wijzigingen in de uitvoering van de *Bijzondere Opdracht* of het niet naleven van de in *ABRO 2026* gestelde beveiligingseisen of instructies van *NBIV* wordt derhalve als contractbreuk beschouwd. Dit kan leiden tot opschorting of intrekking van de verleende *ABRO-Verklaring*, hetgeen beëindiging van het contract tot gevolg kan hebben. Bij beëindiging van het contract dient het *Te Beschermen Belang* te worden ingeleverd of vernietigd conform de vastgestelde procedures.

11. Gebruik van bestaande Certificeringen

Een deel van de eisen die voorgeschreven worden vanuit *ABRO 2026* zijn gebaseerd op of sluiten aan bij andere overheids- en marktstandaarden, zoals Baseline Informatiebeveiliging Overheid (BIO) en ISO27002. Wanneer een *Opdrachtnemer* beschikt over *Certificering(en)* of *Assuranceverklaringen*, kan dit helpen om het proces voor het verkrijgen van een *ABRO-Verklaring* efficiënter te doorlopen. Uiteindelijk moet *NBIV* zelf kunnen vaststellen of de opzet, het bestaan en de werking van beveiligingsmaatregelen toereikend is. Een *Certificering* biedt geen garantie voor de afgifte van een *ABRO-Verklaring*.

12. Risicoanalyse

Voorafgaand aan de *Bijzondere Opdracht* voert *Opdrachtnemer* een eigen *Risicoanalyse* uit en neemt daarbij de resultaten van de door *Opdrachtgever* uitgevoerde *Risicoanalyse* mee voor het betreffende *Te Beschermen Belang*. Deze analyse vormt de basis voor het correct vaststellen en implementeren van beveiligingsmaatregelen, passend bij de *TBB*-categorie en dient doorlopend te worden meegenomen in het algehele risicomanagement van de *Opdrachtnemer*.

13. Advies en controle

NBIV is het aanspreekpunt voor en ziet toe op de *ABRO-Verklaring* in het kader van de *Bijzondere Opdracht*. Hiertoe kan *NBIV* een bezoek brengen aan *Opdrachtnemer,* bijvoorbeeld voor:

- **Advies:** Gedurende het *NBIV*-Onderzoek en tijdens de *Bijzondere Opdracht* adviseert *NBIV* over de maatregelen die moeten worden getroffen om te voldoen aan de beveiligingseisen van *ABRO 2026* passend bij de dreigingen en risico's van de *Bijzondere Opdracht*. Daarnaast kan *NBIV* zich proactief wenden tot *Opdrachtnemer*, bijvoorbeeld voor het geven van presentaties t.a.v. beveiligingsbewustzijn, het in kaart brengen van additionele dreigingen of het notificeren van potentiële slachtoffers van een *Beveiligingsincident*, om de weerbaarheid te vergroten.

- **Nalevingscontrole:** *NBIV* voert vooraf aangekondigd een formele integrale nalevingscontrole uit op de implementatie en toereikendheid van de beveiligingsmaatregelen. De resultaten worden vastgelegd in een rapport. Indien bevindingen niet tijdig worden geadresseerd, kan dat er toe leiden dat de eerder afgegeven *ABRO-Verklaring* wordt ingetrokken.

- **Beveiligingsincident:** Na *Melding* van een (mogelijk) *Beveiligingsincident* verricht *NBIV* onderzoek naar mogelijke *Compromittatie* van een *Te Beschermen Belang* en adviseert over eventuele aanvullende beveiligingsmaatregelen met als doel de schade te beperken en herhaling te voorkomen.

14. Overgangsregeling (ABDO naar ABRO)

ABRO 2026 is een doorontwikkeling van *Algemene Beveiligingseisen voor Defensieopdrachten (ABDO)* 2019 om te voorzien in een rijksbrede behoefte om de *Betrouwbaarheid* van een leveranciersketen te waarborgen waar deze raakt aan de nationale veiligheid. Hierbij zijn aanpassingen gedaan om te voorzien in verschillende behoeftes binnen de *Rijksoverheid* en Politie en zijn de beveiligingseisen geactualiseerd op de huidige wetgeving, technologische ontwikkelingen en het huidige dreigingslandschap.

Met het in werking treden van *ABRO* 2026 wordt *ABDO* 2019 geheel vervangen. Dat betekent dat op nieuwe contracten, subcontracten, projecten, deelprojecten, internationale opdrachten, opdrachten onder raamcontract, etc. *ABRO* 2026 van toepassing is. Op bestaande contracten blijft de destijds geldende versie van *ABDO* van toepassing. Hierbij wordt het hanteren van de vigerende *ABRO* aangemoedigd.

15. Aanhaling van ABRO 2026

Deze beveiligingseisen kunnen worden aangehaald als *Algemene Beveiligingseisen voor Rijksoverheidsopdrachten* 2026, afgekort *ABRO* 2026.

16. Leeswijzer

ABRO 2026 is opgedeeld in vijf hoofdstukken op basis van de categorieën: 1) Bestuur en Organisatie, 2) Personeel, 3) Fysiek, 4) Cyber en 5) Cloud. Voor sommige eisen is een nadere specificatie opgenomen in een bijlage. Wanneer dit het geval is wordt in betreffende eis expliciet verwezen naar de relevante bijlage. De in *ABRO* 2026 gebruikte afkortingen en begrippen zijn cursief weergegeven en opgenomen in de lijst met afkortingen en begrippen.

Formulieren waarnaar wordt verwezen in de eisen en bijlagen, zijn beschikbaar gesteld op de website. Daarnaast zijn op de website voor verschillende onderwerpen handreikingen opgenomen om *Opdrachtnemer* op weg te helpen bij het correct implementeren van *ABRO* 2026. De handreikingen worden periodiek aangepast en geactualiseerd.

1. BESTUUR EN ORGANISATIE

Inleiding

Adequate beveiliging van een *Bijzondere Opdracht* begint met een breed gedragen, geïmplementeerd en structureel gehandhaafd beveiligingsbeleid, bekrachtigd door het hoogste bestuursorgaan van *Opdrachtnemer*. Het *Beveiligingsplan*, de zelfinspectielijst en de beveiligingsorganisatie vormen de basis voor de beveiliging van de *Bijzondere Opdracht*.

In dit hoofdstuk is onder andere aandacht voor bedrijfsstructuur, eigendom, *Significante invloed* en *Zeggenschap*, omdat hiermee ongewenste invloed op *Opdrachtnemer* en daarmee op de uitvoering van de *Bijzondere Opdracht* mogelijk is.

ABRO 2026 vereist dat de *Opdrachtnemer* een medewerker aandraagt voor de rol van *Beveiligingsfunctionaris*. De *Beveiligingsfunctionaris* coördineert de beveiliging van de *Bijzondere Opdracht*. Door de grootte van de *Bijzondere Opdracht* of de benodigde specialismen kan de *Beveiligingsfunctionaris* worden ondersteund door één of meerdere sub-*Beveiligingsfunctionarissen* of bijvoorbeeld door een *Cyber-Beveiligingsfunctionaris*, zie ook bijlage 2.

Voor het uitvoeren van de *Bijzondere Opdracht* is het van belang dat het geheel van *(Toe)leveranciers* en *Onderaannemers* inzichtelijk is. Ook via levering van op zichzelf 'onschuldige' componenten of diensten is invloed op de *Bijzondere Opdracht* mogelijk.

Indien een *Beveiligingsincident* plaatsvindt of het vermoeden bestaat dat een *Beveiligingsincident* heeft plaatsgevonden, dient dit aan *NBIV* te worden gemeld. *Opdrachtnemer* dient een *Incident Response Procedure* (IRP) in te richten voor het afhandelen van *Beveiligingsincidenten*.

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.1	**Inrichten van de beveiligingsorganisatie**				
1.1.1	*Opdrachtnemer* beschikt over een door het *Hoogste bestuursorgaan* van de *Opdrachtnemer* bekrachtigd integraal beveiligingsbeleid dat organisatorische, personele, fysieke en cybersecurity-aspecten beschrijft. Dit beleid kent geen belemmeringen om te kunnen voldoen aan de vanuit *ABRO 2026* vereiste maatregelen.	•	•	•	•
1.1.2	*Opdrachtnemer* voert een *Risicoanalyse* uit voor de *Bijzondere Opdracht(en)* en neemt daarbij de resultaten van de door *Opdrachtgever* uitgevoerde *Risicoanalyse* mee. De *Risicoanalyse* wordt minimaal jaarlijks door *Opdrachtnemer* geëvalueerd en indien nodig herzien. Hierin is ten minste: • uitgewerkt met welke soort dreigingen *Opdrachtnemer* rekening moet houden bij het uitvoeren van de *Bijzondere Opdracht(en)*; • geïdentificeerd, geanalyseerd en geëvalueerd welke risico's van toepassing zijn op het uitvoeren van de *Bijzondere Opdracht(en)* inclusief het *Te Beschermen Belang*.	•	•	•	•
1.1.3	*Opdrachtnemer* heeft een risicomanagementproces vastgesteld en geïmplementeerd in relatie tot de *Bijzondere Opdracht(en)* en het *Te Beschermen Belang*.	•	•	•	•
1.1.4	*Opdrachtnemer* draagt een medewerker aan voor de rol van *Beveiligingsfunctionaris* bij *NBIV* conform formulier 'Aanstelling Beveiligingsfunctionaris'. Na goedkeuring wordt de *Beveiligingsfunctionaris* benoemd door *NBIV*. Afhankelijk van de aard en omvang van de *Bijzondere Opdracht(en)*, het aantal betrokken locaties en specialismen kunnen zo nodig één of meerdere sub-*Beveiligingsfunctionarissen* worden benoemd.	•	•	•	•
1.1.5	Afhankelijk van de aard en omvang van de *Bijzondere Opdracht(en)*, kan *Opdrachtnemer* een medewerker aandragen voor de rol van *Cyber-Beveiligingsfunctionaris* bij *NBIV* conform formulier 'Aanstelling Beveiligingsfunctionaris'. Na goedkeuring wordt de *Cyber-Beveiligingsfunctionaris* benoemd door *NBIV*. Zo nodig kunnen één of meerdere sub-*Cyber-Beveiligingsfunctionarissen* worden benoemd, zie ook bijlage 2.	•	•	•	•
1.1.6	De *Beveiligingsfunctionaris* fungeert als primair contactpersoon voor *NBIV*. De *Beveiligingsfunctionaris*: • is in loondienst van het betreffende bedrijf; • heeft een directe rapportagelijn met het *Hoogste bestuursorgaan* van *Opdrachtnemer*; • beschikt over voldoende mandaat, senioriteit, uitvoeringsvermogen en controle over relevante uitvoerende medewerkers om zonder tussenkomst van superieuren de verantwoordelijkheden uit te voeren; • beschikt over een *VOG* of een *VGB* op het hoogst geldende *Rubriceringsniveau* van de *Bijzondere Opdracht(en)*.	•	•	•	•
1.1.7	Indien bij de *Bijzondere Opdracht* gebruik wordt gemaakt van *Cryptografische beveiligingsoplossingen* draagt *Opdrachtnemer* een medewerker aan voor de rol van *Cryptobeheerder* bij *NBIV* conform formulier 'Aanstelling Cryptobeheerder'. Na goedkeuring wordt de *Cryptobeheerder* benoemd door *NBIV*. Zo nodig kunnen meerdere *Cryptobeheerders* worden benoemd, zie ook bijlage 3.	•	•	•	•

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.1.8	*Opdrachtnemer* beschikt over een *Beveiligingsplan* opgesteld door de *Beveiligingsfunctionaris*, conform bijlage 1. Het *Beveiligingsplan* is goedgekeurd door het *Hoogste bestuursorgaan* van *Opdrachtnemer*, geaccordeerd door *NBIV* en eenduidig geïmplementeerd.	•	•	•	•
1.1.9	Het *Beveiligingsplan* is alleen toegankelijk voor *Geautoriseerde Medewerkers* en bij het opstellen en behandelen van het *Beveiligingsplan* zijn maatregelen getroffen om de *Integriteit* en *Vertrouwelijkheid* te waarborgen, waaronder het toepassen van '*Need-to-Be*' en '*Need-to-Know*'.	•	•	•	•
1.1.10	*Opdrachtnemer* voert op verzoek van *NBIV* voor het verkrijgen van een *ABRO-Verklaring* een *Zelfinspectie* uit met behulp van de zelf-inspectielijst om in te schatten in welke mate *Opdrachtnemer* voldoet aan de op grond van *ABRO 2026* vereiste maatregelen en verstrekt deze aan *NBIV*.	•	•	•	•
1.1.11	*Opdrachtnemer* overlegt zo snel als mogelijk en uiterlijk binnen 48 uur na een daartoe strekkend verzoek van *NBIV* een actuele registratie van *Bedrijfsmiddelen* die worden gebruikt voor de *Bijzondere Opdracht(en)*.	•	•	•	•
1.1.12	Minimaal jaarlijks en op verzoek van *NBIV* verstrekt de *Beveiligingsfunctionaris* een overzicht aan *NBIV* met alle door de *Opdrachtnemer* gebruikte externe *IP-adressen*, Internet Service Provider(s) en domeinnamen, conform formulier 'IP-adressen en domeinnamen'.	•	•	•	•
1.1.13	*Opdrachtnemer* heeft bij het inrichten van beveiligingsmaatregelen rekening gehouden met vigerende wetgeving om te zorgen dat het welzijn en de veiligheid van medewerkers niet in het geding komt. Indien vigerende wetgeving, zoals de Arbowet, maakt dat bepaalde beveiligingsmaatregelen niet volledig kunnen worden geïmplementeerd, heeft *Opdrachtnemer* in afstemming met *NBIV* passende mitigerende maatregelen genomen.	•	•	•	•
1.1.14	*Opdrachtnemer* geeft volledige medewerking bij nalevingscontroles en onderzoeken in relatie tot de *Bijzondere Opdracht* bij *Opdrachtnemer* door *NBIV*.	•	•	•	•
1.1.15	Toegang tot een *Te Beschermen Belang* of *Systeem* uit hoofde van controles of audits door anderen dan wettelijke toezichthouders of andere bij wet gemandateerde instanties, is vooraf goedgekeurd door *NBIV*.	•	•	•	•
1.1.16	In het geval van controles, audits en onderzoeken in relatie tot de *Bijzondere Opdracht* door derden (zoals *NAVO*, *EU* of *ESA*), stemt *Opdrachtnemer* op voorhand af met *NBIV*.	•	•	•	•
1.1.17	Bij beëindiging van de *Bijzondere Opdracht* dient *Opdrachtnemer* alle door *Opdrachtgever* verstrekte of tijdens de *Bijzondere Opdracht* gegenereerde *Te Beschermen Belangen* te retourneren conform een met *Opdrachtgever* vastgesteld proces, tenzij *Opdrachtgever* in afstemming met *NBIV*, voorafgaand schriftelijk goedkeuring heeft verleend het *Te Beschermen Belang* te vernietigen middels goedgekeurde procedures en methodes.	•	•	•	•

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.2	**Beveiligingsfunctionaris**				
1.2.1	De *Beveiligingsfunctionaris* is ten minste verantwoordelijk voor de taken zoals beschreven in bijlage 2.	•	•	•	•
1.2.2	De *Beveiligingsfunctionaris* is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert jaarlijks een *Zelfinspectie* uit met behulp van de zelfinspectielijst. De resultaten en de opvolging van bevindingen zijn schriftelijk vastgelegd en gerapporteerd aan het *Hoogste bestuursorgaan* van *Opdrachtnemer*.	•	•	•	•
1.2.3	De *Beveiligingsfunctionaris* toetst jaarlijks en bij wijzigingen het *Beveiligingsplan* en onderliggende beveiligingsmaatregelen aan de praktijk. Hierbij wordt ten minste gebruik gemaakt van de zelfinspectielijst. De resultaten hiervan zijn schriftelijk vastgelegd en gerapporteerd aan het *Hoogste bestuursorgaan* van *Opdrachtnemer,* met afschrift aan *NBIV*. Bij wijzigingen wordt het *Beveiligingsplan* geactualiseerd.	•	•	•	•
1.2.4	Wijzigingen van beveiligingsmaatregelen of (beleids)wijzigingen die invloed hebben op de beveiligingsmaatregelen in het kader van de *Bijzondere Opdracht(en)* zijn goedgekeurd door *NBIV* en opgenomen in het *Beveiligingsplan*.	•	•	•	•
1.2.5	Wijzigingen in beveiligingsmaatregelen, bijvoorbeeld naar aanleiding van een gewijzigd dreigingsbeeld of een *Beveiligingsincident,* zijn vastgelegd in het *Beveiligingsplan* binnen de door *NBIV* gestelde termijn.	•	•	•	•
1.2.6	De *Beveiligingsfunctionaris* houdt een actuele registratie bij van alle medewerkers met een *VGB*, *VOG* en ondertekende *Geheimhoudingsverklaring(en)*.	•	•	•	•
1.2.7	De *Beveiligingsfunctionaris* beschikt over een actueel overzicht van alle *Te Beschermen Belangen* die in beheer zijn van *Opdrachtnemer*.	•	•	•	•
1.2.8	De *Beveiligingsfunctionaris* houdt een actuele registratie bij van wie werkzaamheden aan de *Bijzondere Opdracht* heeft uitgevoerd of wie toegang heeft tot een *Te Beschermen Belang*.		•	•	•
1.2.9	De *Beveiligingsfunctionaris* houdt een actuele registratie bij van wie welke *Bijzondere Informatie* in zijn bezit heeft.	•	•	•	•
1.3	**Zeggenschap en bedrijfsstructuur**				
1.3.1	*Opdrachtnemer* heeft ten behoeve van de *ABRO-Verklaring* een verklaring van eigendom, *Zeggenschap* en bedrijfsstructuur opgesteld conform formulier 'Verklaring van eigendom, Zeggenschap en bedrijfsstructuur' en verstrekt aan *NBIV*.	•	•	•	•
1.3.2	*Opdrachtnemer* legt elke voorgenomen wijziging in eigendom, *Zeggenschap* (inclusief bestuurders), bedrijfsstructuur of aandeelhouderschap (inclusief wijzigingen naar aanleiding van voorgenomen (her)financiering) van *Opdrachtnemer* onmiddellijk conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur' schriftelijk ter goedkeuring voor aan *NBIV*, zodanig dat *NBIV* de voorgenomen wijziging tijdig kan beoordelen.	•	•	•	•
1.3.3	*Opdrachtnemer* meldt elke voorgenomen samenwerking met buitenlandse bedrijven of overheden onmiddellijk schriftelijk aan *NBIV*.	•	•	•	•

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.3.4	*Opdrachtnemer* meldt elk van de volgende gebeurtenissen onmiddellijk conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur' schriftelijk aan *NBIV*: voorgenomen splitsing, strategische samenwerking, *Uitbesteding*, sourcing, fusie, verandering in *Significante invloed*, dreigende gedeeltelijke of volledige overname (inclusief binding en 'non-binding offers'), bedrijfsbeëindiging, surseance van betaling of faillissement.	•	•	•	•
1.3.5	Managementbeslissingen aangaande voorgenomen splitsing, strategische samenwerking, *Uitbesteding*, sourcing, fusie, veranderingen in *Significante invloed* en dreigende gedeeltelijke of volledige overname (inclusief binding en 'non-binding offers') worden onmiddellijk conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur' schriftelijk ter goedkeuring voorgelegd aan *NBIV*, zodanig dat *NBIV* de voorgenomen wijziging tijdig kan beoordelen.	•	•	•	•
1.3.6	*Opdrachtnemer* meldt elke voorgenomen wijziging van bedrijfsactiviteiten, locaties of veranderende omgevingsfactoren rond bestaande locaties die (in)direct betrekking hebben op een *Bijzondere Opdracht*, onmiddellijk schriftelijk aan *NBIV* conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur'.	•	•	•	•
1.3.7	Het verplaatsen van een *Te Beschermen Belang* of werkzaamheden in het kader van een *Bijzondere Opdracht* anders dan opgenomen in het *Beveiligingsplan*, gebeurt alleen na schriftelijke goedkeuring van *NBIV* en in afstemming met *Opdrachtgever*.	•	•	•	•
1.3.8	*Opdrachtnemer* verschaft duidelijkheid bij welk (onderdeel van het) bedrijf en op welke locatie de *Bijzondere Opdracht* wordt belegd en streeft maximaal naar onderbrenging van alle *Bijzondere Opdrachten* bij één duidelijk herkenbaar en juridisch en organisatorisch af te schermen (onderdeel van het) bedrijf.	•	•	•	•
1.3.9	*Opdrachtgever* kan op basis van een *Risicoanalyse*, in afstemming met *NBIV* vaststellen dat er additionele risico's zijn waarvoor aanvullende beveiligingsmaatregelen moeten worden getroffen door *Opdrachtnemer*. Voorbeelden van aanvullende beveiligingsmaatregelen zijn verplichte verwerking of behandeling op Nederlands grondgebied door een in Nederland gevestigde rechtspersoon.	•	•	•	•
1.4	**Rubricering en aanvullende beveiligingsafspraken**				
1.4.1	*Opdrachtnemer* beschikt over een actueel, door *Opdrachtgever* ingevuld en geaccordeerd, opdrachtspecifiek overzicht van *Te Beschermen Belangen*, zie bijlage 4.	•	•	•	•
1.4.2	Indien de *Bijzondere Opdracht* met een buitenlandse *Opdrachtgever* aanvullende of afwijkende specifieke beveiligingsmaatregelen vereist, beschikt *Opdrachtnemer* over een actuele *Project Security Instruction (PSI)* of *Security Aspect Letter (SAL)*.	•	•	•	•
1.4.3	E-mailverkeer tussen *Opdrachtgever* en *Opdrachtnemer* is, ook wanneer het geen *Bijzondere Informatie* bevat, zodanig beveiligd (zoals middels Forced TLS) dat de *Vertrouwelijkheid* en *Integriteit* gewaarborgd is.	•	•	•	•
1.4.4	*Opdrachtnemer* treft maatregelen om te waarborgen dat *Bijzondere Informatie* met verschillende *Rubriceringsdomeinen* en *-niveaus* gescheiden wordt verwerkt en opgeslagen.	•	•	•	•

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.4.5	Voorafgaand aan het genereren van informatie in het kader van de *Bijzondere Opdracht* waarop redelijkerwijs een *Rubricering* van toepassing is, doet de *Beveiligingsfunctionaris* een verzoek tot *Rubricering* aan *Opdrachtgever*. Na vaststelling door *Opdrachtgever* wordt deze informatie als zodanig gegenereerd, geregistreerd en behandeld door *Opdrachtnemer*.	•	•	•	•
1.4.6	In geval van onvoorziene situaties, bijvoorbeeld door een gewijzigd dreigingsbeeld, nieuwe aanvalsmethodieken, uitvoering van meerdere *Bijzondere Opdrachten* op een locatie of *Systeem*, of kennisaggregatie, kunnen binnen redelijke grenzen additionele organisatorische, personele, fysieke of *Cyber* beveiligingsmaatregelen worden voorgeschreven. *Opdrachtnemer* geeft invulling aan deze beveiligingsmaatregelen.	•	•	•	•
1.5	**Onderaannemers en (toe)leveranciers**				
1.5.1	*Opdrachtnemer* legt voorgenomen *Uitbesteding* van werkzaamheden in het kader van een *Bijzondere Opdracht* aan een *Onderaannemer* vooraf ter goedkeuring voor aan de *Opdrachtgever* en *NBIV* conform formulier 'Aanvraag Onderaannemer'.	•	•	•	•
1.5.2	*Opdrachtnemer* heeft in afstemming met *Opdrachtgever* en *NBIV* een opdrachtspecifiek overzicht van *Te Beschermen Belangen* voor elke bij de *Bijzondere Opdracht* betrokken *Onderaannemer* en eventuele achterliggende *Onderaannemers* opgesteld, zodanig dat voor *Opdrachtgever* en *NBIV* inzichtelijk is welke *Onderaannemer* toegang heeft tot welke *Te Beschermen Belangen*, zie ook bijlage 4.	•	•	•	•
1.5.3	Na goedkeuring van *Opdrachtgever* en *NBIV* tot *Uitbesteding* heeft *Opdrachtnemer* in het contract met *Onderaannemer* die op enigerwijze in aanraking komen met een *Te Beschermen Belang* de vigerende *ABRO* bedongen.	•	•	•	•
1.5.4	Na toestemming van *NBIV* op basis van een door een *Buitenlandse partner* verstrekte *Facility Security Clearance*, heeft *Opdrachtnemer* in het contract met de buitenlandse *Onderaannemer(s)* de in het betrokken land geldende beveiligingseisen bedongen. Een overzicht van *Te Beschermen Belangen* is hierbij verstrekt aan *NBIV*.	•	•	•	•
1.5.5	*Opdrachtnemer* bepaalt in afstemming met *Opdrachtgever* op basis van een *Risicoanalyse* of de door *(Toe)leverancier(s)* geleverde producten en/of diensten een risico vormen voor de *Bijzondere Opdracht*. Indien dit het geval is wordt de *(Toe)leverancier* als *Onderaannemer* aangemerkt en heeft *Opdrachtnemer* de vigerende *ABRO* contractueel bedongen.	•	•	•	•
1.5.6	*Opdrachtnemer* draagt de verantwoordelijkheid voor het voldoen aan de eisen uit *ABRO 2026* door *Onderaannemer(s)*.	•	•	•	•
1.5.7	*Opdrachtnemer* heeft een proces vastgesteld en geïmplementeerd om veranderingen in en naleving van gemaakte beveiligingsafspraken met *Onderaannemer(s)* doorlopend te beheren, controleren en te evalueren. In geval van geconstateerde tekortkomingen die invloed hebben op een *Te Beschermen Belang* informeert *Opdrachtnemer NBIV* conform de *Incident Response Procedure*.	•	•	•	•
1.5.8	Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan de *Bijzondere Opdracht* zijn de werkzaamheden aan een *Te Beschermen Belang* zoveel mogelijk gecentraliseerd.	•	•	•	•

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.5.9	*Opdrachtnemer* verstrekt een overzicht aan *NBIV* van de gehele keten van *Onderaannemer(s)* en *(Toe)leverancier(s)* en de landen waarin zij gevestigd zijn voor alle bedrijfsactiviteiten die van toepassing zijn op de *Bijzondere Opdracht(en)* en werkzaamheden die raken aan een *Te Beschermen Belang*.	•	•	•	•
1.5.10	Wanneer een *Te Beschermen Belang* wordt ondergebracht bij een door *Opdrachtnemer* gekozen *Escrow Agent*, is de vigerende *ABRO* contractueel bedongen en beschikt de *Escrow Agent* over een *ABRO-Verklaring* voor de *Bijzondere Opdracht* voordat een *Te Beschermen Belang* wordt overgedragen.	•	•	•	•
1.6	**Opnamen en publicaties**				
1.6.1	*Opdrachtnemer* maakt het bestaan van, of opgedane kennis tijdens, de *Bijzondere Opdracht* op geen enkele wijze bekend buiten de geautoriseerde personen of organisaties. Dit geldt voor alle informatie waarvan *Opdrachtnemer* het vertrouwelijk karakter kent of redelijkerwijs kan vermoeden. Enkel na voorafgaand, uitdrukkelijk en schriftelijke goedkeuring van *Opdrachtgever* of organisatie aan wie de informatie toebehoort, mag over de *Bijzondere Opdracht* buiten de geautoriseerde personen of organisaties worden gecommuniceerd.	•	•	•	•
1.6.2	Het maken van *Opnamen* van een *Te Beschermen Belang* en/of het *Compartiment*, anders dan noodzakelijk voor het uitvoeren van de *Bijzondere Opdracht*, is niet toegestaan. Tenzij in afstemming met *NBIV* voorafgaande schriftelijke goedkeuring van *Opdrachtgever* is verkregen.	•	•	•	•
1.6.3	*Opdrachtnemer* maakt contactgegevens van en afspraken met *NBIV* op geen enkele wijze (publiekelijk) bekend.	•	•	•	•
1.7	**Beveiligingsincidenten**				
1.7.1	*Opdrachtnemer* heeft een *Incident Response Procedure* vastgesteld en geïmplementeerd voor het afhandelen en evalueren van *Beveiligingsincidenten*. Deze is bekend bij alle medewerkers die werken aan of toegang hebben tot een *Te Beschermen Belang*.	•	•	•	•
1.7.2	In geval van een geconstateerde *Compromittatie* van een *Te Beschermen Belang* wordt de *Beveiligingsfunctionaris* onmiddellijk geïnformeerd.	•	•	•	•
1.7.3	*Beveiligingsincidenten* worden na constatering geverifieerd en direct aan *NBIV* gemeld conform formulier 'Melding Beveiligingsincident'.	•	•	•	•
1.7.4	Gegevens ten aanzien van toegang tot en inzicht in een *Te Beschermen Belang* zijn vastgelegd en worden 3 maanden bewaard om achteraf onderzoek naar vermoede *Beveiligingsincidenten* mogelijk te maken.	•	•		
1.7.5	Gegevens ten aanzien van toegang tot en inzicht in een *Te Beschermen Belang* zijn vastgelegd en worden 6 maanden bewaard om achteraf onderzoek naar vermoede *Beveiligingsincidenten* mogelijk te maken.			•	•
1.7.6	Alle beschikbare informatie die direct gerelateerd is aan een *Beveiligingsincident* wordt bewaard voor een periode die na *Melding* in afstemming met *NBIV* wordt bepaald.	•	•	•	•

Hoofdstuk 1: Bestuur en organisatie

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
1.7.7	Er is een evaluatiemechanisme gedefinieerd waarmee men specifieke lessen identificeert, bijvoorbeeld naar aanleiding van een *Beveiligingsincident*, en waar nodig deze verwerkt in het beveiligingsbeleid en implementeert.	•	•	•	•
1.7.8	In geval van grove nalatigheid of bewuste *Compromittatie* van een *Te Beschermen Belang* door een medewerker informeert de *Beveiligingsfunctionaris NBIV* direct.	•	•	•	•
1.7.9	*Opdrachtnemer* heeft in haar beveiligingsbeleid vastgelegd hoe wordt omgegaan met medewerkers die bewust of onbewust een *Beveiligingsincident* veroorzaken, welke disciplinaire maatregelen mogelijk zijn en dat in het geval van strafbare feiten aangifte wordt gedaan.	•	•	•	•

2. PERSONEEL

Inleiding

Personele beveiliging betreft maatregelen gericht op het verkrijgen van een bepaalde mate van zekerheid dat een medewerker van de *Opdrachtnemer* de *Betrouwbaarheid* van de *Bijzondere Opdracht* niet schaadt. Dit omvat niet de fysieke beveiliging van personeel of persoonsbeveiliging.

In dit hoofdstuk worden betrouwbaarheidseisen gesteld aan medewerkers van *Opdrachtnemer* die een *Bijzondere Opdracht* uitvoeren. Het beveiligingsbewustzijn van medewerkers is hierbij van groot belang. Medewerkers moeten zich bewust zijn van de potentiële beveiligingsrisico's, bijvoorbeeld bij het zakelijk reizen naar het buitenland, en het nut en noodzaak van de getroffen beveiligingsmaatregelen.

Voor het toegang hebben tot of in aanraking komen met een *Te Beschermen Belang* in het kader van een *Bijzondere Opdracht* is in de meeste gevallen een *VGB* noodzakelijk. Bij een internationale opdracht, bijvoorbeeld verstrekt door *NAVO*, *EU* of *ESA* kan een *PSC* nodig zijn. In beide gevallen wordt door de Unit Veiligheidsonderzoeken van de *AIVD* en *MIVD* een *Veiligheidsonderzoek* uitgevoerd. In verschillende gevallen, bijvoorbeeld bij functiewijziging of beëindiging van de *Bijzondere Opdracht,* kan een medewerker worden ontheven uit zijn rol en/of *Vertrouwensfunctie*. Indien het niet naleven van ABRO 2026 valt terug te voeren op een individu, kan dit leiden tot de intrekking van diens *VGB*.

Voor sommige *Bijzondere Opdrachten*, bijvoorbeeld wanneer er enkel gewerkt wordt met TBB 4 of Departementaal VERTROUWELIJK, kan worden volstaan met een *VOG*. Deze wordt aangevraagd bij en afgegeven door Justis van het ministerie van Justitie en Veiligheid.

In het geval van een *Bijzondere Opdracht* voor de Politie, waarbij werkzaamheden worden verricht die een risico kunnen vormen voor de integriteit van de Politie, wordt door de Politie een *Betrouwbaarheidsonderzoek (BO* en *BO+)* uitgevoerd.

Hoofdstuk 2: Personeel

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
2.1	**Veiligheidsonderzoek, VGB en VOG**				
2.1.1	*Betrokken Medewerkers* beschikken over een *VOG* op basis van het door *Opdrachtgever* vastgestelde screeningsprofiel voor het uitvoeren van de betreffende functie. Een *VOG* is niet ouder dan de door *Opdrachtgever* gestelde termijn.	●			
2.1.2	*Betrokken Medewerkers* beschikken over een geldige *VGB* voor het vervullen van een *Vertrouwensfunctie* op het door *Opdrachtgever* vastgesteld niveau. Een *VGB* is niet ouder dan 5 jaar.		●	●	●
2.1.3	*Opdrachtnemer* houdt een actuele registratie bij van de *Bijzondere Opdracht(en)* en de *Betrokken Medewerker(s)* met daarbij de *VOG* of *VGB* en afgiftedatum.	●	●	●	●
2.1.4	Indien bij een internationale opdracht nationaliteitseisen worden vastgesteld door *Opdrachtgever*, worden deze door *Opdrachtnemer* nageleefd.	●	●	●	●
2.1.5	*Opdrachtnemer* heeft in afstemming met *NBIV* vastgesteld of er medewerkers zijn die voor de uitvoering van hun functie beschikken over *Buitengewone bevoegdheden of toegangsrechten* (bijvoorbeeld *Beheerders*) en daarmee een bovengemiddeld risico vormen voor een *Te Beschermen Belang*.	●	●	●	●
2.1.6	Voor *Betrokken Medewerkers* met *Buitengewone bevoegdheden of toegangsrechten*, zoals *Beheerders*, facilitair medewerkers, servicedeskmedewerkers en securityanalisten, heeft *Opdrachtnemer* in afstemming met *Opdrachtgever* en *NBIV* additionele beveiligingsmaatregelen getroffen.	●	●	●	●
2.1.7	Indien *Opdrachtgever* periodieke vernieuwing van een *VOG* van *Betrokken Medewerkers* vereist, vraagt de *Beveiligingsfunctionaris* minimaal 1 maand voor het verstrijken van de afgesproken termijn een nieuw *VOG* aan.	●			
2.1.8	Ten minste 3 maanden voor het verstrijken van de termijn voor hernieuwd onderzoek van een *VGB* van *Betrokken Medewerkers* vraagt de *Beveiligingsfunctionaris* een hernieuwd *Veiligheidsonderzoek* aan.		●	●	●
2.2	**Geheimhoudingsverklaring**				
2.2.1	*Betrokken Medewerkers* hebben een *Geheimhoudingsverklaring* ondertekend conform formulier 'Geheimhoudingsverklaring'. Deze verklaringen worden bewaard door de *Beveiligingsfunctionaris* en op verzoek worden specifieke *Geheimhoudingsverklaringen* verstrekt aan *NBIV*.	●	●	●	●
2.2.2	De *Cryptobeheerder* is als *Vertrouwensfunctionaris* aangemerkt en heeft een *Geheimhoudingsverklaring* getekend conform formulier 'Geheimhoudingsverklaring Cryptobeheerder'. Deze verklaring wordt bewaard door de *Beveiligingsfunctionaris* en op verzoek worden specifieke verklaringen verstrekt aan *NBIV*.	●	●	●	●

Hoofdstuk 2: Personeel

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
2.3	**Ontheffing uit een Vertrouwensfunctie**				
2.3.1	Wanneer een medewerker door *Opdrachtnemer* ontheven wordt als *Vertrouwensfunctionaris* meldt de *Beveiligingsfunctionaris* dit aan *NBIV*. Dit gebeurt bijvoorbeeld bij of gelijktijdig met de volgende aanleidingen: • functiewijziging van een *Vertrouwensfunctionaris*; • ontslag van een *Vertrouwensfunctionaris*; • intrekken van de *VGB*; • overtreding van beveiligingsregels door een *Vertrouwensfunctionaris*.	•	•	•	•
2.3.2	De *Beveiligingsfunctionaris* heeft aan de medewerker een toelichting gegeven op de ontheffingsverklaring, de *VOG* en *VGB*-registratie bijgewerkt, en zeker gesteld dat de medewerker geen toegang meer heeft tot of beschikt over een *Te Beschermen Belang*. Bij ontheffing uit een *Vertrouwensfunctie* ontvangt *NBIV* van de *Beveiligingsfunctionaris* een door de medewerker getekende ontheffingsverklaring conform formulier 'Ontheffing uit Vertrouwensfunctie'.	•	•	•	•
2.3.3	Er is een procedure voor veranderingen op personeelsvlak (o.a. verandering of beëindiging van functie of dienstverband) of in de contractuele relatie tussen *Opdrachtnemer* en *Opdrachtgever*. Deze omvat minimaal: • het intrekken van toegangsrechten; • het innemen van *ICT-bedrijfsmiddelen*; • de verantwoordelijkheden en taken met betrekking tot beveiliging van de *Bijzondere Opdracht* die ook na de beëindiging van het dienstverband van kracht blijven, zoals bijvoorbeeld de geheimhouding; • hoe uitgevoerde handelingen naar aanleiding van de verandering of beëindiging worden vastgelegd.	•	•	•	•
2.4	**Wijziging van de beveiligingsorganisatie**				
2.4.1	*Opdrachtnemer* verleent medewerking bij het ontheffen van een *(Cyber-)Beveiligingsfunctionaris* of *Cryptobeheerder* op aangeven van *NBIV*. Dit gebeurt bijvoorbeeld bij of gelijktijdig met de volgende aanleidingen: • overtreding van beveiligingsregels of -beleid; • handelen in strijd met *ABRO 2026*; • geen uitvoering geven aan instructies van *NBIV*; • niet naleven van wetgeving aangaande de *Bijzondere Opdracht*.	•	•	•	•
2.4.2	Bij ontheffing van de *(Cyber-)Beveiligingsfunctionaris* ontvangt *NBIV* een door de medewerker getekende ontheffingsverklaring conform formulier 'Ontheffing Beveiligingsfunctionaris'.	•	•	•	•
2.4.3	Bij ontheffing van de *Cryptobeheerder* ontvangt *NBIV* een door de medewerker getekende ontheffingsverklaring conform formulier 'Ontheffing Cryptobeheerder'.	•	•	•	•
2.5	**Training en bewustzijn**				
2.5.1	*Betrokken Medewerkers* doorlopen aantoonbaar, voorafgaand aan werkzaamheden aan een nieuwe *Bijzondere Opdracht* en daarna minimaal jaarlijks de relevante training(en). Hierin worden de beleidsregels en procedures uitgelegd voor het behandelen van een *Te Beschermen Belang* en worden relevante dreigingen besproken.	•	•	•	•

Hoofdstuk 2: Personeel

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
2.5.2	*Opdrachtnemer* informeert aantoonbaar alle *Betrokken Medewerkers* minimaal jaarlijks dat zij zwakke plekken in de beveiliging direct melden bij de *Beveiligingsfunctionaris*.	•	•	•	•
2.5.3	Minimaal jaarlijks worden *Betrokken Medewerkers* en intern *Beveiligingspersoneel* getraind in het uitvoeren van beveiligingsmaatregelen.	•	•	•	•
2.5.4	De *Beveiligingsfunctionaris* toetst minimaal jaarlijks in samenwerking met relevante *Betrokken Medewerkers* en intern *Beveiligingspersoneel* de werking van beveiligingsmaatregelen in de praktijk aan de hand van realistische scenario's voor *Compromittatie*, zowel gericht op potentiële externe als interne dreigingen.		•	•	•
2.5.5	De *Beveiligingsfunctionaris* heeft iedere *Vertrouwensfunctionaris* gewezen op de verantwoordelijkheden die voortvloeien uit het bekleden van een *Vertrouwensfunctie*.	•	•	•	•
2.5.6	De *Beveiligingsfunctionaris* heeft iedere *Vertrouwensfunctionaris* gewezen op mogelijke aanleidingen voor een hernieuwd *Veiligheidsonderzoek* en adviseert om in het geval dat zo'n aanleiding zich voordoet hier *Melding* van te doen.	•	•	•	•
2.5.7	De *Beveiligingsfunctionaris* geeft individueel advies en begeleiding aan *Betrokken Medewerkers* die werken aan een *Bijzondere Opdracht* bijvoorbeeld over het hebben van buitenlandse contacten of zakelijke reizen naar een *Risicoland*.	•	•	•	•
2.5.8	Binnen een *Compartiment* wordt gewerkt met de *Clear Desk* en *Clear Screen* principes. Een *Te Beschermen Belang* wordt nooit onbeheerd achtergelaten en een *Compact Te Beschermen Belang* wordt na gebruik opgeborgen.	•	•	•	•
2.6	**Reizen naar het buitenland**				
2.6.1	Bij een zakelijke reis van een *Vertrouwensfunctionaris* naar een *Risicoland* meldt de *Beveiligingsfunctionaris* dit bij *NBIV* conform formulier 'Melding bezoek Risicoland'.	•	•	•	•
2.6.2	Indien voor een zakelijke reis in het kader van de *Bijzondere Opdracht* een *Request for Visit (RfV)* benodigd is, dient de *Vertrouwensfunctionaris* tijdig via de *Beveiligingsfunctionaris* een *RfV* ter goedkeuring in bij *NBIV*. Zonder goedgekeurde *RfV* kan de reis niet plaatsvinden.	•	•	•	•
2.6.3	De *Beveiligingsfunctionaris* brieft en debrieft de *Vertrouwensfunctionaris* ten aanzien van de zakelijke reis naar een *Risicoland*. Van de debriefing wordt een verslag opgesteld en op verzoek overhandigd aan *NBIV*.	•	•	•	•
2.6.4	Bij een zakelijke reis van een *Betrokken Medewerker* naar een *Risicoland* wordt gebruik gemaakt van dedicated *Mobiele apparatuur* die alleen voor deze reis wordt ingezet en na terugkomst wordt gewist.	•	•	•	•

3. FYSIEK

Inleiding

Om invulling te geven aan de fysieke beveiligingseisen is *Beveiligingsrendement* leidend. Dit houdt in dat voldoende beveiligingsmaatregelen worden getroffen om het benodigde vertragende effect (*Uitsteltijd*) te genereren. Onder *Compromittatie* wordt het moment verstaan waarop een indringer ongeautoriseerde toegang heeft tot, kennis kan nemen van en schade kan toebrengen aan een *Te Beschermen Belang* dan wel de mogelijkheid heeft tot kennisname of toegang tot een *Te Beschermen Belang*. Om *Compromittatie* te voorkomen kunnen zowel Organisatorische, Bouwkundige, Elektronische als Reactieve (OBER) maatregelen worden getroffen.

Op basis van een *Risicoanalyse* brengt *Opdrachtnemer* de fysieke dreigingen ten aanzien van de *Bijzondere Opdracht* in kaart. Met het benodigde *Beveiligingsrendement* en de *Interventietijd* kan vervolgens in afstemming met *NBIV* worden bepaald welke beveiligingsmaatregelen nodig zijn. Hierbij wordt geredeneerd van binnen naar buiten met het *Te Beschermen Belang* als startpunt, waarbij aan de hand van verschillende beveiligingsmaatregelen het benodigde *Beveiligingsrendement* wordt gerealiseerd. *NBIV* kan adviseren bij het selecteren van de benodigde beveiligingsmaatregelen, zie ook bijlage 5.

Naast de vereiste OBER-maatregelen, worden in dit hoofdstuk eisen gesteld aan de fysieke opslag van een *Te Beschermen Belang* op locatie van de *Opdrachtnemer*. Dit omvat onder andere de verwerking, ontwikkeling en vernietiging van een *Te Beschermen Belang*. Wanneer een *Te Beschermen Belang* wordt getransporteerd of verzonden, is het kwetsbaarder dan wanneer het zich bevindt op een beveiligde locatie. Daarom dienen passende beveiligingsmaatregelen getroffen te worden om de *Integriteit* en *Vertrouwelijkheid* van het *Te Beschermen Belang* te waarborgen gedurende *Transport* en *Verzenden*, zie ook bijlage 7.

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.1	**Organisatorische maatregelen**				
3.1.1	*Opdrachtnemer* neemt in zijn *Risicoanalyse* voor de *Bijzondere Opdracht(en)* mee welke methoden en hulpmiddelen potentiële daders tot hun beschikking hebben om het *Te Beschermen Belang* fysiek te compromitteren.	•	•	•	•
3.1.2	*Opdrachtnemer* heeft in afstemming met *NBIV* op basis van de *Risicoanalyse* het vereiste *Beveiligingsrendement* vastgesteld. Op basis van het *Beveiligingsrendement* en de *Interventietijd* zijn de benodigde (Organisatorische-, Bouwkundige-, Elektronische-, Reactieve-) maatregelen getroffen om het benodigde vertragende effect (*Uitsteltijd*) te realiseren. Hiervoor is gebruikgemaakt van NEN-normering zoals genoemd in bijlage 6.1.	•	•	•	•
3.1.3	De maatregelen in relatie tot de *Interventietijd* waarborgen aantoonbaar (middels gecertificeerde componenten) dat *Interventie* maximaal 120 minuten na *Compromittatie* van een *Te Beschermen Belang* plaatsvindt.		•		
3.1.4	De maatregelen in relatie tot de *Interventietijd* waarborgen aantoonbaar (middels gecertificeerde componenten) dat *Interventie* eerder plaatsvindt dan *Compromittatie* van een *Te Beschermen Belang* (een positief *Beveiligingsrendement*).			•	•
3.1.5	Detecterende maatregelen zorgen ervoor dat *Compromittatie* van een *Te Beschermen Belang* of pogingen daartoe binnen de vereiste tijd worden gedetecteerd om het *Beveiligingsrendement* te realiseren, zie ook bijlage 5.	•	•	•	•
3.1.6	De fysieke beveiligingsmaatregelen zijn volgens een schillenstructuur opgebouwd met toepassing van '*Need-to-Know*' en '*Need-to-Be*' principes.	•	•	•	•
3.1.7	Toegang tot een *Compartiment* met een *Te Beschermen Belang* is geregistreerd om te waarborgen dat alleen *Geautoriseerde Medewerkers* toegang hebben.	•	•	•	•
3.1.8	In de toegangsregistratie voor een *Compartiment* is minimaal de naam van de persoon, de datum en het tijdstip van aankomst en vertrek vastgelegd. In geval van niet digitale registratie is deze voorzien van een handtekening.	•	•	•	•
3.1.9	Toegang tot een *Compartiment* vereist *Multi-factor authenticatie*.		•	•	•
3.1.10	Alleen *Geautoriseerde Medewerkers* hebben zelfstandig toegang tot een *Compartiment*.	•	•	•	•
3.1.11	Medewerkers hebben uitsluitend toegang tot een *Te Beschermen Belang* na *Autorisatie* door de *Beveiligingsfunctionaris*. *Geautoriseerde Medewerkers* beschikken over een *VOG* of indien vereist een geldige *VGB* van het voorgeschreven niveau.	•	•	•	•

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.1.12	In het geval dat een *Bezoeker* toegang krijgt tot een *Compartiment*: • is het bezoek in het directe belang van de *Bijzondere Opdracht*; • is de *Bezoeker* vooraf aangemeld bij de *Beveiligingsfunctionaris*; • wordt vooraf de identiteit van de *Bezoeker* vastgesteld; • is de *Bezoeker* geregistreerd waarbij ten minste de naam van de *Bezoeker* en de datum en het tijdstip van aankomst en vertrek is vastgelegd; • wordt de *Bezoeker* gedurende het gehele bezoek onafgebroken begeleid door een *Geautoriseerde Medewerker*; • draagt de *Bezoeker* een duidelijk herkenbare en zichtbare bezoekerspas; • zijn de aanwezige medewerkers vooraf geïnformeerd. De medewerkers nemen hierop maatregelen om *Compromittatie* te voorkomen.	•	•	•	•
3.1.13	Toegangsregistratie tot een *Compartiment* wordt minimaal 6 maanden bewaard en op verzoek verstrekt aan *NBIV*.	•	•	•	•
3.1.14	Binnen een *Compartiment* wordt de toegangspas zichtbaar gedragen. Op de pas staat ten minste de naam van de persoon.	•	•	•	•
3.1.15	De voorgenomen toegang tot een *Compartiment* door een *Bezoeker* is minimaal 5 werkdagen voor het bezoek ter goedkeuring aan *NBIV* voorgelegd middels formulier 'Autorisatie Bezoeker'.		•	•	•
3.1.16	Aan de buitenzijde van het *Compartiment* zijn de beveiligingsinstructies bevestigd die van toepassing zijn voor het *Compartiment*.		•	•	•
3.1.17	Voor de uitgifte van *Fysieke toegangsauthenticatiemiddelen* voor een *Compartiment* geldt: • bij de uitgifte van *Fysieke toegangsauthenticatiemiddelen* wordt gecontroleerd of de ontvangende medewerker over de juiste *Autorisatie* beschikt; • de uitgifte van *Fysieke toegangsauthenticatiemiddelen* wordt geregistreerd; • de registratie wordt minimaal jaarlijks geactualiseerd.	•	•	•	•
3.1.18	Bij het gebruik van *Biometrie* is de gebruikte apparatuur voorzien van beveiligingsmaatregelen om ongeautoriseerde fysieke toegang tot de inhoud van de apparatuur, het aanpassen en het verwisselen van de apparatuur te voorkomen.	•	•	•	•
3.1.19	Bij het gebruik van *Biometrische* apparatuur zijn *Cryptografische beveiligingsoplossingen* toegepast om de authenticiteit, Integriteit en Vertrouwelijkheid van *Biometrische* informatie te waarborgen.	•	•	•	•
3.1.20	Bij het gebruik van *Biometrie* is de gebruikte apparatuur aantoonbaar bestand tegen bekende methoden om *Biometrische apparatuur* te misleiden of te omzeilen.	•	•	•	•
3.1.21	*Fysieke toegangsauthenticatiemiddelen* zijn conform relevante NEN-normeringen gecertificeerd, zie ook bijlage 6.1.		•	•	•
3.1.22	Fysieke sleutels en reservesleutels welke toegang geven tot een *Compartiment* blijven te allen tijde op het terrein van *Opdrachtnemer* en worden alleen achtergelaten in een daartoe bestemd *Opbergmiddel*. Reservesleutels worden nooit in hetzelfde *Opbergmiddel* bewaard als het origineel.		•	•	•
3.1.23	*Fysieke toegangsauthenticatiemiddelen*, cijfercombinaties en *Certificaten* worden beheerd door de *Beveiligingsfunctionaris*.		•	•	•

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.1.24	*Fysieke toegangsauthenticatiemiddelen* en cijfercombinaties voor *Compartimenten* en *Opbergmiddelen* zijn, wanneer niet in gebruik, opgeborgen in een *Opbergmiddel* conform bijlage 6.1.		•	•	•
3.1.25	Cijfercombinaties van sloten van *Opbergmiddelen* worden minimaal iedere 6 maanden gewijzigd en onmiddellijk gewijzigd indien: • een nieuw *Opbergmiddel* of slot in gebruik wordt genomen; • de *Autorisatie* van een medewerker die de cijfercombinatie kent wordt ingetrokken of gewijzigd; • er onderhoud heeft plaatsgevonden aan het slot; • het vermoeden bestaat of vaststaat dat *Compromittatie* heeft plaatsgevonden. Bij het herzien van de cijfercombinatie wordt geen eerder gebruikte combinatie gekozen.		•	•	•
3.1.26	Het verlies of diefstal van een *Fysieke toegangsauthenticatiemiddel* wordt behandeld als een *Beveiligingsincident*.	•	•	•	•
3.1.27	Fysieke apparatuur, beveiligingscomponenten en *Beveiligingssystemen* worden beheerd en onderhouden om ze blijvend te laten functioneren.	•	•	•	•
3.1.28	Wanneer voor het beheer en onderhoud van fysieke apparatuur, beveiligingscomponenten of *Beveiligingssystemen* gebruik wordt gemaakt van *Cloudoplossingen*, is de leverancier van deze *Cloudoplossing* aangemeld als onderaannemer bij *NBIV*.	•			
3.1.29	Voor het beheer en onderhoud van fysieke apparatuur, beveiligingscomponenten of *Beveiligingssystemen* wordt geen gebruik gemaakt van *Cloudoplossingen*.		•	•	•
3.1.30	*Beveiligingspersoneel* heeft de beschikking over alarmeringsmiddelen.		•	•	•
3.1.31	Bij het verlaten van een *Compartiment* door de laatste medewerker wordt een sluitronde gemaakt, waarbij ten minste gecontroleerd wordt of: • het *Opbergmiddel*, het *Compartiment* en zo mogelijk de etage en/of het gebouw is afgesloten; • ramen en deuren zijn afgesloten; • er geen personen meer aanwezig zijn; • de verzegeling van nooddeuren intact is; • eventuele beveiligingsmaatregelen zijn geactiveerd (bijvoorbeeld een Indringer Detectie en Signalering Systeem, *IDSS*). De sluitprocedure is opgenomen in het *Beveiligingsplan*.	•	•	•	•
3.1.32	Een *Verboden Plaats* moet voldoen aan de TBB 1 beveiligingseisen op alle beveiligingsgebieden (organisatorisch, fysiek en cybersecurity).		•	•	•
3.1.33	De *Beveiligingsfunctionaris* onderhoudt contact met de gemeente en lokale politie om op de hoogte te zijn van relevante lokale ontwikkelingen en eventuele dreigingen die de beveiliging van een *Te Beschermen Belang* aangaan. Indien nodig treft de *Beveiligingsfunctionaris* additionele maatregelen.		•	•	•

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.2	**Bouwkundige maatregelen**				
3.2.1	Een *Compact Te Beschermen Belang* is opgeslagen in een afsluitbaar *Opbergmiddel* dat voldoet aan de normering gesteld in bijlage 6.1.	•	•	•	•
3.2.2	Een *Te Beschermen Belang* is geplaatst in een *Compartiment*.	•	•	•	•
3.2.3	De specificaties van een *Opbergmiddel* en/of *Compartiment* dat gebruikt wordt voor de opslag van een *(Compact) Te Beschermen Belang* zijn afgestemd met *NBIV*.				•
3.2.4	Een *Compartiment* waarin een *Te Beschermen Belang* is opgeborgen, is afgesloten met een gecertificeerd mechanisme, waardoor onge-autoriseerde toegang niet mogelijk is zonder sporen van braak, zie bijlage 6.1.		•	•	•
3.2.5	Toegangsdeuren tot een *Compartiment* zijn aan de binnenzijde voorzien van een deurdranger en een elektronisch en akoestisch alarm dat afgaat wanneer een deur langer openstaat dan noodzakelijk.		•	•	•
3.2.6	Nooddeuren in een *Compartiment* zijn alleen naar buiten toe te openen. Tevens zijn nooddeuren verzegeld, voorzien van een elektronisch en akoestisch alarm en bij opening vindt alarmering plaats.		•	•	•
3.2.7	*Opbergmiddelen* tot 1000 kilogram zijn verankerd.		•		
3.2.8	*Opbergmiddelen* tot 1000 kilogram zijn *Chemisch verankerd*.			•	•
3.2.9	Bevestigingspunten van *Opbergmiddelen* die van buitenaf bereikbaar zijn, zijn fysiek beveiligd.		•	•	•
3.2.10	*Opbergmiddelen* zijn voorzien van *Multi-factor authenticatie*.		•	•	•
3.2.11	Er is *Beveiligingsverlichting* toegepast rondom het gebouw en/ of terrein met een *Te Beschermen Belang*.		•	•	•
3.2.12	Bij de aanleg van infrastructuur, zoals bestrating, begroeiing of watergangen, is rekening gehouden met inbraakpreventie.		•	•	•
3.2.13	Een *Compartiment* is op alle vlakken voorzien van inkijkbeperkende maatregelen.		•	•	•
3.2.14	Het gebouw waarin zich een *Te Beschermen Belang* bevindt, is tegen opklimmen beveiligd. Losse opklimmogelijkheden zoals (afval) containers en ladders zijn verwijderd. Hemelwaterafvoeren, lage muren e.d. zijn van opklimbeveiliging voorzien.		•	•	•
3.3	**Elektronische maatregelen**				
3.3.1	*Beveiligingssystemen* ten behoeve van het beveiligen van de *Bijzondere Opdracht* mogen niet voortkomen uit een land dat een *Offensief cyberprogramma* tegen Nederlandse belangen heeft.	•	•	•	•
3.3.2	*Beveiligingssystemen* zijn geïnstalleerd conform normeringen gesteld in bijlage 6.1. Onderhoud en controle vinden minimaal jaarlijks plaats door een gecertificeerd bedrijf (bijvoorbeeld BORG-certificaat).		•	•	•

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.3.3	*Beveiligingssystemen* staan onder detectie zodat ongeautoriseerde toegang, sabotage of pogingen daartoe leiden tot alarmering en *Interventie* binnen de vereiste tijd om het benodigde *Beveiligingsrendement* te realiseren.		●	●	●
3.3.4	Systeemklokken van *Beveiligingssystemen* maken gebruik van dezelfde tijdsynchronisatie en zijn zodanig beveiligd tegen wijzigingen dat deze niet onopgemerkt aangepast of gemanipuleerd kunnen worden.		●	●	●
3.3.5	Een *Beveiligingssysteem* is niet gekoppeld aan een centraal gebouwbeheersysteem of andere *Systemen* die het mogelijk maken een beveiligingssysteem op afstand te beheren.		●	●	●
3.3.6	Draadloze verbindingsmogelijkheden van *Beveiligingssystemen* zijn uitgeschakeld en alle componenten zijn beveiligd tegen digitale (*Cyber*) *Compromittatie*.		●	●	●
3.3.7	*Beveiligingssystemen*, inclusief achterliggende beheersystemen, zijn alleen verbonden via een dedicated en afgeschermd beheernetwerk.		●	●	●
3.3.8	Bewegingsmelders zijn voorzien van anti-masking maatregelen.		●	●	●
3.3.9	Buiten een *Compartiment* zijn voorzieningen getroffen conform bijlage 6.1 om personen visueel te herkennen voordat zij het *Compartiment* betreden.		●	●	●
3.3.10	Camerabeelden worden 28 dagen bewaard. Camerabeelden gerelateerd aan een (mogelijk) *Beveiligingsincident* worden zolang als nodig voor het onderzoek en de afhandeling van het *Beveiligingsincident* bewaard. In afstemming met *NBIV* en *Opdrachtgever* kan worden besloten om de camerabeelden langer te bewaren.		●	●	●
3.3.11	De toegang tot een *Compartiment* is beveiligd door middel van een elektronisch of mechanisch toegangsbeheersysteem.		●	●	●
3.3.12	Waar een *Elektronisch Toegangsbeheersysteem (ETS)* wordt gebruikt, zijn maatregelen getroffen om situaties te detecteren waar toegang 'onder dwang' is verleend.			●	●
3.3.13	Een *ETS* is uitgerust met een Anti Pass Back *Systeem*.		●	●	●
3.3.14	Een *ETS* is voorzien van *Logging*, waarbij geldt dat de logs minimaal 6 maanden worden bewaard. De logs worden maandelijks door de *Beveiligingsfunctionaris* gecontroleerd op opvallende afwijkingen.		●	●	●
3.3.15	Een *ETS* is zodanig uitgevoerd dat wanneer het *Systeem* uitschakelt of uitvalt, alle toegangen tot het *Compartiment* worden afgesloten en/of afgesloten blijven.		●	●	●
3.3.16	Een *Compartiment* beschikt over een noodknopbediening of mechanische paniekontgrendeling voor calamiteiten. De procedure rondom het gebruik hiervan is beschreven in het *Beveiligingsplan*.		●	●	●
3.3.17	Een *Te Beschermen Belang* staat onder detectie van een *IDSS*. Het *IDSS* kan geïnstalleerd zijn op het *Compartiment*, het *Opbergmiddel* of het *Te Beschermen Belang* zelf.		●	●	●

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.3.18	*IDSS*-onderdelen zijn zodanig geplaatst dat *Compromittatie* van een *Te Beschermen Belang* of pogingen daartoe worden ontdekt en een alarm genereren.		•	•	•
3.3.19	Het *Compartiment* met een *Te Beschermen Belang* is binnen het *IDSS* als aparte zone opgenomen. Deze zone is actief wanneer er geen *Geautoriseerde Medewerker* is in de betreffende ruimte.		•	•	•
3.3.20	Het *IDSS* is altijd geactiveerd, tenzij *Geautoriseerde Medewerkers* aanwezig zijn in het *Compartiment*.		•	•	•
3.3.21	Het deactiveren van een *IDSS* is alleen mogelijk door een daartoe aangewezen persoon middels *Multi-factor authenticatie*.		•	•	•
3.3.22	Het *IDSS* functioneert te allen tijde en onder alle (klimatologische) omstandigheden.		•	•	•
3.3.23	Doormelding van een *IDSS* alarm voldoet aan normeringen gesteld in bijlage 6.1.		•	•	
3.3.24	Doormelding van een *IDSS* alarm is in afstemming met *NBIV* vastgesteld.				•
3.3.25	Het *IDSS* beschikt over een gegarandeerde stroomvoorziening die het functioneren garandeert tot ten minste de maximale *Interventietijd*.		•	•	•
3.3.26	Het *IDSS* signaleert en registreert uitval van de stroomvoorziening van een *IDSS*. Bij stroomuitval wordt gehandeld alsof het een alarmering betreft.		•	•	•
3.3.27	Alleen elektronische apparatuur die strikt noodzakelijk is voor het uitvoeren van de werkzaamheden is toegestaan in een *Compartiment*. Het goedkeuren van elektronische apparatuur in een *Compartiment* geschiedt op basis van een *Risicoanalyse*. Hierbij is elektronische apparatuur afkomstig uit een land met een *Offensief cyberprogramma* uitgesloten. Een lijst van de apparatuur en de bijbehorende *Risicoanalyse* is vooraf in afstemming met *NBIV* goedgekeurd door *Opdrachtgever*, en opgenomen in het *Beveiligingsplan*.		•	•	•
3.3.28	Er zijn (procedurele) maatregelen getroffen om elektronische apparatuur die niet strikt noodzakelijk is voor het uitvoeren van werkzaamheden buiten het *Compartiment* te houden.		•	•	•
3.3.29	Elektronische apparatuur van toepassing in de beveiliging of het gebouwbeheer (waaronder *GBS* en connected devices (IoT)) worden beschouwd als *Systeem* en zijn alleen toegestaan in een *Compartiment* wanneer deze op het voor de *Bijzondere Opdracht* vastgestelde beveiligingsniveau zijn beveiligd.	•	•	•	•
3.3.30	In een *Compartiment* zijn geen camera's, smart devices, microfoons of andere apparatuur met een opname- of communicatiefunctionaliteit aanwezig.		•	•	•
3.3.31	Voorafgaand aan de ingebruikname van een *Compartiment* en bij toevoeging of wijziging van *Middelen* is, in afstemming met *NBIV*, een *Elektronisch veiligheidsonderzoek (EVO)* en *Geluidsdempingsmeting* uitgevoerd. Eventuele maatregelen zijn voorafgaand aan implementatie afgestemd met *NBIV*.			•	•

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.3.32	Voorafgaand aan de ingebruikname van een *Compartiment* en bij toevoeging of wijziging van *Middelen* zijn, in afstemming met *NBIV*, *TEMPEST*-maatregelen getroffen. De instructies voor de benodigde maatregelen zijn bij *NBIV* op te vragen.		•		
3.3.33	Voorafgaand aan de ingebruikname van een *Compartiment* en bij toevoeging of wijziging van *Middelen* is, in afstemming met *NBIV*, een *Zoneringsmeting (TEMPEST)* uitgevoerd. Eventuele maatregelen zijn voorafgaand aan implementatie afgestemd met *NBIV*. De instructies voor de benodigde maatregelen zijn op te vragen via *NBIV*.			•	•
3.4	**Reactieve maatregelen**				
3.4.1	Alarmeringen uit een *IDSS* en *ETS* moeten leiden tot *Interventie* binnen de vereiste tijd om het vastgestelde *Beveiligingsrendement* te realiseren.		•	•	•
3.4.2	*Interventie* vindt plaats door daartoe aangewezen en opgeleid *Beveiligingspersoneel*.		•	•	•
3.4.3	Bij een (technische) storing worden mitigerende beveiligings-maatregelen getroffen om het *Beveiligingsrendement* te waarborgen.		•	•	•
3.4.4	Alarmverificatie vindt initieel aan de buitenzijde van het *Compartiment* plaats. Hierbij zijn alle toegangen, gevelopeningen, daken e.d. gecontroleerd.		•	•	•
3.4.5	Medewerkers of *Beveiligingspersoneel* dat alarmverificatie uitvoert, heeft ten tijde van de alarmverificatie niet de beschikking over *Fysieke toegangsauthenticatiemiddelen* die toegang geven tot het *Te Beschermen Belang*.		•	•	•
3.4.6	Een *PAC* beschikt over een justitiële erkenning en voldoet aan de normeringen gesteld in bijlage 6.1.		•	•	•
3.4.7	Een *BAC* wordt beveiligd als een *Compartiment* op TBB 4 niveau.		•	•	•
3.4.8	Na een alarm of *Melding* controleert de *Beveiligingsfunctionaris* het betreffende *Te Beschermen Belang* en neemt indien nodig maat-regelen om het vereiste *Beveiligingsrendement* te herstellen.	•	•	•	•
3.5	**Transport en verzenden algemeen**				
3.5.1	Een *Te Beschermen Belang* wordt uitsluitend buiten het *Compartiment* gebracht als dit voor de voortgang van de werkzaamheden abso-luut noodzakelijk is.	•	•	•	•
3.5.2	Een *Te Beschermen Belang* en gerelateerde apparatuur, informatie en software van *Opdrachtnemer* die gebruikt wordt bij een *Bijzondere Opdracht* verlaten het *Compartiment* van *Opdrachtnemer* niet zonder vooraf gegeven toestemming van de *Beveiligingsfunctionaris*.	•	•	•	•
3.5.3	De *Beveiligingsfunctionaris* beschrijft in het *Beveiligingsplan* op welke wijze om wordt gegaan met het *Transport* en *Verzenden* van een *Te Beschermen Belang* in het kader van de *Bijzondere Opdracht* conform bijlage 7. Dit wordt in afstemming met *NBIV* ter goedkeuring voor-gelegd aan *Opdrachtgever*.	•	•	•	•

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.5.4	Voorafgaand aan een *Transport* of *Verzenden* van een *Te Beschermen Belang* wordt door de *Beveiligingsfunctionaris* vastgesteld dat de ontvangende partij het *Te Beschermen Belang* conform het vastgestelde beveiligingsniveau kan behandelen en geautoriseerd is om te beschikken over het *Te Beschermen Belang*.	•	•	•	•
3.6	**Fysiek Verzenden**				
3.6.1	Voorafgaand aan *Verzenden* wordt het *Te Beschermen Belang* verpakt zodat de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	•			
3.6.2	Verzenden van een *Te Beschermen Belang* is uitsluitend toegestaan wanneer dit aangetekend wordt verzonden met track en trace nummer en met onmiddellijke ontvangstbevestiging.	•			
3.6.3	Verzenden van een *Te Beschermen Belang* per post is niet toegestaan.		•	•	•
3.7	**Fysiek Transport Te Beschermen Belangen**				
3.7.1	Het fysiek *Transport* van een *Te Beschermen Belang* (zoals goederen en materieel) wordt uitgevoerd conform de door *Opdrachtgever* vastgestelde beveiligingsmaatregelen.	•	•	•	•
3.8	**Fysiek Transport Bijzondere Informatie**				
3.8.1	Voorafgaand aan *Transport* van *Bijzondere Informatie* wordt een transportplan opgesteld conform formulier 'Transportplan' en ter goedkeuring voorgelegd aan *NBIV*.		•	•	•
3.8.2	Het transportplan voor *Transport* van *Bijzondere Informatie* buiten Nederland wordt tenminste 10 werkdagen voorafgaand aan *Transport* in afstemming met *NBIV* ter goedkeuring voorgelegd aan de *Opdrachtgever.*		•	•	•
3.8.3	*Bijzondere Informatie* wordt getransporteerd in een afsluitbaar *Transportmiddel* waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	•			
3.8.4	*Bijzondere Informatie* wordt getransporteerd in een door *de Opdrachtgever* vooraf goedgekeurd *Transportmiddel*.		•	•	•
3.8.5	*Transport* van *Bijzondere Informatie* gaat zonder onnodige en ongeplande onderbrekingen. De *Bijzondere Informatie* blijft onder toezicht.		•	•	•
3.8.6	*Transport* van *Bijzondere Informatie* vindt op één van onderstaande manieren plaats: • handcarried, al dan niet met eigen vervoer, door een *Geautoriseerde Medewerker*; • door een koeriersbedrijf.	•			
3.8.7	*Transport* van *Bijzondere Informatie* vindt op één van onderstaande manieren plaats: • handcarried, al dan niet met eigen vervoer, door een *Geautoriseerde Medewerker*; • door een *Opdrachtgever* goedgekeurd koeriersbedrijf: • het koeriersbedrijf is aangemeld als *Onderaannemer*.		•		

Hoofdstuk 3: Fysiek

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
3.8.8	*Transport* van *Bijzondere Informatie* vindt op één van onderstaande manieren plaats: • handcarried, al dan niet met eigen vervoer, door ten minste twee *Geautoriseerde Medewerkers*; • door een *Opdrachtgever* goedgekeurd koeriersbedrijf; • het koeriersbedrijf is aangemeld als *Onderaannemer*.			•	
3.8.9	*Transport* van *Bijzondere Informatie* geschiedt uitsluitend in afstemming met, en na voorafgaande goedkeuring van *Opdrachtgever*.				•
3.9	**Fysieke opslag, verwerken, ontwikkelen en vernietigen**				
3.9.1	Door de *Opdrachtnemer* in ontvangst of in beheer genomen *Te Beschermen Belang* wordt opgenomen in een actuele registratie, met daarin de locatie, uitgifte, inname en herkomst van het *Te Beschermen Belang*. Deze registratie wordt beheerd door de *Beveiligingsfunctionaris* en is te allen tijde direct opvraagbaar door *NBIV*.		•	•	•
3.9.2	*Gegevensdragers* waarop *Bijzondere Informatie* wordt verwerkt of opgeslagen, zijn voorzien van een kenmerk (labeling) conform bijlage 8, waarbij verschillende *Rubriceringsdomeinen* en *-niveaus* duidelijk te onderscheiden zijn.	•	•	•	•
3.9.3	De reproductie van *Bijzondere Informatie* geschiedt alleen met goedkeuring van *Opdrachtgever*.		•	•	•
3.9.4	Er zijn niet meer reproducties gemaakt dan noodzakelijk voor de uitvoering van de *Bijzondere Opdracht*.	•	•	•	•
3.9.5	Reproducties kennen dezelfde *Rubricering* als het origineel, ook als slechts delen van het origineel zijn gebruikt.	•	•	•	•
3.9.6	*Bijzondere Informatie* en daarvan gemaakte reproducties zijn geregistreerd en voorzien van een uniek exemplaarnummer.		•	•	•
3.9.7	Het maken van reproducties is voorbehouden aan daartoe aangewezen *Geautoriseerde Medewerkers* die ook verantwoordelijk zijn voor de registratie hiervan.		•	•	•
3.9.8	Beveiligingsmaatregelen voor reproductiemiddelen worden in afstemming met *NBIV* vastgesteld.	•	•	•	•
3.9.9	Het vernietigen van *Bijzondere Informatie* geschiedt na toestemming van *Opdrachtgever* conform de in bijlage 8 gespecificeerde vernietigingsmethode door een *Geautoriseerde Medewerker*.	•			
3.9.10	Het vernietigen van *Bijzondere Informatie* geschiedt na toestemming van *Opdrachtgever* conform de in bijlage 8 gespecificeerde vernietigingsmethode door een *Geautoriseerde Medewerker* en onder toezicht van een tweede *Geautoriseerde Medewerker*.		•	•	•
3.9.11	Van de vernietiging wordt door de *Beveiligingsfunctionaris* een bevestiging van vernietiging opgemaakt conform formulier ‘Bevestiging van vernietiging’.		•	•	•
3.9.12	De *Opdrachtnemer* stelt in overleg met *Opdrachtgever* een *Noodvernietigingsplan* op. Het *Noodvernietigingsplan* wordt opgenomen in het *Beveiligingsplan* en bevat procedures en instructies met betrekking tot de vernietiging van een *Te Beschermen Belang* in een noodsituatie.		•	•	•

4. CYBER

Inleiding

Bij een *Bijzondere Opdracht* kunnen ICT-voorzieningen van *Opdrachtnemer* betrokken zijn bij het uitvoeren van de werkzaamheden. De term *Cyber* wordt gebruikt om naast de IT-infrastructuur (de hardware en software) ook de bijbehorende processen én het menselijk handelen te omschrijven. Deze zullen als geheel de beveiliging van een *Te Beschermen Belang* moeten waarborgen. Een gedegen *Risicoanalyse* voor het verwerken en opslaan van *Bijzondere Informatie* vormt de basis van cybersecurity waarbij zowel technische maatregelen, als het stelsel van activiteiten als geheel, conform de *ABRO*-eisen zijn ingeregeld. De beveiligingseisen in dit hoofdstuk zijn gestructureerd langs een selectie van domeinen van het Secure Controls Framework (SCF).

ABRO 2026 stelt eisen aan een breed scala van cybersecurity maatregelen, waarbij expliciet rekening wordt gehouden met statelijke actoren en hun capaciteiten. Een *Opdrachtnemer* moet onder meer zicht hebben op alle componenten van de IT-infrastructuur waarop *Bijzondere Informatie* wordt verwerkt, weten waar zich *Bijzondere Informatie* bevindt en wie waar toegang toe heeft. De IT-infrastructuur moet zijn ingericht volgens moderne standaarden, up-to-date zijn en zijn gescheiden van onvertrouwde omgevingen. Er dient een veelvoud aan beveiligingsmaatregelen te worden getroffen om voldoende zicht te hebben op *Netwerk*- en systeemactiviteiten en om *Malware* te detecteren. Het gebruik van specifieke *Cryptografische Beveiligingsoplossingen* speelt daarnaast een belangrijke rol om *Bijzondere Informatie* op het juiste beveiligingsniveau te beveiligen.

Een specifiek risico waarmee rekening moet worden gehouden is het weglekken van elektromagnetische straling. De bijbehorende beveiligingseisen zijn opgenomen in hoofdstuk 3. Daarnaast is het van belang dat de ontwikkeling van software en het doorvoeren van wijzigingen op een veilige en betrouwbare manier gebeurt. Hierbij speelt ook de continuïteit van de bedrijfsvoering een belangrijke rol. Centraal in al deze aspecten is de rol van medewerkers en de risico's die menselijk handelen met zich meebrengt. Dit gaat zowel over toegangscontrole als het adequaat instrueren van medewerkers in het correct gebruik van *ICT-Bedrijfsmiddelen.*

Op het gebied van *Cyber* kan, naast een *Beveiligingsfunctionaris*, ook een *Cyber-Beveiligingsfunctionaris* worden aangewezen, zie ook bijlage 2. De *Cyber-Beveiligingsfunctionaris* ondersteunt de *Beveiligingsfunctionaris* met de *Cyber* gerelateerde beveiligingsvraagstukken.

In hoofdstuk 5 wordt specifiek ingegaan op de aanvullende eisen rondom het gebruik van *Cloudoplossingen*.

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.1	**Beheer van ICT-bedrijfsmiddelen**				
4.1.1	Door de *Opdrachtnemer* in ontvangst of in beheer genomen digitale *Bijzondere Informatie* wordt opgenomen in een actuele registratie, met daarin de locatie, uitgifte, inname en herkomst van de *Bijzondere Informatie*. Deze registratie wordt beheerd door de *(Cyber-)Beveiligingsfunctionaris* en is te allen tijde direct opvraagbaar door *NBIV*.		•	•	•
4.1.2	*ICT-bedrijfsmiddelen* en de bijbehorende software, processen en gegevensverzamelingen worden bijgehouden in een registratie, voorzien van een eigenaar, een *Beheerder*, de gerelateerde *Bijzondere Opdracht* en de onderlinge relatie met andere onderdelen van de registratie, waaronder de overdracht van data.	•	•	•	•
4.1.3	Systeem- en netwerkcomponenten gerelateerd aan een *Bijzondere Opdracht* worden bijgehouden in een gedetailleerd netwerkdiagram.	•	•	•	•
4.1.4	*Systemen* waar *Bijzondere Informatie* op wordt verwerkt en opgeslagen worden alleen ingezet binnen het deel van de IT-infrastructuur dat ingericht is voor het betreffende *Rubriceringsdomein* en *-niveau*.	•	•	•	•
4.1.5	Het gebruik van een *KVM-switch* om te schakelen tussen *Systemen* van verschillende *Rubriceringsniveaus* is alleen toegestaan wanneer dit binnen eenzelfde *Rubriceringsdomein* is en gebruik wordt gemaakt van *Goedgekeurde Middelen*.	•	•	•	•
4.1.6	Voor het beheer en onderhoud van fysieke apparatuur, beveiligingscomponenten of *Beveiligingssystemen* wordt geen gebruik gemaakt van *Cloudoplossingen.*	•	•	•	•
4.1.7	Het hergebruik van *ICT-bedrijfsmiddelen* voor de uitvoering van een *Bijzondere Opdracht* is toegestaan onder de volgende voorwaarden: • het *ICT-bedrijfsmiddel* is eerder gebruikt voor eenzelfde *Rubriceringsdomein* en *-niveau;* • het *ICT-bedrijfsmiddel* is gewist voor het gebruik door middel van *Goedgekeurde Middelen*.		•	•	•
4.1.8	*Verwijderbare gegevensdragers* worden voor gebruik gecontroleerd met een speciaal voor dit doel ingerichte *Scrubber* conform bijlage 10.	•	•	•	•
4.1.9	Voor het verwijderen van *ICT-bedrijfsmiddelen* zijn procedures opgesteld, welke door *NBIV* zijn goedgekeurd.	•	•	•	•
4.1.10	Na beëindigen van de *Bijzondere Opdracht* of bij het afvoeren van (defecte) hardware worden deze met *Goedgekeurde Middelen* en een door *NBIV* goedgekeurde procedure gewist. Indien wissen niet (volledig) mogelijk is, worden de (defecte) hardware conform de in bijlage 8 gespecificeerde methoden vernietigd.	•			
4.1.11	Na beëindigen van de *Bijzondere Opdracht* of bij het afvoeren van (defecte) hardware worden deze conform de in bijlage 8 gespecificeerde methoden vernietigd. Er wordt hierbij een bevestiging van vernietiging opgesteld conform formulier 'Bevestiging van vernietiging' en op verzoek verstrekt aan *Opdrachtgever* en/of *NBIV*.		•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.2	**Data classificatie en verwerking**				
4.2.1	Voorafgaand aan de overdracht of uitwisseling van *Bijzondere Informatie* is door de *Beveiligingsfunctionaris* vastgesteld dat de ontvangende partij de *Bijzondere Informatie* conform het vastgestelde beveiligingsniveau kan behandelen en geautoriseerd is om te beschikken over de *Bijzondere Informatie*.	•	•	•	•
4.2.2	*Verwijderbare gegevensdragers* worden alleen gebruikt als onderdeel van een vastgestelde procedure voor data-uitwisseling. Voor deze procedure is onder andere vastgelegd welke specifieke *Verwijderbare gegevensdrager* gebruikt wordt en op welke wijze deze beveiligd, bewaard, gewist of vernietigd dient te worden.	•	•	•	•
4.2.3	*Verwijderbare gegevensdragers* zijn voorzien van een fysiek label conform bijlage 8 op basis van de hoogste *Rubricering* van hetgeen opgeslagen is op de betreffende *Verwijderbare gegevensdrager*.	•	•	•	•
4.2.4	*Gegevensdragers* waar *Bijzondere Informatie* op staat, zijn versleuteld door *Goedgekeurde Middelen*.	•	•	•	•
4.2.5	Voor het wissen van (*Verwijderbare*) *Gegevensdragers*, waar *Bijzondere Informatie* op staat, wordt alleen gebruikgemaakt van *Goedgekeurde Middelen*.	•	•	•	•
4.2.6	Data Leak Prevention (DLP) maatregelen zijn geïmplementeerd in *Systemen*, *Netwerken* en andere apparaten waarop of waarmee *Bijzondere Informatie* wordt gegenereerd, verwerkt of opgeslagen ter voorkoming van het onbedoeld delen (bijvoorbeeld per e-mail) van *Bijzondere Informatie*.	•	•	•	•
4.2.7	*Bijzondere Informatie* van *NAVO* en *EU* wordt, indien vastgesteld door *Opdrachtgever*, verwerkt op een daartoe geaccrediteerd *Systeem*.		•	•	•
4.2.8	Het gebruik van *Artificial Intelligence (AI) systemen* is alleen toegestaan wanneer deze voldoen aan de eisen voor de betreffende *TBB*-categorie en na goedkeuring van *Opdrachtgever*.	•	•	•	•
4.2.9	Bij het gebruik van *AI systemen* is data van verschillende *Rubriceringsdomeinen, -niveaus of Opdrachtgevers* te allen tijde gescheiden.	•	•	•	•
4.2.10	*AI systemen* functioneren volledig binnen het *Vertrouwde Netwerk* en hebben geen koppelingen met onvertrouwde *Netwerken* of *Systemen*.	•	•	•	•
4.2.11	Bij het beëindigen van een *Bijzondere Opdracht* wordt alle (trainings)data, gegenereerde uitkomsten en ontwikkelde *AI* modellen die op basis van *Bijzondere Informatie* tot stand zijn gekomen of herleidbaar zijn tot *Bijzondere Informatie*, overhandigd of vernietigd in afstemming met *NBIV*, tenzij anders overeengekomen met *Opdrachtgever*.	•	•	•	•
4.3	**Identificatie en authenticatie**				
4.3.1	Regels omtrent het gebruik van *ICT-bedrijfsmiddelen* (inclusief het gebruik van wachtwoorden) zijn vastgesteld, gedocumenteerd en ter kennis gesteld aan *Gebruikers*.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.3.2	Toegang tot een *Systeem* is beperkt tot daartoe geautoriseerde *Gebruikers*. Dit wordt voorafgaand aan en tijdens een gebruikers-sessie geautomatiseerd afgedwongen door het *Systeem*.	●	●	●	●
4.3.3	*Authenticatiegegevens* van *Gebruikers* worden bijgehouden in een actuele registratie, op basis waarvan de *Gebruikers* worden geïdentificeerd en geautoriseerd.	●	●	●	●
4.3.4	Op basis van een *Risicoanalyse* is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden toegekend. De risicoafweging, resultaten en maatregelen zijn opgenomen in een autorisatiematrix in het *Beveiligingsplan*.	●	●	●	●
4.3.5	Een account bevat geen indicatie van het privilegeniveau van de *Gebruiker*.	●	●	●	●
4.3.6	Bij de uitgifte van een authenticatiemiddel is de identiteit van de *Gebruiker* en het recht van de *Gebruiker* op het betreffende authenticatiemiddel vastgesteld.	●	●	●	●
4.3.7	Accounts worden voorzien van *Rechten* die noodzakelijk zijn voor de uitvoering van de taken van de *Gebruiker* (‘*Need-to-Know*’, ‘*Need-to-Use*’). Bij het toekennen van *Rechten* wordt ten minste onder-scheid gemaakt tussen lees- en schrijfrechten en de applicaties en commando’s waar een *Gebruiker* toegang tot heeft.	●	●	●	●
4.3.8	De *Rechten* van een *Gebruiker* omvatten niet een gehele cyclus van handelingen in een kritiek *Systeem* voor de beveiliging of uitvoering van de *Bijzondere Opdracht*.	●	●	●	●
4.3.9	Beheerdersrechten zijn beperkt tot *Beheerdersaccounts*. Beheer-activiteiten worden alleen uitgevoerd vanaf *Beheerdersaccounts*.	●	●	●	●
4.3.10	Algemene gebruikersactiviteiten, zoals het gebruik van bedrijfs-applicaties, e-mail en internet, worden alleen uitgevoerd vanaf een *Gebruikersaccount*.	●	●	●	●
4.3.11	*Rechten* van *Beheerders* worden aan een beperkte groep toegekend middels een *Privileged Access Management* (PAM) oplossing. Hiervan wordt een registratie bijgehouden.	●	●	●	●
4.3.12	Toegekende *Rechten* van *Beheerdersaccounts* worden periodiek, minimaal driemaandelijks, geëvalueerd.	●	●		
4.3.13	Toegekende *Rechten* van *Beheerdersaccounts* worden periodiek, minimaal maandelijks, geëvalueerd.			●	●
4.3.14	Activiteiten vanaf een *Beheerdersaccount* zijn gelogd en herleidbaar naar een individu.	●	●	●	●
4.3.15	Alleen daartoe geautoriseerde *Beheerders* kunnen functies en software (de)installeren of (de)activeren.	●	●	●	●
4.3.16	*Serviceaccounts* worden bijgehouden in een actuele registratie, voorzien van eigenaar, doel en datum waarop het *Serviceaccount* voor het laatst is beoordeeld. De noodzaak van een *Serviceaccount* wordt minimaal ieder kwartaal beoordeeld.	●	●	●	●

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.3.17	Systeemprocessen worden uitgevoerd door unieke *Serviceaccounts*, die niet gekoppeld zijn aan een individu. IT-beheer houdt onder toezicht van de *(Cyber-) Beveiligingsfunctionaris* een actuele registratie bij van de *Serviceaccounts* en de bijbehorende *Rechten*.	•	•	•	•
4.3.18	Indien het gebruik van een *Serviceaccount* noodzakelijk is voor de functionaliteit van een *Systeem*, dient deze uitzondering door *NBIV* vooraf goedgekeurd te worden. Bij het gebruik van een *Serviceaccount* gelden de volgende voorwaarden: • er wordt geen persoonlijke of niet-werkgerelateerde informatie verwerkt; • benodigde externe toegang van een *Serviceaccount* is gedocumenteerd in het *Beveiligingsplan*; • een *Serviceaccount* kan niet worden gebruikt om in te loggen op een *Systeem*; • een *Serviceaccount* wordt niet via externe toegang gebruikt.	•	•	•	•
4.3.19	Standaard of automatisch gecreëerde accounts en andere vooraf geconfigureerde accounts worden van een nieuw wachtwoord voorzien en uitgeschakeld door een *Beheerder* onder toezicht van de *(Cyber-)Beveiligingsfunctionaris*.	•	•	•	•
4.3.20	Er is een nood- of 'breakglass' account die enkel toegankelijk is door middel van een 'enveloppenprocedure'. Voor de procedure is vastgelegd hoe een wachtwoord wordt vrijgegeven, wie hiervoor toestemming geeft, hoe het gebruik ervan geregistreerd wordt en dat het wachtwoord na gebruik gewijzigd wordt. Bij gebruik van deze accounts volgt er direct (automatische) alarmering en wordt de *(Cyber-)Beveiligingsfunctionaris* geïnformeerd. Het gebruik wordt geregistreerd door de *(Cyber-)Beveiligingsfunctionaris*.	•	•	•	•
4.3.21	*Rechten* van *Gebruikers* worden periodiek, minimaal halfjaarlijks, geëvalueerd.	•			
4.3.22	*Rechten* van *Gebruikers* worden periodiek, minimaal driemaandelijks, geëvalueerd.		•	•	
4.3.23	*Rechten* van *Gebruikers* worden periodiek, minimaal maandelijks, geëvalueerd.				•
4.3.24	Accounts die 40 dagen niet zijn gebruikt, worden automatisch geblokkeerd.	•	•	•	•
4.3.25	Als een *Gebruiker* vijfmaal een verkeerd wachtwoord invoert, wordt het *Gebruikersaccount* geblokkeerd.	•			
4.3.26	Als een *Gebruiker* driemaal een verkeerd wachtwoord invoert, wordt het *Gebruikersaccount* geblokkeerd.		•	•	•
4.3.27	Als een *Beheerder* driemaal een verkeerd wachtwoord invoert wordt het *Beheerdersaccount* geblokkeerd. Het *Beheerdersaccount* wordt pas na goedkeuring van de *(Cyber-) Beveiligingsfunctionaris* vrijgegeven.	•	•	•	•
4.3.28	Een geblokkeerd account wordt gedeblokkeerd volgens een door de *(Cyber-)Beveiligingsfunctionaris* goedgekeurde procedure.	•			
4.3.29	Een geblokkeerd account mag alleen worden gedeblokkeerd na goedkeuring van de *(Cyber-)Beveiligingsfunctionaris*.		•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.3.30	Wachtwoorden voldoen minimaal aan de volgende kenmerken: • wachtwoorden bestaan uit minimaal 15 karakters; • duidelijke patronen (bijvoorbeeld '1234' en 'qaz') zijn uitgesloten; • het wachtwoord bevat ten minste 3 van de volgende categorieën: hoofdletters, kleine letters, getallen en leestekens.	•	•	•	•
4.3.31	Ten aanzien van het gebruik van wachtwoorden geldt: • minimaal jaarlijks wordt een nieuw wachtwoord ingesteld; • initiële wachtwoorden en wachtwoorden die zijn gereset hebben een maximale geldigheidsduur van 24 uur en dienen bij het eerste gebruik gewijzigd te worden; • initiële wachtwoorden en wachtwoorden die zijn gereset zijn uniek en worden niet hergebruikt; • initiële wachtwoorden voldoen aan alle reguliere vereisten voor wachtwoorden; • wachtwoorden worden op een veilige manier uitgegeven, waarbij ten minste de identiteit van de *Gebruiker* en het recht van de *Gebruiker* op het authenticatiemiddel is gecontroleerd; • wachtwoorden worden niet via hetzelfde kanaal als het *Gebruikersaccount* verstrekt.	•	•	•	•
4.3.32	De regels omtrent het gebruik van een *Te Beschermen Belang* en *ICT-bedrijfsmiddelen* (inclusief het gebruik van wachtwoorden), omvatten minimaal het volgende: • wachtwoorden worden 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 ander persoon; • wachtwoorden worden niet hergebruikt; • wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).	•	•	•	•
4.3.33	Om in te loggen op een *Gebruikersaccount* wordt gebruikgemaakt van persoonsgebonden *Multi-factor authenticatie*, waarbij SMS niet als een factor geldt.	•			
4.3.34	Om in te loggen op een *Gebruikersaccount* wordt gebruikgemaakt van persoonsgebonden *Multi-factor authenticatie,* waarvan één van de factoren een *Hardware token* is en waarbij SMS niet als een factor geldt.		•	•	•
4.3.35	Om in te loggen op een *Beheerdersaccount* wordt gebruikgemaakt van persoonsgebonden *Multi-factor authenticatie*, waarvan één van de factoren een *Hardware token* is en waarbij SMS niet als een factor geldt.	•	•	•	•
4.3.36	Bij het gebruik van *Biometrie* als authenticatiefactor voor *Multi-factor authenticatie* is *Authenticatie* op basis van een pincode als alternatieve mogelijkheid uitgesloten.	•	•	•	•
4.3.37	Indien *Hardware tokens, Biometrische* toepassingen of *Multi-factor authenticatie* worden gebruikt, kunnen deze niet worden uitgeschakeld door *Gebruikers*. De *(Cyber-)Beveiligingsfunctionaris* houdt een actuele registratie bij van gebruikte *Hardware tokens.*	•	•	•	•
4.3.38	Voorafgaand aan het gebruik van een *Systeem* wordt een *Melding* aan de *Gebruiker* getoond dat alleen geautoriseerd gebruik is toegestaan voor de expliciet door de organisatie vastgestelde doeleinden.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.3.39	Een account kan maximaal drie actieve werkplekken (sessies) hebben.	•			
4.3.40	Een account kan maximaal één actieve werkplek (sessie) hebben.		•	•	•
4.3.41	Indien er een operationele noodzaak is voor het gebruik van een groepsaccount, dient deze uitzondering door *NBIV* vooraf goedgekeurd te zijn. Bij het gebruik van een groepsaccount gelden de volgende voorwaarden: • de *(Cyber-)Beveiligingsfunctionaris* verleent toestemming voor het gebruik; • het gebruik van een groepsaccount is te herleiden naar een individu; • het is niet mogelijk om via externe toegang gebruik te maken van een groepsaccount; • het is niet mogelijk om toegang te hebben tot externe *Systemen* (bijvoorbeeld het internet) met behulp van een groepsaccount; • het is niet mogelijk om persoonlijke of niet-werkgerelateerde informatie te verwerken met behulp van een groepsaccount.	•			
4.3.42	Het gebruik van groepsaccounts is niet toegestaan.		•	•	•
4.3.43	Het wachtwoord wordt niet getoond op het scherm tijdens het invoeren en er wordt geen informatie getoond die herleidbaar is tot de *Authenticatiegegevens*.	•	•	•	•
4.3.44	*Gebruikers* kunnen zelf hun wachtwoord kiezen en wijzigen. Hierbij geldt ten minste het volgende: • voordat een *Gebruiker* zijn wachtwoord kan wijzigen, wordt de *Gebruiker* opnieuw geauthentiseerd; • ter voorkoming van typefouten in het nieuw gekozen wachtwoord is een bevestigingsprocedure van toepassing.	•	•	•	•
4.3.45	Wachtwoorden worden niet in originele vorm (plain text) opgeslagen of verstuurd, tenzij het wordt gebruikt ten behoeve van een 'enveloppenprocedure'.	•	•	•	•
4.3.46	Bij een succesvolle aanmelding wordt de datum en tijd van de voorgaande aanmelding of aanmeldpoging aan de *Gebruiker* getoond.		•	•	•
4.4	**Configuratiemanagement**				
4.4.1	Alle functionaliteit van hardware en software (zoals instellingen, netwerkpoorten, USB-poorten, diensten, accounts, systeemhulpmiddelen) die niet vereist zijn voor de *Bijzondere Opdracht*, zijn uitgeschakeld.	•	•	•	•
4.4.2	Op basis van een *Risicoanalyse* kan wanneer strikt noodzakelijk voor de uitvoering van de *Bijzondere Opdracht* met goedkeuring van de *(Cyber-) Beveiligingsfunctionaris* een uitzondering worden gemaakt voor het inschakelen van functionaliteiten van hardware en software, zoals bijvoorbeeld *Gegevensdragers*. De *(Cyber-) Beveiligingsfunctionaris* houdt een actuele registratie bij van deze uitzonderingen.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.4.3	Van alle apparatuur die gebruikt wordt in het kader van de *Bijzondere Opdracht* of die zich binnen het *Compartiment* bevindt, zijn alle componenten voor *Draadloze communicatie* (zoals Wi-Fi, Bluetooth, NFC en 5G) en alle camera's en microfoons verwijderd of hardwarematig onklaar gemaakt. Indien specifieke functionaliteit noodzakelijk is voor de uitvoering van een *Bijzondere Opdracht* kan een uitzondering gemaakt worden. Uitzonderingen zijn vooraf goedgekeurd door *NBIV*.		•	•	•
4.4.4	*Hardening* is toegepast op hardware en software, inclusief authenticatieprotocollen en -mechanismen, in lijn met de door de fabrikant voorgeschreven en aanbevolen beveiligingsmaatregelen, aangevuld op basis van recente marktstandaarden.	•	•	•	•
4.4.5	Het interne en externe dataverkeer wordt op basis van een *Risicoanalyse* beperkt tot de noodzakelijke protocollen en sessies.	•	•	•	•
4.4.6	Software, servers, gebruikers-, netwerk- en opslagapparatuur worden middels een vastgesteld proces voorzien van veilige configuraties. Deze configuraties zijn vastgelegd, worden minimaal jaarlijks beoordeeld en waar nodig aangepast en op verzoek gedeeld met *NBIV*.	•	•	•	•
4.4.7	Een mechanisme controleert de instellingen van informatiebeveiligingsfuncties (zoals securitysoftware) op het *Koppelvlak* tussen verschillende *Netwerken* op ongeautoriseerde wijzigingen.	•	•	•	•
4.4.8	De instellingen van logmechanismen zijn zodanig beschermd dat deze niet onopgemerkt aangepast of gemanipuleerd kunnen worden. Wijzigingen worden gecontroleerd middels het vier-ogen principe.	•	•	•	•
4.4.9	Systeemklokken maken gebruik van dezelfde tijdsynchronisatie en zijn zodanig beveiligd tegen wijzigingen dat deze niet onopgemerkt aangepast of gemanipuleerd kunnen worden.	•	•	•	•
4.4.10	Er wordt alleen door de *(Toe)leverancier* actief onderhouden hardware en software gebruikt.	•	•	•	•
4.4.11	*Systeemdocumentatie* is, wanneer deze gevoelige informatie bevat over beveiligingsmaatregelen van een *Te Beschermen Belang* die zich op het *Systeem* bevindt, op hetzelfde niveau beveiligd als het *Te Beschermen Belang*.	•	•	•	•
4.4.12	Ten behoeve van het uitvoeren van beheertaken zijn systeemconfiguraties, met inbegrip van hardware, software, diensten, *Netwerken* en beveiliging, gedocumenteerd.	•	•	•	•
4.5	**Netwerkbeveiliging**				
4.5.1	*Netwerken*, *Systemen* en applicaties worden gemonitord en beheerd zodat aanvallen, storingen en/of fouten ontdekt en hersteld kunnen worden en de *Beschikbaarheid* niet onder het afgesproken minimum niveau komt. Dit minimum is opgenomen in het *Beveiligingsplan*.	•	•	•	•
4.5.2	Continue real-time *Monitoring* en *Logging* van al het inkomende en uitgaande netwerkverkeer en netwerkkoppelingen zijn ingericht, waarbij wordt gelet op afwijkingen van het normaalbeeld en waar nodig (geautomatiseerd) wordt ingegrepen.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.5.3	Alle *Draadloze communicatie* wordt behandeld als *Externe (netwerk) koppeling*.	●			
4.5.4	Het gebruik van *Draadloze communicatie* is niet toegestaan.		●	●	●
4.5.5	In geval van een *Externe (netwerk) koppeling* is een *DMZ* toegepast.	●			
4.5.6	Voor in- en uitgaand dataverkeer van en naar een onvertrouwde omgeving, zowel intern als extern, zijn beveiligingsmaatregelen getroffen zoals een *DMZ*, *Proxy*-server en/of sandbox.	●			
4.5.7	Alle beveiligingsmechanismes maken gebruik van actuele indicatoren, zoals virusdefinities en *Signatures*.	●	●	●	●
4.5.8	Beveiligingsmechanismes ten behoeve van de *Bijzondere Opdracht* mogen niet voortkomen uit een land dat een *Offensief cyberprogramma* tegen de Nederlandse belangen heeft.	●	●	●	●
4.5.9	Minimaal jaarlijks worden de geïmplementeerde beveiligingsmaatregelen op een *Koppelvlak* getest op de werking. Bevindingen worden opgevolgd en gedocumenteerd.	●	●	●	●
4.5.10	Minimaal elke 6 maanden worden de geïmplementeerde beveiligingsmechanismen van *Netwerken*, *Systemen* en applicaties gecontroleerd op de werking. Bevindingen worden opgevolgd en gedocumenteerd.		●	●	●
4.5.11	*Toegang op afstand* tot een *Te Beschermen Belang* (via een remote inlogvoorziening) vindt alleen plaats middels *Goedgekeurde Middelen* en door *NBIV* goedgekeurde procedures. De gebruikte apparatuur voldoet aan de relevante beveiligingseisen voor het betreffende *Rubriceringsniveau*.	●			
4.5.12	In *Koppelvlakken* met externe of onvertrouwde *Netwerken* zijn maatregelen getroffen om mogelijke aanvallen die de *Betrouwbaarheid* van de informatievoorziening negatief beïnvloeden (bijvoorbeeld *(D)DoS*-aanvallen) te signaleren en hierop te reageren.	●	●	●	●
4.5.13	*Systemen* die voor hun functionaliteit gebruikmaken van een verbinding met een externe dienst (zoals licentieservers en Device Management oplossingen) zijn vooraf goedgekeurd door *NBIV*. Hierbij zijn mechanismes geïmplementeerd om: • data-uitwisseling tot het strikt noodzakelijke te beperken; • te voorkomen dat (informatie die herleidbaar is tot) *Bijzondere Informatie*, *Vertrouwensfuncties* en unieke kenmerken van de *Technische infrastructuur* het *Vertrouwde Netwerk* verlaat; • alle interacties met een externe dienst te monitoren, te loggen en frequent te evalueren om verdachte activiteiten vroegtijdig te detecteren.	●			
4.5.14	*Netwerken* zijn voorzien van beheersmaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron- en bestemmingsadressen.	●	●	●	●
4.5.15	Er zijn technische maatregelen getroffen om te voorkomen dat interne netwerkadressen naar buiten toe routeren, zoals het toepassen van Outbound Traffic Filtering.	●	●	●	●

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.5.16	*Bijzondere Informatie* wordt alleen verzonden over een onvertrouwde verbinding wanneer de *Bijzondere Informatie* versleuteld is door middel van *Goedgekeurde Middelen*.	●	●		
4.5.17	Technische en procedurele maatregelen zijn getroffen om te waarborgen dat alleen geïdentificeerde en geauthentiseerde apparatuur kan worden verbonden met het *Netwerk*. Wanneer onbekende apparatuur wordt aangesloten vindt er alarmering plaats.	●	●	●	●
4.5.18	TOR (The Onion Router)/Darknet verkeer is geblokkeerd.	●	●	●	●
4.5.19	Op verzoek van *NBIV* wordt door *Opdrachtnemer* medewerking verleend aan: • het plaatsen van een detectiemiddel; • het monitoren van netwerkverkeer en hosts door gebruik van een detectiemiddel; • het uitvoeren en aanleveren van specifieke *Logging* verzoeken voor de lokale- en *Cloud* omgevingen (inclusief telemetrie); • het installeren van host based detectie; • het gebruik maken van een door de *Rijksoverheid* geleverde *DNS*-dienst.	●	●	●	●
4.5.20	De gebruikte versleutelingsprotocollen zijn de meest recente conform (inter)nationale beveiligingsstandaarden. Nieuw gepubliceerde standaarden dienen binnen de minimaal haalbare termijn geïmplementeerd te worden. Aansluitvoorwaarden van *Opdrachtgever* prevaleren en afwijkingen worden gemeld aan *NBIV*.	●	●	●	●
4.5.21	*Netwerken* voor verschillende *Rubriceringsdomeinen* zijn gescheiden en toegang is beveiligd middels *Goedgekeurde Middelen*.	●			
4.5.22	*Netwerken* voor verschillende *Rubriceringsdomeinen* zijn fysiek gescheiden en toegang is beveiligd middels *Goedgekeurde Middelen*.		●	●	●
4.5.23	*Internationale Netwerkkoppelingen* maken gebruik van door *NBIV* goedgekeurde producten en procedures.	●	●	●	●
4.5.24	*Netwerken* van eenzelfde juridische entiteit waarop een *Te Beschermen Belang* is opgeslagen zijn alleen gekoppeld middels *Goedgekeurde Middelen* en door *NBIV* goedgekeurde procedures.	●	●	●	●
4.5.25	*Netwerken* van verschillende juridische entiteiten waarop een *Te Beschermen Belang* is opgeslagen zijn alleen gekoppeld na goedkeuring van *Opdrachtgever*. Alle entiteiten beschikken over de vereiste *ABRO-Verklaring*, de koppeling maakt gebruik van *Goedgekeurde Middelen* en door *NBIV* goedgekeurde procedures, en er is voldaan aan de aansluitvoorwaarden van de betreffende *Netwerken*.	●	●	●	●
4.5.26	Bij *Koppelvlakken* tussen *Netwerken* van verschillende *Rubriceringsniveaus* is informatie-uitwisseling alleen mogelijk van een *Netwerk* met een lager *Rubriceringsniveau* naar een *Netwerk* met een hoger *Rubriceringsniveau*. De koppeling maakt gebruik van *Goedgekeurde Middelen*. Uitgewisselde informatie wordt behandeld conform het *Rubriceringsniveau* van het *Segment* waarop de informatie zich bevindt.	●	●	●	●

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.5.27	Bij *Koppelvlakken* tussen *Netwerken* van verschillende *Rubriceringsniveaus* is informatie-uitwisseling van een *Netwerk* met een hoger *Rubriceringsniveau* naar een *Netwerk* met een lager *Rubriceringsniveau* niet mogelijk.		●	●	●
4.5.28	Ontsluiting van een *Te Beschermen Belang* op een *Netwerk* tussen verschillende locaties van de *Opdrachtnemer* (WAN) is niet toegestaan.				●
4.5.29	De *Technische infrastructuur* is ingedeeld in *Segmenten*. *Opdrachtnemer* draagt zorg dat binnen één *Segment* alleen *Bijzondere Informatie* wordt verwerkt van hetzelfde *Rubriceringsdomein* en *-niveau*. *Opdrachtnemer* evalueert dit minimaal jaarlijks en herziet *Segmenten* indien nodig.	●	●	●	●
4.5.30	Elk *Segment* heeft een gedefinieerd *Rubriceringsdomein* en *-niveau*. Bij *Koppelvlakken* tussen *Segmenten* vindt controle plaats op protocol, inhoud en richting van de communicatie.	●	●	●	●
4.5.31	*Segmenten* zijn alleen ingericht met voorzieningen die strikt noodzakelijk zijn voor de functionaliteit. Beheer en audit van *Segmenten* vindt plaats vanuit een logisch gescheiden *Segment*.	●			
4.5.32	*Segmenten* zijn alleen ingericht met voorzieningen die strikt noodzakelijk zijn voor de functionaliteit. Beheer en audit van *Segmenten* vindt plaats vanuit een *Segment*.		●	●	●
4.5.33	Segmentering is toegepast om groepen van *Systemen*, diensten en *Gebruikers* te scheiden in het *Netwerk*. Bijvoorbeeld door middel van een firewall of *DMZ*.	●	●	●	●
4.5.34	Bij de toepassing van *Virtualisatie* in het kader van de *Bijzondere Opdracht* wordt een *Risicoanalyse* uitgevoerd door de *(Cyber-) Beveiligingsfunctionaris* en een *Beheerder*. Hierbij gelden ten minste de volgende voorwaarden: • beveiligingsfunctionaliteiten draaien op fysiek gescheiden virtualisatieplatforms; • alleen systeemcomponenten met hetzelfde *Rubriceringsdomein* en *-niveau* worden gecombineerd; • het ontwerp en de implementatie zijn vooraf goedgekeurd door *NBIV*; • de management interface is enkel bereikbaar vanuit het beheersegment; • het *Virtualisatie* platform is gehardend conform de instructie van de leverancier.	●	●	●	●
4.5.35	Het toepassen van VLAN's is alleen toegestaan in *Netwerken* met hetzelfde *Rubriceringsdomein* en *-niveau*. Het ontwerp en de implementatie zijn vooraf goedgekeurd door NBIV. Hierbij gelden ten minste de volgende voorwaarden: • een firewall wordt gebruikt om ongewenst verkeer te filteren; • marktstandaarden voor de configuratie van VLAN's zijn toegepast; • netwerkpoorten worden statisch of op basis van een certificaat toegewezen aan een VLAN.	●	●	●	●

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.6	**Endpoint beveiliging**				
4.6.1	Voorzieningen voor *Toegang op afstand* zijn zo ingericht dat op het werkstation of *Mobiel apparaat* geen enkele informatie vanuit een *Vertrouwde Netwerk* wordt opgeslagen (*Zero footprint*). Het werkstation of *Mobiel apparaat* is versleuteld met een binnen het *Systeem* beschikbare harde schijf encryptie module, waarbij gebruikt wordt gemaakt van Firmware TPM, Secure boot en Pre-boot authentication.	•			
4.6.2	Voorzieningen voor *Toegang op afstand* zijn zo ingericht dat mogelijke *Malware* vanaf het werkstation of *Mobiele apparaat* niet in het deel terecht kan komen waar *Bijzondere Informatie* is opgeslagen.	•			
4.6.3	Het is niet mogelijk ongeautoriseerde software of scripts te installeren of uit te voeren op een werkstation of *Mobiele apparatuur.* Dit wordt technisch afgedwongen, waarbij afwijkingen worden gedetecteerd en opgevolgd. Uitzonderingen worden schriftelijk goedgekeurd en geregistreerd door de *(Cyber-) Beveiligingsfunctionaris*.	•	•	•	•
4.6.4	Indien een *Gebruiker* ingelogd is op een werkplek(sessie), dan vindt het overnemen van de werkplek(sessie) door een *Beheerder* alleen plaats na toestemming van de *Gebruiker*. Er is een mogelijkheid om overname van de werkplek(sessie) zelf te beëindigen en er verschijnt een *Melding* dat de werkplek(sessie) is beëindigd. De *Gebruiker* houdt toezicht dat de *Beheerder* niet kennisneemt van een *Te Beschermen Belang*.	•	•	•	•
4.6.5	Apparaten die toegang geven tot een *Te Beschermen Belang* zijn, voorafgaand aan de toegang, geautomatiseerd gecontroleerd op naleving van een vooraf gedefinieerd beveiligingsbeleid.	•	•	•	•
4.6.6	Een werkplek (sessie) wordt na 10 minuten inactiviteit automatisch vergrendeld (*Clear Screen*).	•	•		
4.6.7	Een werkplek (sessie) wordt na 5 minuten inactiviteit automatisch vergrendeld (*Clear Screen*).			•	•
4.6.8	Bij het gebruik van een *Hardware token* wordt de werkplek (sessie) automatisch vergrendeld bij het verwijderen van de *Hardware token.*	•	•	•	•
4.6.9	Voor het uitzetten/uitstellen van de automatische vergrendeling op een werkplek (sessie) gelden de volgende voorwaarden: • automatische vergrendeling is alleen uitgezet of uitgesteld wanneer er een operationele noodzaak is; • voordat automatische vergrendeling wordt uitgezet of uitgesteld, is hiervoor toestemming verleend door de *(Cyber-) Beveiligingsfunctionaris*; • de *(Cyber-)Beveiligingsfunctionaris* onderhoudt een actuele registratie van de werkplek (sessie) waar dit het geval is en de noodzaak waarom toestemming is gegeven; • iedere toestemming wordt jaarlijks geëvalueerd.	•	•	•	•
4.6.10	Anti-*Malware* software scant periodiek, minimaal dagelijks, *Systemen* en voert directe scans uit op bestanden, e-mails en overige informatie wanneer deze worden gedownload, geopend, opgeslagen of uitgevoerd. Gevonden *Malware* wordt in quarantaine geplaatst.	•			

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.6.11	Anti-*Malware* software scant periodiek, minimaal dagelijks, *Systemen* en voert directe scans uit op bestanden en overige informatie wanneer deze worden geopend, opgeslagen of uitgevoerd. Gevonden *Malware* wordt in quarantaine geplaatst.		•	•	•
4.6.12	De update voor de detectiedefinities vindt minimaal dagelijks plaats. Indien hiervoor gebruik wordt gemaakt van online/*Cloud* gebaseerde anti-*Malware* services dan wordt dit vooraf ter goedkeuring voorgelegd aan *NBIV* en beschreven in het *Beveiligingsplan*.	•	•	•	•
4.7	**Beheer van mobiele apparatuur**				
4.7.1	Een *Te Beschermen Belang* wordt alleen opgeslagen of verwerkt op *Mobiele apparatuur* voor zover dit strikt noodzakelijk is voor de *Bijzondere Opdracht*, waarbij: • voor de versleuteling gebruikt wordt gemaakt van *Goedgekeurde Middelen*; • alleen de strikt noodzakelijke hoeveelheid informatie is opgeslagen; • de betreffende *Mobiele apparatuur* alleen wordt gebruikt waar en wanneer kennisname door ongeautoriseerde personen niet mogelijk is; • er wordt voldaan aan de relevante beveiligingseisen voor het betreffende *Rubriceringsniveau*.	•	•	•	•
4.7.2	*Mobiele apparatuur* buiten het *Compartiment* bevat geen kenmerken die direct herleidbaar zijn tot *Opdrachtgever* of *Opdrachtnemer* (zowel fysiek op de *Mobiele apparatuur* als weergegeven op het scherm van de *Mobiele apparatuur*).	•	•	•	•
4.7.3	*Mobiele apparatuur* waarop een *Te Beschermen Belang* wordt gegenereerd, is opgeslagen of wordt verwerkt, maakt alleen gebruik van een *Externe koppeling* wanneer deze is goedgekeurd door *NBIV*.	•			
4.7.4	Bij *Toegang op afstand* wordt al het verkeer van en naar de apparatuur gerouteerd over een versleutelde verbinding middels *Goedgekeurde Middelen*. Op basis van een *Risicoanalyse* kan met voorafgaande goedkeuring van *NBIV* een uitzondering worden gemaakt, bijvoorbeeld ten behoeve van Mobile Device Management, updates of het wissen van data.	•			
4.7.5	Voor het gebruik van *Mobiele apparatuur* en *Toegang op afstand* zijn gebruiksinstructies opgesteld.	•			
4.7.6	Na verlies of diefstal van *Mobiele apparatuur* wordt de communicatiemogelijkheid met de centrale applicaties afgesloten, het authenticatiemechanisme gereset en bijbehorende *Certificaten* direct ingetrokken. De data wordt zo snel mogelijk op afstand gewist.	•			
4.7.7	Indien *Mobiele apparatuur* zich buiten het *Compartiment* bevindt, wordt deze, bij geen gebruik, binnen 2 minuten vergrendeld.	•			
4.7.8	Inkijkbeperkende maatregelen (bijv. screenfilters) zijn toegepast voor *Mobiele Apparatuur* die zich buiten het *Compartiment* bevindt.	•			
4.7.9	Inkijkbeperkende maatregelen (bijv. screenfilters) zijn toegepast op alle apparatuur.		•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.8	**Cryptografie**				
4.8.1	*Cryptografische beveiligingsoplossingen* zijn ingericht en worden beheerd conform de via *NBIV* verkregen documentatie. Daarnaast worden de volgende adviezen en voorwaarden opgevolgd en gedocumenteerd in het *Beveiligingsplan*: • de aansluitvoorwaarden van de *Opdrachtgever*; • het inzetadvies, zoals verkregen via *NBIV*; • adviezen van de fabrikant. Voor zover deze met elkaar in tegenspraak zijn, prevaleren de aansluitvoorwaarden boven het inzetadvies, welke prevaleert boven de adviezen van de fabrikant.	•	•	•	•
4.8.2	Het proces, de rollen, functionarissen en hun verantwoordelijkheden ten aanzien van het beheer van *Cryptografische beveiligingsoplossingen* zijn vastgelegd in het cryptografiebeleid (*RASCI*), als onderdeel van het *Beveiligingsplan*.	•	•	•	•
4.8.3	Indien *Opdrachtnemer* cryptografische sleutels krijgt aangeleverd via de Nationale Distributie Autoriteit of *Opdrachtgever*, zijn er ten minste twee *Cryptobeheerders* aangesteld, tenzij met *NBIV* anders is overeengekomen. De *Cryptobeheerder* voert de taken uit zoals beschreven in bijlage 3.	•	•	•	•
4.8.4	De geldigheidsduur van cryptografische sleutels is bepaald door de leverancier of het inzetadvies en is vastgelegd in het cryptografiebeleid, als onderdeel van het *Beveiligingsplan*.	•	•	•	•
4.8.5	Het beheer van *Cryptografische beveiligingsoplossingen* vindt plaats middels het vier-ogen principe.	•	•	•	•
4.8.6	Voor het beheer van *Cryptografische beveiligingsoplossingen* zijn *Beheerders* opgeleid en zijn beheerdersinstructies aan *Beheerders* overhandigd.	•	•	•	•
4.8.7	Voor het gebruik van *Cryptografische beveiligingsoplossingen* zijn gebruikersinstructies aan *Gebruikers* overhandigd.	•	•	•	•
4.8.8	*Gebruikers* van *Cryptografische beveiligingsoplossingen* zijn hiertoe opgeleid door *Opdrachtnemer*.		•	•	•
4.8.9	*Cryptografische beveiligingsoplossingen* worden alleen toegepast als gebruik gemaakt wordt van *Goedgekeurde Middelen*.	•	•	•	•
4.8.10	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften (zoals exportrestricties) *Cryptografische beveiligingsoplossingen* moeten voldoen. Dit is vastgelegd in het *Beveiligingsplan*. De *Beveiligingsfunctionaris* houdt hier toezicht op.	•	•	•	•
4.8.11	Cryptografische sleutels, apparatuur en documentatie worden tijdens de gehele levensduur op minimaal hetzelfde niveau beveiligd als de *Te Beschermen Belangen* die versleuteld worden met de betreffende sleutel, tenzij het inzetadvies anders voorschrijft.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.8.12	Cryptografische sleutels die zijn verlopen worden niet gebruikt en worden vernietigd of behandeld conform het inzetadvies. Verlopen sleutels waarvoor geen inzetadvies beschikbaar is, worden in afstemming met *NBIV* vernietigd of behandeld.	•	•	•	•
4.8.13	Van alle cryptografische sleutels die zijn of worden gebruikt, wordt een actuele registratie bijgehouden door de *Cryptobeheerder*. De registratie is voorzien van de ontvanger, de locatie, het gebruik en de vernietiging van de sleutels conform de voorwaarden van de eigenaar van de sleutel.	•	•	•	•
4.8.14	Voorafgaand aan het inladen van een nieuwe cryptografische sleutel worden *Cryptografische beveiligingsoplossingen* gecontroleerd op *Compromittatie*, zoals beschreven in de beheerdersinstructie. Denk hierbij aan het controleren van fysieke zegels, *Logging* en software validatie. Er is een registratie bijgehouden door de *Cryptobeheerder* of, indien deze niet is aangesteld, door de *(Cyber-) Beveiligingsfunctionaris*.	•	•	•	•
4.8.15	Een procedure is vastgesteld voor het omgaan met (mogelijk) gecompromitteerde *Cryptografische beveiligingsoplossingen*. Bij *Compromittatie* wordt dit direct gemeld bij de eigenaar van de sleutel en *NBIV*.	•	•	•	•
4.8.16	Beheer van *Cryptografische beveiligingsoplossingen* vindt plaats vanuit een beheersegment zonder toegang tot externe of onvertrouwde *Netwerken* met uitzondering van bestandsversleuteling middels *Goedgekeurde Middelen*.	•			
4.8.17	Beheer van *Cryptografische beveiligingsoplossingen* vindt plaats vanuit een beheersegment dat specifiek voor dit doeleinde is ingericht conform het *Rubriceringsniveau*.		•	•	•
4.8.18	Voor de gehele life cycle van digitale *Certificaten* die binnen de organisatie worden gebruikt voor IT-voorzieningen ten behoeve van een *Bijzondere Opdracht* is een procedure vastgesteld.	•	•	•	•
4.8.19	Een extern controleerbaar *Certificaat* is verstrekt door een daartoe gecertificeerde *Leverancier* (zoals WebTrust of ETSI).	•			
4.8.20	Een Root Certificate Authority-sleutel is opgeslagen in een stand-alone *Hardware Security Module (HSM)* die voldoet aan FIPS 140-3.	•	•	•	•
4.8.21	Een *HSM* waarop een Root Certificate Authority-sleutel is opgeslagen is fysiek minimaal beveiligd op het beveiligingsniveau dat geldt voor TBB 3. Hierbij is *Need-to-Know* en *Need-to-Be* strikt toegepast.	•			
4.8.22	Een *HSM* waarop een Root Certificate Authority-sleutel is opgeslagen is fysiek minimaal beveiligd op het beveiligingsniveau van de *Bijzondere Opdracht*. Hierbij is *Need-to-Know* en *Need-to-Be* strikt toegepast.		•	•	•
4.9	**Fysieke- en omgevingsbeveiliging**				
4.9.1	Apparatuur en bekabeling is zo geplaatst en beschermd dat risico's van schade en storing van buitenaf zijn teruggebracht tot een aanvaardbaar niveau, op basis van een *Risicoanalyse*.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.9.2	Ter voorkoming van geleiding en emissie dienen niet gebruikte spannings- of databekabeling of losse metaalgeleiders te worden verwijderd.		•	•	•
4.9.3	Printers maken standaard gebruik van een 'beveiligd afdrukken' functie (bijvoorbeeld door middel van pincodeverificatie).	•	•	•	•
4.9.4	Alle *Bijzondere Informatie* die zich buiten het daarvoor bestemde fysieke *Compartiment* bevindt, is versleuteld door middel van *Goedgekeurde Middelen*.	•	•	•	•
4.10	**Kwetsbaarheden- en patchmanagement**				
4.10.1	Een proces is ingericht voor het identificeren en *Mitigeren* van technische kwetsbaarheden. Dit omvat o.a. detectie van technische kwetsbaarheden (minimaal ieder kwartaal) en periodieke *Penetratietests* (minimaal jaarlijks). De resultaten hiervan worden op verzoek gedeeld met *NBIV*. *Penetratietests* zijn enkel van toepassing op *Netwerken* met een verbinding naar een ander (extern) *Netwerk*.	•	•	•	•
4.10.2	Een proces is ingericht om nieuwe updates en *Patches* tijdig te identificeren en door te voeren. Het doorvoeren van een update of *Patch* vindt plaats na controle.	•	•	•	•
4.10.3	Kritieke updates en *Patches* worden zo spoedig mogelijk doorgevoerd.	•	•	•	•
4.10.4	Indien een kwetsbaarheid bekend is met een *CVSS* score van 4.0 of hoger voor een *Systeem* met een *Externe koppeling*, dan wordt de *Externe koppeling* met het *Systeem* in overleg met *Opdrachtgever* verbroken en het *Systeem* buiten gebruik gesteld tot de kwetsbaarheid gepatcht of aantoonbaar gemitigeerd is. *Opdrachtnemer* informeert *NBIV* hierover gedurende dit proces.	•	•	•	•
4.11	**Wijzigingenbeheer**				
4.11.1	Wijzigingen aan een *Te Beschermen Belang* verlopen via een vastgesteld wijzigingsbeheerproces waarmee wijzigingen herleidbaar zijn en mogelijke negatieve effecten inzichtelijk gemaakt kunnen worden. Het doorvoeren van wijzigingen geschiedt enkel met voorafgaande goedkeuring van de *(Cyber-)Beveiligingsfunctionaris*.	•	•	•	•
4.11.2	Wijzigingen aan de configuratie van *Systemen* worden alleen doorgevoerd na aantoonbare controle en acceptatie van een andere daartoe aangewezen *Geautoriseerde Medewerker*. Van de acceptatie is een log bijgehouden.	•	•	•	•
4.12	**Onderhoud**				
4.12.1	Apparatuur, software en *Gegevensdragers* worden geïnstalleerd, gebruikt en onderhouden conform de voorschriften van de fabrikant, voor zover dit niet conflicteert met en past binnen het gebruik en onderhoudsplan van *Opdrachtnemer*. Afwijkingen dienen gemeld te worden bij *NBIV*.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.12.2	Procedures (inclusief rollen en verantwoordelijkheden) voor het beheer van de IT-voorzieningen waarin *Bijzondere Informatie* wordt verwerkt (o.a. ten aanzien van back-up en herstel, afhandelen van fouten en noodprocedures) zijn vastgesteld en beschikbaar gesteld aan *Beheerders* en worden minimaal jaarlijks geëvalueerd en waar nodig aangepast.	•	•	•	•
4.12.3	*Beheer op afstand* van *Systemen* is beperkt tot situaties waarin dit strikt noodzakelijk is en gebeurt aan de hand van een vast-gestelde procedure via een verbinding die enkel kan worden geactiveerd door een *Geautoriseerde Medewerker*.	•			
4.12.4	Voor *Onderhoud* en *Beheer op afstand* worden enkel *Goedgekeurde Middelen* gebruikt.	•			
4.12.5	Toegang voor *Onderhoud op afstand* door een *(Toe)leverancier* gebeurt enkel op basis van een wijzigingsverzoek of storings-melding met voorafgaande goedkeuring van de *(Cyber-) Beveiligingsfunctionaris*. Hiervan wordt een actuele registratie bijgehouden.	•			
4.12.6	*Onderhoud* en *beheer op afstand* van *Systemen* is niet toegestaan.		•	•	•
4.12.7	Onderhoud aan *Netwerkapparatuur* of apparatuur waarvan de datadrager niet te verwijderen is, vindt uitsluitend plaats op locatie van *Opdrachtnemer* met toepassing van door *NBIV* goed-gekeurde procedures. De procedures ten aanzien van onderhoud zijn als bijlage opgenomen in het *Beveiligingsplan*.	•			
4.12.8	Onderhoud aan apparatuur vindt uitsluitend plaats op locatie van *Opdrachtnemer* met toepassing van door *NBIV* goedgekeurde procedures. De procedures ten aanzien van onderhoud zijn als bijlage opgenomen in het *Beveiligingsplan*.		•	•	•
4.13	**Monitoring en logging**				
4.13.1	*Systeem*- en gebruikersactiviteiten worden minimaal gelogd conform de richtlijnen van de *JSCU Logging-essentials*. Op basis van een *Risicoanalyse* is vastgesteld welke aanvullende *Logging* noodzakelijk is. Deze logbestanden zijn minimaal 6 maanden beschikbaar.	•			
4.13.2	Systeem- en gebruikersactiviteiten worden minimaal gelogd conform de richtlijnen van de *JSCU Logging-essentials*. Op basis van een *Risicoanalyse* is vastgesteld welke aanvullende *Logging* noodzakelijk is. Deze logbestanden zijn minimaal 12 maanden beschikbaar.		•	•	•
4.13.3	Activiteiten van *Gebruikers* binnen *Systemen* zijn herleidbaar tot een individu.	•	•	•	•
4.13.4	Er zijn maatregelen getroffen (zoals *IDS*, Intrusion Prevention System (IPS) en Security Information & Event Management (SIEM)) om afwijkingen van het normbeeld (anomalies) en ongebruikelijke creaties, aanwezigheid en/of beëindiging van processen te detecteren en te onderzoeken op dreigingen.	•	•	•	•
4.13.5	Op basis van vastgestelde drempelwaardes of use cases voor (gelogde) systeemactiviteiten wordt automatisch gealarmeerd.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.13.6	De capaciteit en *Beschikbaarheid* van een logserver wordt gemonitord, waarbij overschrijding van een grenswaarde leidt tot automatische alarmering.	•	•	•	•
4.13.7	Logbestanden worden alleen geraadpleegd door een daartoe geautoriseerde *Gebruiker*. De toegang is beperkt tot leesrechten.	•	•	•	•
4.13.8	Logbestanden zijn zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in een nieuw aangelegde log.	•	•	•	•
4.13.9	Loggegevens over een (vermoed) *Beveiligingsincident* worden zolang als nodig voor het onderzoek en de afhandeling van het *Beveiligingsincident* bewaard en op verzoek verstrekt aan *NBIV*.	•	•	•	•
4.13.10	Loggegevens waaruit *Bijzondere Informatie* of informatie over het *Te Beschermen Belang* is af te leiden, zijn beveiligd op hetzelfde beveiligingsniveau als het *Te Beschermen Belang* waarop zij betrekking hebben.	•	•	•	•
4.14	**Bedrijfscontinuïteit en herstel**				
4.14.1	Technische en procedurele maatregelen zijn getroffen en opgenomen in het *Beveiligingsplan* om het contractueel overeengekomen niveau van *Beschikbaarheid* (*RTO* en *RPO*) te waarborgen.	•	•	•	•
4.14.2	Er zijn voorzieningen ingesteld om voortdurend de *Beschikbaarheid* van de componenten die betrokken zijn bij de verwerking en opslag van *Bijzondere Informatie* te monitoren. Op basis van voorspellende analyses van het gebruik worden tijdig maatregelen genomen om de capaciteit indien nodig uit te breiden.	•	•	•	•
4.14.3	Er zijn beperkingen opgelegd aan *Gebruikers* en *Systemen* ten aanzien van het gebruik van gemeenschappelijke *Middelen*, zodat een enkele *Gebruiker* (of *Systeem*) de *Beschikbaarheid* van *Systemen* voor andere *Gebruikers* (of *Systemen*) niet in gevaar kan brengen.	•	•	•	•
4.14.4	Procedures voor back-up van *Bijzondere Informatie* en voor herinrichting en foutherstel van verwerkingen (recovery) zijn gedocumenteerd en worden minimaal elke 6 maanden getest. Deze procedures zijn gebaseerd op het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken (*RPO*) en de maximaal toelaatbare hersteltijd (*RTO*).	•	•	•	•
4.14.5	Back-upactiviteiten en de locatie van *Gegevensdragers* waarop de back-ups staan worden geregistreerd en beschreven in het *Beveiligingsplan*.	•	•	•	•
4.14.6	Back-ups worden bewaard op een locatie die zodanig is gekozen dat een *Beveiligingsincident* op de oorspronkelijke locatie niet leidt tot schade aan de back-ups.	•	•	•	•
4.14.7	Back-ups worden minimaal 1 jaar en maximaal voor de duur van de *Bijzondere Opdracht* bewaard. Bij beëindiging van de *Bijzondere Opdracht* worden deze vernietigd middels een door *NBIV* goedgekeurde procedure. Een bevestiging van vernietiging wordt opgesteld, gedeeld met *NBIV* en gearchiveerd conform formulier 'Bevestiging van vernietiging'.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.14.8	Back-ups worden behandeld conform hetzelfde beveiligings-niveau als het *Systeem* waarop de originele data staat.	•	•	•	•
4.15	**Ontwikkeling en acquisitie**				
4.15.1	Het (laten) ontwikkelen van software verloopt via een gedocumenteerde Secure Software Development Life Cycle (SSDLC) methodiek waarbij: • gebruik wordt gemaakt van een gestandaardiseerd proces (zoals een code repository) op basis van best practices; • ontwikkelaars bekend zijn met relevante secure coding practices; • secure development een expliciet onderdeel is van alle stappen in de methodiek; • zo veel mogelijk gebruik wordt gemaakt van software om fouten en kwetsbaarheden vroegtijdig te ondervangen.	•	•	•	•
4.15.2	Ontwikkel-, Test-, Acceptatie- en Productieomgevingen zijn logisch gescheiden. De *Systemen* en applicaties in deze omgevingen beïnvloeden *Systemen* en applicaties in andere omgevingen niet.	•			
4.15.3	Ontwikkel-, Test- en Acceptatieomgevingen zijn fysiek gescheiden van Productieomgevingen. De *Systemen* en applicaties in deze omgevingen beïnvloeden *Systemen* en applicaties in andere omgevingen niet.		•	•	•
4.15.4	Ontwikkel-, Test-, Acceptatie- en Productieomgevingen worden op hetzelfde *Rubriceringsniveau* beveiligd als de *Bijzondere Informatie.*	•	•	•	•
4.15.5	*Gebruikers* hebben gescheiden *Gebruiksaccounts* voor Ontwikkel-, Test-, Acceptatie- en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk *Systeem* gewerkt wordt.	•	•	•	•
4.15.6	Digitale experimenteer- of laboratoriumomgevingen zijn fysiek gescheiden van de andere omgevingen.	•	•	•	•
4.15.7	Overdracht tussen Ontwikkel-, Test-, Acceptatie- en Productie-omgeving vindt plaats conform een vastgestelde procedure. Deze procedure is door *NBIV* goedgekeurd.	•	•	•	•
4.15.8	Software wordt pas geïnstalleerd op een Productieomgeving nadat een formele test- en acceptatieprocedure is doorlopen.	•	•	•	•
4.15.9	Van acceptatietesten wordt een log bijgehouden.	•	•	•	•
4.15.10	Software wordt pas geïnstalleerd op een Productieomgeving als er een rollbackstrategie is geformuleerd en getest.	•	•	•	•
4.15.11	Binnenkomende software (zowel op fysieke media als gedown-load) is gecontroleerd op ongeautoriseerde wijzigingen (integriteitscontrole) aan de hand van een door de *(Toe)leverancier* via een gescheiden kanaal geleverde checksum, *Certificaat* of *Software Bill of Materials (SBOM).*	•	•	•	•
4.15.12	In de ontwerpfase van projecten als onderdeel van de *Bijzondere Opdracht* worden *Risicoanalyses* uitgevoerd en worden maatregelen gedefinieerd. Ook bij wijzigingen in het projectontwerp worden beveiligingsconsequenties meegenomen en gedocumenteerd. Jaarlijks en bij wijzigingen wordt gecontroleerd of de beveiligings-risico's en maatregelen nog actueel zijn.	•	•	•	•

Hoofdstuk 4: Cyber

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
4.15.13	De invoer van gegevens wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledigheid, format en inconsistentie.	●	●	●	●
4.15.14	Het *Systeem* bevat functies waarmee kan worden vastgesteld of gegevens correct (juist en volledig) verwerkt zijn.	●			
4.15.15	Het *Systeem* bevat een geautomatiseerde controle op transactie- en verwerkingsfouten waarmee vastgesteld kan worden of gegevens juist en volledig verwerkt zijn.		●	●	●
4.15.16	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen.	●	●	●	●
4.15.17	De beveiliging van *Systemen* wordt getest aan de hand van tevoren vastgestelde acceptatiecriteria.	●	●	●	●
4.15.18	Testgegevens en testaccounts worden verwijderd voordat *Systemen* en/of componenten in productie worden genomen.	●	●	●	●
4.15.19	Acceptatie van *Systemen* of software vindt plaats nadat vast-gesteld is dat de ABRO 2026 eisen zijn geïmplementeerd.	●	●	●	●
4.15.20	Bij het gebruik van *Externe Code Libraries* in het kader van de *Bijzondere Opdracht* heeft *Opdrachtnemer* de kwaliteit en integriteit onafhankelijk geverifieerd en de rapportage hiervan gedeeld met *Opdrachtgever*. Een *Software Bill of Materials* wordt op verzoek verstrekt aan *NBIV*.	●	●	●	●
4.15.21	Er zijn maatregelen getroffen om de *Broncode* welke is ontwikkeld of wordt gebruikt in het kader van de *Bijzondere Opdracht*, tegen onbedoelde wijzigingen te beschermen.	●	●	●	●
4.15.22	Alleen *Geautoriseerde medewerkers* hebben toegang tot de *Broncode*, wanneer deze is ontwikkeld of specifiek wordt gebruikt in het kader van een *Bijzondere Opdracht*.	●	●	●	●
4.15.23	*Broncode* ontwikkeld ten behoeve van de *Bijzondere Opdracht* wordt nooit opgeslagen door middel van een *Cloudoplossing*.	●	●	●	●

5. CLOUD

Inleiding

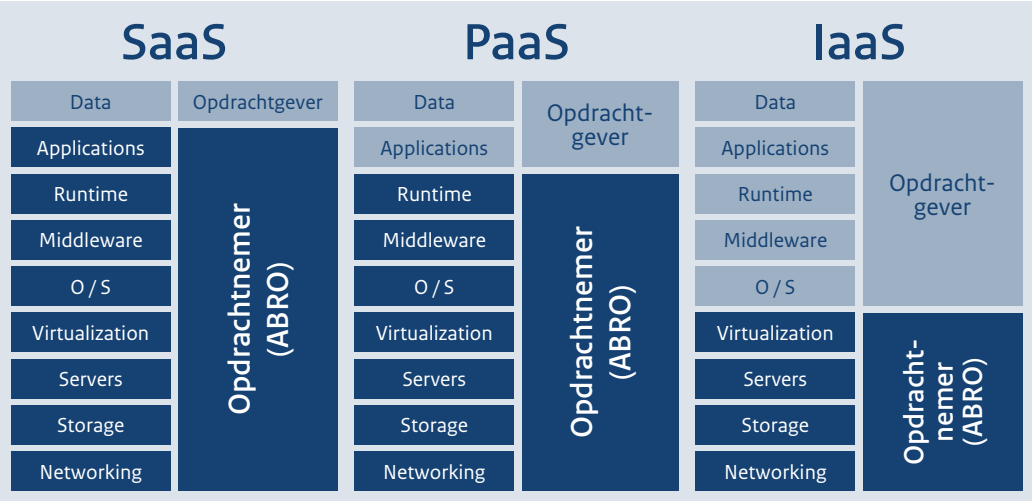
Om het gebruik van publieke *Cloudoplossingen* in het kader van *Bijzondere Opdrachten* te faciliteren zijn er specifieke beveiligingseisen gesteld. *Cloudoplossingen* kunnen enkel voor Departementaal VERTROUWELIJK (TBB 4) worden ingezet. Voor hoger gerubriceerde informatie (Stg. CONFIDENTIEEL tot en met Stg. ZEER GEHEIM) kan geen gebruikgemaakt worden van *Cloudoplossingen*.

Private Cloudoplossingen vallen niet binnen de reikwijdte van de *Cloudoplossingen* zoals bedoeld in dit hoofdstuk en worden behandeld als reguliere IT-oplossingen en dus beoordeeld op basis van hoofdstuk 4, *Cyber*.

Wanneer gebruik wordt gemaakt van *Cloudoplossingen* moeten zowel *Opdrachtgever* als de aanbieder van de *Cloudoplossing* – de *Cloud Service Provider (CSP)* beveiligingsmaatregelen treffen om de *Bijzondere Informatie* adequaat te beveiligen.

Type clouddiensten en toepassing ABRO 2026

De gestelde eisen zijn van toepassing op zowel *SaaS*, *PaaS* en *IaaS* diensten. Afhankelijk hiervan is *ABRO 2026* van toepassing op verschillende onderdelen van de *Cloudoplossing*. Wanneer *Opdrachtgever* een dienst direct *Uitbesteedt* aan een *CSP*, dan is *ABRO 2026* van toepassing op de onderdelen die onder de verantwoordelijkheid van *CSP* vallen. Voor de onderdelen die onder de verantwoordelijkheid van *Opdrachtgever* vallen, dienen op basis van het vigerende beleid de benodigde maatregelen te worden geïmplementeerd. Deze situatie is weergegeven in het onderstaande overzicht. Dit vereist heldere verantwoordelijkheden en nauwe samenwerking, zodat er een dekkende set aan maatregelen wordt gecreëerd. Wanneer *Opdrachtnemer* gebruik maakt van een *CSP* voor een *Bijzondere Opdracht* is voor zowel *Opdrachtnemer* als *CSP ABRO 2026* van toepassing.



Risicomanagement

Opdrachtgever heeft voorafgaand aan het gebruik van een *Cloudoplossing* in het kader van een *Bijzondere Opdracht* een *Risicoanalyse* uitgevoerd om inzichtelijk te krijgen welke risico's er zijn. In deze *Risicoanalyse* worden onder meer de betrouwbaarheidseisen, de ingeschatte dreigingen en de kosten en baten afgewogen. De uitkomst van de *Risicoanalyse* resulteert in een opdrachtspecifieke set aan eisen op basis van *ABRO 2026*, die *Opdrachtgever* vastlegt in de overeenkomst met *Opdrachtnemer.* Dit kan betekenen dat er in sommige gevallen een andere, alternatieve invulling aan een beveiligingseis wordt gegeven dan expliciet wordt voorgeschreven door *ABRO 2026*.

Uitgangspunt van de Cloudeisen

In de basis wordt gesteund op marktstandaarden en *Assuranceverklaringen* om vast te stellen of een *CSP* haar interne beheersing en beveiligingsmaatregelen op orde heeft. In aanvulling hierop zijn additionele eisen gesteld om specifieke risico's af te dekken en het gebruik van *Cloudoplossingen* in het kader van de nationale veiligheid mogelijk te maken.

Voorbeelden toepassing van ABRO 2026 op Cloudoplossing

Er zijn verschillende scenario's mogelijk waarin een *Cloudoplossing* en daarmee een *CSP* een rol speelt bij een *Bijzondere Opdracht.* Een *CSP* kan de 'primaire' *Opdrachtnemer* zijn en heeft dan een directe contractuele relatie met *Opdrachtgever.* Daarnaast komt het ook regelmatig voor dat een *Opdrachtnemer* een dienst levert waarbij (deels) gebruik wordt gemaakt van een *Cloudoplossing* die wordt geleverd door *CSP* als *Onderaannemer.* Per situatie zal moeten worden gekeken welke maatregelen van toepassing zijn en waar de verantwoordelijkheid voor het nemen van de maatregelen ligt. Onderstaand zijn twee voorbeelden toegelicht en samengevat in tabel 1.

1. Opdrachtnemer is een CSP

Wanneer de dienst die een *Opdrachtnemer* verstrekt een *Cloudoplossing* betreft en de *Opdrachtnemer* dus wordt beschouwd als een *CSP*, dan zijn de *Cloud*-specifieke beveiligingseisen leidend. Deze vervangen daarmee grotendeels de eisen die in hoofdstuk 3 en 4 worden gesteld. In deze situatie dient *Opdrachtnemer* te voldoen aan de eisen zoals gesteld in hoofdstuk 1, 2, 5 en een beperkt aantal eisen uit hoofdstuk 3 en 4. De eisen uit hoofdstuk 3 en 4 die ook van toepassing zijn op *Cloudoplossingen* zijn opgenomen in bijlage 11.

2. Onderaannemer is een CSP

Wanneer een *Opdrachtnemer* voor de dienstverlening gedeeltelijk steunt op een *Cloudoplossing* en daarbij gebruik maakt van een *CSP* als *Onderaannemer* dan gelden de Cloud-specifieke beveiligingseisen voor dat deel van de dienstverlening en gelden de reguliere beveiligingseisen voor *Opdrachtnemer*. In deze situatie geldt voor *Opdrachtnemer* hoofdstuk 1 tot en met 4 en voor de *CSP* als *Onderaannemer* hoofdstuk 1, 2, 5 en een beperkt aantal eisen uit hoofdstuk 3 en 4. De eisen uit hoofdstuk 3 en 4 die ook van toepassing zijn op *Cloudoplossingen* zijn opgenomen in bijlage 11.

Tabel 1 - Toepassing ABRO 2026 hoofdstukken bij Cloudoplossingen

	Opdrachtnemer is een CSP en levert primair een Cloudoplossing	**Opdrachtnemer is geen CSP,** maar gebruikt een CSP als Onderaannemer	**Onderaannemer is een CSP,** voor Onderaannemer gelden onderstaande hoofdstukken
H1 - Bestuur en Organisatie	√	√	√
H2 - Personeel	√	√	√
H3 - Fysiek	*	√	*
H4 – Cyber (exclusief Cloud)	*	√	*
H5 – Cloud	√	-	√

*Een beperkt aantal eisen uit hoofdstuk 3 en 4 zijn van toepassing

Wanneer een *CSP* als *Opdrachtnemer* of als *Onderaannemer* niet in staat is om aan de *Cloud*-specifieke beveiligingseisen te voldoen, dan wordt op basis van de in hoofdstuk 3 en 4 voorgeschreven eisen in afstemming met *Opdrachtgever* en *NBIV* bepaald hoe het benodigde beveiligingsniveau kan worden gerealiseerd.

Hoofdstuk 5: Cloud

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
5.1	**Algemeen**				
5.1.1	Het gebruik van een *Public Cloud*-dienst (computing, opslag, transport) is niet toegestaan.		•	•	•
5.1.2	Het gebruik van een *Public Cloud*-dienst (computing, opslag, transport) voor *Bijzondere Informatie* van de *NAVO*, *EU* of *ESA* is niet toegestaan zonder voorafgaande goedkeuring van *NBIV*.	•	•	•	•
5.1.3	*CSP* is niet gelieerd aan, niet gevestigd in, noch voert beheer-werkzaamheden uit in een land dat een *Offensief cyberprogramma* tegen Nederlandse belangen heeft.	•			
5.1.4	Data van *Opdrachtgever* (inclusief *Metadata* en telemetrie) blijven at-rest, in-transit en in-use binnen Nederland of, indien goed-gekeurd door *Opdrachtgever,* het grondgebied van de *Europese Economische Ruimte (EER)*.	•			
5.1.5	Beheer en onderhoud van de *Cloud*-dienst en -infrastructuur in het kader van de *Bijzondere Opdracht* vindt plaats binnen het grondge-bied van de *EER*.	•			
5.1.6	*Opdrachtnemer* voldoet aan de voor *Cloud*-diensten relevante eisen uit *ABRO* 2026 hoofdstuk 3 en 4 zoals vermeld in bijlage 11.	•			
5.2	**Governance**				
5.2.1	*Opdrachtnemer* heeft een *Risicoanalyse* uitgevoerd op het gebruik van de *Cloud*-dienst op basis van de resultaten van de door *Opdrachtgever* uitgevoerde *Risicoanalyse* en relevante dreigingen inclusief statelijke actoren. Deze *Risicoanalyse* is in afstemming met *NBIV* goedgekeurd door *Opdrachtgever* en opgenomen in het *Beveiligingsplan*.	•			
5.2.2	*CSP* beschikt gedurende de gehele contractperiode over een SOC2 type 2 verklaring op basis van alle trusted services criteria of een door *NBIV* als gelijkwaardig beoordeelde *Assuranceverklaring*, voor de volledige scope van de werkzaamheden. Deze verklaring is verstrekt aan *NBIV*.	•			
5.2.3	*CSP* heeft op basis van de meest recente *CSA Cloud Control Matrix (CCM)* maatregelen geïmplementeerd en kan opzet, bestaan en werking aantonen, of heeft op basis van een door *Opdrachtgever* goedgekeurde *Risicoanalyse* onderbouwd waarom een of meerdere controls niet van toepassing zijn. Dit is opgenomen in het *Beveiligingsplan*. Wijzigingen hierin worden direct gemeld bij *NBIV*.	•			
5.2.4	Wijzigingen in een voor de *Bijzondere Opdracht* relevante *Assurance-verklaring* of wijzigingen van maatregelen die raken aan de *CSA CCM* controls worden voorafgaand aan implementatie ter goedkeuring voorgelegd aan *NBIV*.	•			
5.2.5	*CSP* heeft een opdrachtspecifiek *Cloud*-beveiligingshoofdstuk opgenomen in het *Beveiligingsplan* waarin is vastgelegd: • hoe de *CSA CCM* controls geïmplementeerd zijn en waar eventuele afwijkingen zijn van de controls; • welke aanvullende maatregelen van toepassing zijn op basis van de *Risicoanalyse*. Aanvullende maatregelen zijn vastgesteld in afstemming met *NBIV* en goedgekeurd door *Opdrachtgever.*	•			

Hoofdstuk 5: Cloud

ABRO eis nr.	ABRO eis	TBB 4 / DV	TBB 3 / Stg. C	TBB 2 / Stg. G	TBB 1 / Stg. ZG
5.3	**Inrichten beveiligingsmaatregelen**				
5.3.1	*CSP* heeft een opdrachtspecifieke architectuur verstrekt aan *NBIV* waarin ten minste is gespecificeerd: • welke IT-services, functionaliteit en bedrijfsprocessen van toepassing zijn; • op welke locaties (ondersteunende) werkzaamheden, computing, opslag en transport plaatsvinden; • welke infrastructuur, netwerk- en systeemcomponenten worden gebruikt voor de ontwikkeling en de werking van de clouddienst(en); • of, en zo ja welke, IT-functies door de *CSP* zijn toegewezen of uitbesteed aan *(Toe)leveranciers*.	•			
5.3.2	De verdeling van rollen en verantwoordelijkheden tussen *CSP* en *Opdrachtgever* voor de implementatie en uitvoering van de beveiligingsmaatregelen die van toepassing zijn op de *Cloud*-dienst zijn vastgelegd in een *SLA* en *DAP*. Een afschrift hiervan is opgenomen in het *Beveiligingsplan*.	•			
5.3.3	*CSP* heeft op basis van de *Risicoanalyse*, indien van toepassing, in afstemming met *NBIV* additionele *Monitoring* en *Logging* ingeregeld, gericht op detectie van statelijke actoren.	•			
5.3.4	*CSP* richt de *Cloud*-dienst en -infrastructuur in volgens het concept *Secure by default*.	•			
5.4	**Cryptografie en sleutelbeheer**				
5.4.1	*CSP* ondersteunt sleutelbeheer dat volledig wordt uitgevoerd door *Opdrachtgever*, of ondersteunt dat *Opdrachtgever* op basis van een met *NBIV* afgestemde *Risicoanalyse* een derde partij met *ABRO-Verklaring* kan inschakelen, niet zijnde de *CSP*.	•			
5.4.2	Data van *Opdrachtgever* at-rest en in-transit is versleuteld conform de meest recente markstandaarden.	•			
5.5	**Compliance**				
5.5.1	*CSP* geeft volledige medewerking bij nalevingscontroles en onderzoeken in relatie tot de *Bijzondere Opdracht* door *Opdrachtgever* of *NBIV*, al dan niet uitgevoerd door een gecertificeerde derde partij.	•			
5.5.2	*CSP* heeft en verstrekt procedures voor de afhandeling van onderzoeksvragen van overheidsinstanties die toegang tot *Tenants* of gegevens van *Opdrachtgever* vereisen. De procedures omvatten minimaal: • verificatie van de rechtsgrond van de onderzoeksvraag; • naar vermogen *Opdrachtgever* en *NBIV* informeren over de onderzoeksvraag en betrekken bij de afhandeling ervan; • mogelijkheden voor *Opdrachtgever* om in beroep te gaan tegen de onderzoeksvraag.	•			
5.5.3	*CSP* heeft maatregelen getroffen en processen ingeregeld om invulling te geven aan de exit-strategie van *Opdrachtgever* en daaruit volgende bepalingen, zoals opgenomen in het contract met *Opdrachtgever*.	•			

6. AFKORTINGEN EN BEGRIPPEN

ABDO	Algemene Beveiligingseisen voor Defensieopdrachten. Voorschrift voor het adequaat beveiligen van *Te Beschermen Belangen* (waaronder *Bijzondere Informatie*) die aan een *Leverancier* buiten Defensie zijn of worden toevertrouwd. *ABDO* stelt, in het kader van nationale veiligheid, eisen aan de *Betrouwbaarheid* van een *Opdrachtnemer* op het gebied van mensen, processen, *Middelen* en organisatie om de *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid* (ook wel Exclusiviteit) van *Te Beschermen Belangen* te waarborgen.
ABRO	Algemene Beveiligingseisen voor Rijksoverheidsopdrachten. Voorschrift voor het adequaat beveiligen van *Te Beschermen Belangen* (waaronder *Bijzondere Informatie*) die aan een *Leverancier* buiten de *Rijksoverheid* zijn of worden toevertrouwd. ABRO 2026 stelt, in het kader van nationale veiligheid, eisen aan de *Betrouwbaarheid* van een *Opdrachtnemer* op het gebied van mensen, processen, *Middelen* en organisatie om de *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid* (ook wel Exclusiviteit) van *Te Beschermen Belangen* te waarborgen. Het betreft een doorontwikkeling van *ABDO*.
ABRO-Verklaring	De formele verklaring dat op basis van het oordeel van *NBIV* de *Opdrachtnemer* voldoet aan door *ABRO 2026* voorgeschreven beveiligingseisen voor de betreffende *Bijzondere Opdracht*. Een *ABRO-Verklaring* is alleen van toepassing op de *Bijzondere Opdracht* waarvoor deze is afgegeven. In het geval een aanvraag vanuit een buitenlandse *Opdrachtgever* komt of gericht is op een buitenlandse *Opdrachtnemer*, wordt gesproken van een *Facility Security Clearance (FSC)* in plaats van een *ABRO-Verklaring*.
Access-to-site	Een type *ABRO-Verklaring* waarbij medewerkers van een *Opdrachtnemer* frequent toegang moet worden verleend tot een locatie, *Compartiment* of *Systeem* van *Opdrachtgever* waar zich al dan niet een *Te Beschermen Belang* bevinden.
AI systemen	Artificial Intelligence systemen. *Systemen* met het vermogen om een complex doel te bereiken door middel van flexibele aanpassing aan de omgeving. Dit betreft onder andere Large Language Models en Machine Learning. Hierbij is een *Systeem* in staat om automatisch te leren en te verbeteren op basis van ervaring of data zonder hiervoor expliciet geprogrammeerd te zijn (ook bekend als kunstmatige intelligentie).
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
Assuranceverklaring(en)	Een formele verklaring afgegeven door een onafhankelijke auditor of accountant, waarin wordt bevestigd dat bepaalde informatie betrouwbaar is.
Authenticatie	Het proces waarmee de identiteit van een *Gebruiker*, *Systeem* of entiteit wordt geverifieerd.
Authenticatiegegevens	Informatie die wordt gebruikt om een *Gebruiker*, *Systeem* of entiteit te *Authenticeren* en toegang te verlenen tot beveiligde *Systemen* of gegevens.
Autorisatie(s)	De bevoegdheden van een *Gebruiker*, account, *Systeem* of softwarematig proces om toegang tot een digitaal of fysiek *Middel*, locatie, informatie, data of *Systeem* en al dan niet bepaalde handeling uit te voeren. In het fysieke domein betreft dit de toegang van een persoon tot een *Compartiment*. In het digitale domein kan dat gaan om *Autorisaties* die zijn gekoppelde aan een account voor een natuurlijk persoon, maar bijvoorbeeld ook een softwarematig proces waarbij de *Autorisaties* zijn gekoppeld aan een *Serviceaccount*.
BAC	Bedrijfsalarmcentrale. Een meldkamer in het beheer van *Opdrachtnemer* waar de signalen bij alarmering worden ontvangen vanuit het *IDSS* en andere detectiesystemen en van waaruit alarmopvolging wordt georganiseerd en gecoördineerd.

Bedrijfsmiddel	Elk *Middel* waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt of waarmee toegang tot gebouwen, ruimten en *ICT-bedrijfsmiddelen* kan worden verkregen. Dit kan zijn in de vorm van een apparaat, een *ICT-bedrijfsmiddel* of een gedefinieerde groep gegevens.
Beheer op afstand	Het uitvoeren van beheerwerkzaamheden vanaf een werkstation of *Mobiel Apparaat* dat via een externe netwerkverbinding verbinding maakt met de lokale IT-infrastructuur die is ingericht ten behoeve van een *Bijzondere Opdracht*.
Beheerder	Een *Gebruiker* die verantwoordelijk is voor het configureren, beheren en onderhouden van *Systemen*, applicaties of netwerkcomponenten. Een *Beheerder* heeft doorgaans uitgebreide *Rechten* en bevoegdheden om instellingen aan te passen, *Gebruikersaccounts* te beheren, toegangsrechten toe te wijzen en beveiligingsmaatregelen te implementeren.
Beheerdersaccount	Een *Gebruikersaccount* met uitgebreide of volledige toegangsrechten tot *Systemen*, applicaties of *Netwerken*. Dit account wordt gebruikt door *Beheerders* om beheer- en configuratiewerkzaamheden uit te voeren, zoals het aanmaken en verwijderen van *Gebruikersaccounts*, het aanpassen van *Rechten*, en het configureren van beveiligingsinstellingen.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde *Gebruikers* of *Systemen* op de juiste momenten tijdig toegang hebben tot informatie en aanverwante *Bedrijfsmiddelen*.
Betrokken Medewerker(s)	Medewerkers in loondienst van *Opdrachtnemer*, dan wel extern ingehuurd door *Opdrachtnemer*, die werkzaamheden uitvoeren in het kader van een *Bijzondere Opdracht*.
Betrouwbaarheid	Het geheel van *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid* (ook wel Exclusiviteit).
Betrouwbaarheids-onderzoek (BO en BO+)	Een onderzoek door de Politie krachtens de Politiewet art. 49 q en het besluit screening ambtenaren van politie en politie-externen waarbij de achtergrond, Integriteit en geschiktheid van (toekomstige) politiefunctionarissen worden onderzocht om te waarborgen dat zij voldoen aan de ethische en professionele normen die vereist zijn voor de uitoefening van hun taken. Dit onderzoek kan onder andere bestaan uit antecedentenonderzoek, veiligheidschecks en interviews. Er zijn twee typen onderzoek, het Betrouwbaarheidsonderzoek (BO) en het Betrouwbaarheids- en Omgevingsonderzoek (BO+).
Beveiligingsfunctionaris	Een medewerker in loondienst bij *Opdrachtnemer* die door *Opdrachtnemer* bij *NBIV* is aangedragen als *Beveiligingsfunctionaris*. Na goedkeuring wordt de *Beveiligingsfunctionaris* benoemd door *NBIV*. De *Beveiligingsfunctionaris*, of diens vervanger, is verantwoordelijk voor de implementatie, uitvoering en toezicht op naleving van de voorgeschreven beveiligingsmaatregelen. De *Beveiligingsfunctionaris* is de contactpersoon voor *NBIV*.
Beveiligingsincident	Een gebeurtenis die kan leiden of heeft geleid tot een verstoring van de normale gang van zaken aangaande de integrale beveiliging van een *Te Beschermen Belang*, als gevolg waarvan de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries in gevaar gebracht zijn of kunnen worden.
Beveiligingspersoneel	Personen die verantwoordelijk zijn voor het handhaven van de beveiliging bij *Opdrachtnemer*. Het kan zowel gaan om intern personeel als externe ingehuurd *Beveiligingspersoneel*.
Beveiligingsplan	Beschrijving op welke wijze de beveiliging van een *Bijzondere Opdracht* en een *Te Beschermen Belang* wordt uitgevoerd op basis van de in *ABRO 2026* gestelde richtlijnen voor het opstellen van een *Beveiligingsplan*.

Beveiligingsrendement	In het kader van fysieke beveiliging betreft dit het tijdvak waarbinnen een niet-geautoriseerd persoon kennis kan nemen van, of toegang heeft tot, *een Te Beschermen Belang*. Het *Beveiligingsrendement* is afhankelijk van het vertragende effect van getroffen beveiligingsmaatregelen in het fysieke domein (*Uitsteltijd*) in relatie tot de *Interventietijd*. Er is sprake van een positief *Beveiligingsrendement* wanneer de *Uitsteltijd* langer is dan de *Interventietijd*. In dit geval zal *Interventie* voorkomen dat er *Compromittatie* plaatsvindt. Er is sprake van een negatief *Beveiligingsrendement* wanneer de *Uitsteltijd* korter is dan de *Interventietijd*. In dit geval kan *Interventie* pas plaatsvinden na *Compromittatie* en zorgt *Interventie* ervoor dat het tijdvak waarbinnen de *Compromittatie* plaatsvindt zo kort mogelijk is.
Beveiligingssystemen	*Systemen* die als primaire functie hebben het detecteren of controleren van toegang tot een *Compartiment* of een *Te Beschermen Belang*.
Beveiligingsverdrag	Een multi- of bilateraal verdrag dat de uitwisseling en wederzijdse beveiliging van *Bijzondere Informatie* tussen twee of meer landen faciliteert, ook wel General Security Agreement (GSA).
Beveiligingsverlichting	Een vorm van (buiten)verlichting die is ontworpen om de veiligheid te verbeteren en criminaliteit te ontmoedigen. Het heeft als doel om gebieden ‘s nachts goed verlicht te houden, zodat potentiële dreigingen of indringers gemakkelijker kunnen worden opgemerkt.
Bezoeker	Een niet-geautoriseerde persoon die, op basis van het *Need-to-Know* en *Need-to-Be* onder begeleiding van een *Geautoriseerde Medewerker* toegang heeft tot een *Compartiment.*
Bijzondere Informatie	Informatie waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries. *Bijzondere Informatie* is informatie die voorzien is van een *Rubricering* en overeenkomstig moet worden beveiligd. *Bijzondere Informatie* valt, afhankelijk van het *Rubriceringsniveau* in een *TBB*-categorie. *Bijzondere Informatie* is altijd een *Te Beschermen Belang*, maar een *Te Beschermen Belang* is niet altijd gerubriceerd.
Bijzondere Opdracht	Een overheidsopdracht die raakt aan de nationale veiligheid, verstrekt aan een civiele partij als *Opdrachtnemer* waarbij een *Te Beschermen Belang* betrokken is.
Biometrie	Methode om een *Gebruiker* te *Authenticeren* op basis van biologische metingen of lichamelijke kenmerken. Denk aan een vingerafdruk of irisscan.
Broncode	De leesbare tekst die een programmeur heeft geschreven in een programmeertaal. Er bestaan verschillende programmeertalen, zoals C, C++ en Pascal. De *Broncode* wordt door een compiler omgezet naar een voor computer uitvoerbare machine code.
Buitengewone bevoegdheden of toegangsrechten	Speciale *Rechten* of privileges (zowel fysiek als logisch) die aan bepaalde medewerkers of systemen worden toegekend, waardoor zij acties kunnen uitvoeren die buiten de normale autorisatiegrenzen liggen. Deze bevoegdheden zijn vaak noodzakelijk voor systeembeheer, onderhoud, of voor specifieke rollen binnen een organisatie. Misbruik van de *Buitengewone Bevoegdheden* of *Toegangsrechten* zorgt veelal voor een verhoogde kans op *Compromittatie* en vereist daarom additionele of specifieke maatregelen.
Buitenlandse partner	Een buitenlands equivalent van *NBIV* dat namens het betreffende land toezicht houdt op de industrieveiligheid in het betreffende land.
CCM	Cloud Control Matrix. Een raamwerk van beveiligingscontroles die zijn ontworpen om fundamentele beveiligingsprincipes te waarborgen in *Cloudoplossingen.*

Certificaat	Een verklaring van een onafhankelijke instantie waarin staat dat een product, proces of persoon voldoet aan de eisen in het *Certificaat*. In een digitale context betreft het een digitaal document dat de identiteit van een *Gebruiker*, *Systeem* of entiteit aantoont. Dit kan bijvoorbeeld worden gebruikt om een beveiligde verbinding tot stand te brengen. Een erkende instantie (Certificate Authority) geeft het document uit.
Chemisch verankerd	Een bevestigingstechniek waarbij chemische mortels gebruikt worden om beveiligingsmiddelen stevig in materiaal als beton of metselwerk te verankeren.
Clear Desk	Het uitgangspunt dat er geen gevoelige informatie op een werkplek ligt.
Clear Screen	Het uitgangspunt dat bij het verlaten van het werkstation de *Gebruiker* het werkstation vergrendelt.
Cloud(oplossing)	Een model voor het mogelijk maken van on-demand netwerktoegang tot een gedeelde pool van configureerbare computerbronnen (bijvoorbeeld *Netwerken*, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven. Hierbij wordt onderscheid gemaakt tussen *SaaS*, *PaaS* en *IaaS*.
Compact Te Beschermen Belang	*Te Beschermen Belang* dat redelijkerwijs fysiek opgeborgen kunnen worden in een afsluitbaar *Opbergmiddel*, zoals een laptop.
Compartiment	Een aangewezen en beveiligde, afgescheiden, afsluitbare, fysieke ruimte waar een *Te Beschermen Belang* wordt verwerkt of opgeslagen. Het kan hierbij gaan om een ruimte met verschillende afmetingen, zoals een kamer, etage, gebouw, zeecontainer, fabriekshal of een terrein.
Compromittatie	Kennisname van of toegang tot een *Te Beschermen Belang* door niet-geautoriseerden, dan wel het verlies van een *Te Beschermen belang*, waarbij vastgesteld is of redelijkerwijs aan te nemen valt dat de *Beschikbaarheid*, *Integriteit* of *Vertrouwelijkheid* van een *Te Beschermen Belang* is aangetast.
Cryptobeheerder	Een *Vertrouwensfunctie* waarbij de betreffende medewerker verantwoordelijk is voor het verwerken, administreren, en beheren van *Cryptografische beveiligingsoplossingen*.
Cryptografische beveiligingsoplossingen	Hardware of software (inclusief fysieke en digitale sleutels) die gebruikmaakt van encryptie om de *Vertrouwelijkheid* en *Integriteit* van informatie, zowel in-rest als in-transit, te waarborgen.
CSA	Cloud Security Alliance. Een organisatie die zich richt op het ontwikkelen en bevorderen van best practices voor beveiliging in *Cloud* computing en het bieden van educatieve bronnen voor organisaties.
CSC	Cloud Service Consumer. Een afnemer of *Gebruiker* van cloudservices die worden geleverd door een *Cloud Service Provider*.
CSP	Cloud Service Provider. Een bedrijf dat cloudgebaseerde platformen, infrastructuur, applicaties of opslagdiensten levert aan andere organisaties of individuen via een netwerkverbinding.
CVSS	Common Vulnerability Scoring System
Cyber	Een voorvoegsel om zaken aan te duiden die te maken hebben met computers, netwerken en de digitale wereld (zoals: cybercrime, cybersecurity, cyberdreiging).
Cyber-Beveiligingsfunctionaris	Een specifieke *Beveiligingsfunctionaris* met verantwoordelijkheden gerelateerd aan, en expertise op het gebied van, cybersecurity en informatiebeveiliging die een *Beveiligingsfunctionaris* kan ondersteunen bij specifieke *Cyber*-gerelateerde vraagstukken.

DAP	Dossier, Afspraken en Procedures of Document, Agreements and Procedures. Een type overeenkomst waarin de wederzijds overeengekomen samenwerking tussen klant en leverancier zijn vastgelegd rondom een afgenomen dienst of product. Een *DAP* kan als afspraak bestaan tussen zowel interne (klant) als externe (leverancier) partijen binnen een organisatie. Een *DAP* is hiërarchisch ondergeschikt aan de Service Level Agreement (*SLA*) en betreft naast andere servicedocumentatie, een bijlage bij de algemene hoofdovereenkomst.
DMZ	Demilitarized Zone. Een fysiek of logisch deel van een *Netwerk* dat de extern (vanuit een ander onvertrouwd *Netwerk* of internet) te benaderen services van een organisatie bevat, zodat interne services en werkstations niet rechtstreeks te benaderen zijn (bijvoorbeeld mail- en webservers).
DNS	Domain Name System. Een systeem dat internetdomeinnamen koppelt aan *IP-adressen* en omgekeerd.
DoS/DDoS	(Distributed) Denial of Service. Het onbruikbaar maken van een computer, computernetwerk of dienst door overbelasting van de bandbreedte, geheugen- of verwerkingscapaciteit. Bij een *DDoS*-aanval wordt de aanval uitgevoerd door een verzameling computers of andere apparaten die tegelijk proberen om een computer(netwerk) of dienstverlening uit te schakelen, waarbij deze aanval centraal gecoördineerd wordt, vaak via een botnet.
Draadloze communicatie	Een methode voor het verzenden van informatie tussen twee of meer punten door middel van elektromagnetische golven. Voorbeelden zijn middels Bluetooth, Wifi en 5G.
DSA	Designated Security Authority
EER	Europese Economische Ruimte. Het grondgebied bestaande uit de *EU*-lidstaten en Noorwegen, Liechtenstein en IJsland, óf grondgebied van het Verenigd Koninkrijk of Zwitserland.
Elektronisch Veiligheidsonderzoek	Onderzoek naar de potentiële aanwezigheid van ongewenste apparatuur in een *Compartiment*, ook wel afgekort als EVO.
ESA	European Space Agency
Escrow Agent	Een derde partij waar digitale sleutels of *Broncode* wordt opgeslagen.
ETS	Elektronisch Toegangsbeheer Systeem
EU	Europese Unie
Externe (netwerk)koppeling	Een *Externe koppeling* is een verbinding of interface tussen een *Vertrouwd Systeem* of *Netwerk* en een onvertrouwd *Systeem* of *Netwerk*.
Externe Code Libraries	Verzamelingen van herbruikbare code, ontwikkeld door derden buiten eigen ontwikkelteams, die kunnen worden geïmporteerd en gebruikt binnen een softwareproject om bepaalde functies en mogelijkheden te implementeren.
FSC	Facility Security Clearance. De verklaring van het *NBIV* aan een (doorgaans buitenlandse) aanvrager dat een bedrijf vanuit beveiligingsoptiek in staat is een *Bijzondere Opdracht* uit te voeren.

Fysieke toegangsauthenticatie-middelen	Alle vormen van (reserve) sleutels, passen, elektronische sleutels of andere fysieke objecten waarmee toegang kan worden verschaft tot een *Compartiment* of *Opbergmiddel*.
GBS	Gebouwbeheersysteem. Een geïntegreerd systeem dat het beheer en de controle van de technische installaties en diensten in een gebouw centraliseert en automatiseert.
Geautoriseerde Medewerker(s)	Medewerkers in loondienst van *Opdrachtnemer*, dan wel extern ingehuurd door *Opdrachtnemer*, die toestemming van *Opdrachtnemer* hebben om kennis te nemen van, of toegang te hebben tot een *Te Beschermen Belang*.
Gebruiker	Een *Geautoriseerde Medewerker* die toegang heeft tot (informatie)*Systemen* om zijn of haar taken uit te voeren. *Gebruikers* hebben beperkte toegangsrechten die alleen de benodigde toegang bieden om hun functie uit te oefenen, in lijn met het principe van 'least privilege'.
Gebruikersaccount	Een individueel inlogaccount die aan een individu is toegekend om toegang te krijgen tot *Systemen*, applicaties of informatiebronnen om zijn of haar werkzaamheden uit te voeren. *Gebruikersaccounts* hebben beperkte *Rechten*, afgestemd op de taken van een specifieke *Gebruiker*, in lijn met het principe van 'least privilege'.
Gegevensdragers	Fysieke *Middelen*, zoals een CD, tape, harde schijf of USB stick waarop informatie kan worden opgeslagen.
Geheimhoudingsverklaring	Een juridisch bindende verklaring waarin is vastgelegd dat bepaalde informatie niet kenbaar wordt gemaakt aan niet-geautoriseerde personen.
Geluidsdempingsmeting	Een controle om vast te stellen of het geluid voldoende wordt gedempt voor het betreffende beveiligingsniveau. Dit is onderdeel van het *Elektronische Veiligheidsonderzoek*.
Goedgekeurde Middelen	Software en hardware die geschikt is bevonden om in te zetten voor de beoogde functionaliteit in het kader van een *Bijzondere Opdracht*. Goedkeuring wordt, afhankelijk van de beoogde inzet en de *Opdrachtgever*, gegeven door verschillende instantie. Zie ook bijlage 9. Hierbij verloopt het aanvragen en afgeven van de goedkeuring via *NBIV*.
Hardening	Het proces van uitschakelen of verwijderen van ongebruikte functies in hardware en software en de rechten van andere functies waar mogelijk beperken met als doel het aanvalsoppervlak en daarmee het risico van aanvallen te beperken.
Hardware token	Een fysiek *Middel* met veelal een cryptografische module waarmee de authenticiteit van de *Gebruiker* vastgesteld kan worden. Bijvoorbeeld voor *Multi-factor authenticatie*.
Hoogste bestuursorgaan	Het hoogste orgaan binnen een organisatie, instelling of overheidsentiteit die verantwoordelijk is voor het nemen van strategische beslissingen en het bepalen van het algemene beleid. Dit orgaan heeft de ultieme zeggenschap over de richting en het beheer van de organisatie en is vaak belast met toezicht, goedkeuring van budgetten, naleving van wettelijke vereisten, en het waarborgen van de belangen van belanghebbenden.
HSM	Hardware Security Module. Een fysiek apparaat voor het beheren en genereren van digitale sleutels en het uitvoeren van cryptografische verwerkingen met maatregelen om (onopgemerkte) fysieke en niet fysieke manipulatie te voorkomen.
IaaS	Infrastructure as a Service. Een dienst geleverd aan een CSC waarbij verwerking, opslag, *Netwerken* en andere fundamentele dataverwerkings- en opslagcapaciteit wordt geleverd. Hierop kan de CSC willekeurige software installeren en uitvoeren, zoals besturingssystemen en applicaties. De CSC heeft geen directe controle over, noch beheert de CSC de onderliggende cloudinfrastructuur, maar heeft wel controle over besturingssystemen, opslag, geïnstalleerde software en mogelijk beperkte controle over bepaalde netwerkcomponenten.

ICT-bedrijfsmiddel(en)	Een (fysiek of logisch) technisch *Middel* (zoals hardware, software, applicatie of faciliteit) waarmee een IT-dienst, geheel of gedeeltelijk en direct of indirect, wordt gerealiseerd of gebruikt.
IDS	Intrusion Detection System. Een *Systeem* dat *Netwerk*- en systeemactiviteiten analyseert met als doel het detecteren en alarmeren in het geval van pogingen tot het verkrijgen van ongeautoriseerde toegang tot digitale *Systemen* of informatie.
IDSS	Indringer Detectie en Signalering Systeem. Een *Systeem* dat gebruikt wordt om de ongeautoriseerde fysieke toegang tot een ruimte te signaleren en te alarmeren.
Incident Response Procedure	Een procedure waarin is opgenomen welke stappen in onderzoek en afhandeling moeten worden uitgevoerd als een *Beveiligingsincident* wordt gedetecteerd.
Integriteit	Het waarborgen van de juistheid, volledigheid en actualiteit van informatie en de verwerking ervan.
Internationale Netwerkkoppeling	Koppelingen naar *Netwerken* van bijvoorbeeld buitenlandse overheden, *NAVO*, *EU* of *ESA* die ingericht zijn om internationale *Bijzondere Informatie* uit te wisselen.
Interventie	De reactie naar aanleiding van een alarmering (vermoeden van poging tot *Compromittatie* van het *Te Beschermen Belang*) met als doel de alarmering te verifiëren en indien nodig de *Compromittatie* te stoppen dan wel het *Te Beschermen Belang* veilig te stellen. Het betreft daarom het geheel van maatregelen en/of activiteiten met als doel om *Compromittatie* van een *Te Beschermen Belang* te voorkomen en het beveiligingsniveau te herstellen. Interventie dient plaats te vinden door daartoe opgeleide en *Geautoriseerde* personen, waarbij de *Need-to-Know* en *Need-to-Be* principes gehandhaafd blijven.
Interventietijd	De tijd tussen detectie/verificatie van een poging tot *Compromittatie* en het ter plaatse ingrijpen door medewerkers, het *Beveiligingspersoneel* of de politie.
IP-adres	Internet Protocol-adres. Een *IP-adres* is een op dat *Netwerk*, uniek identificatienummer dat aan elk apparaat op een *Netwerk* wordt toegekend dat gebruikmaakt van het Internet Protocol om te communiceren.
JSCU Logging-essentials	Richtlijnen van de Joint Sigint Cyber Unit (JSCU) van de *AIVD* en *MIVD* voor inrichten van *Logging*, zoals gepubliceerd op de github van de Joint Sigint Cyber Unit.
Koppelvlak	Een verbinding tussen twee of meerdere *Netwerken* of *Systemen* waarbij informatie, al dan niet van een verschillend *Rubriceringsniveau*, kan worden uitgewisseld.
KVM-switch	Een apparaat dat *Gebruikers* in staat stelt om meerdere *Systemen* te beheren en bedienen met één toetsenbord, monitor en muis.
(Toe)leverancier	Een individu of organisatie die goederen, materialen of diensten levert aan een andere entiteit.
Logging	Het vastleggen van gegevens die betrekking hebben op (pogingen tot) de toegang tot of activiteiten die raken aan een *Te Beschermen Belang*, zowel fysiek als digitaal.
Malware	Software met ongewenste/kwaadaardige functies, zoals virussen en trojans.
Melding	Het officieel rapporteren of doorgeven van een gebeurtenis, situatie, of bevinding aan een bevoegde persoon of instantie. Dit kan betrekking hebben op uiteenlopende zaken zoals *Beveiligingsincidenten*, klachten, problemen, of andere relevante informatie die actie of aandacht vereist. Het doel van een *Melding* is om de verantwoordelijke partij op de hoogte te stellen zodat zij passende maatregelen kunnen nemen.

Merking	Aanduiding op informatie die een bepaalde wijze van behandelen en beperking van verspreiding inhoudt. Indien vastgesteld door *Opdrachtgever* wordt gemerkte informatie behandelt conform de vastgestelde *TBB*-categorie.
Metadata	Gegevens die de eigenschappen van andere gegevens beschrijven. Bijvoorbeeld van wie de gegevens zijn, wie ze verstuurd heeft, of wanneer ze voor het laatst gewijzigd zijn.
Middel(en)	Apparatuur, software, hardware, netwerkbekabeling en andere technologie die informatie verwerken of communiceren.
Mitigeren	Het minimaliseren van het risico op (digitale) *Compromittatie* door middel van beveiligingsmaatregelen of het minimaliseren van het effect van een (digitale) *Compromittatie* door middel van *Interventie(s)*.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
Mobiele apparatuur	Draagbare elektronische apparaten zoals smartphones, tablets, laptops die toegang geven tot *Bijzondere Informatie* of deze genereren, verwerken of opslaan.
Monitoring	Het continu in de gaten houden van (fysieke) omgevingen, *Netwerken* en *Systemen* om afwijkende activiteiten en (potentiële) poging tot *Compromittatie* te detecteren.
MoU	Memorandum of Understanding. Een bilateraal verdrag waarin beveiligingsafspraken worden gemaakt. Bijvoorbeeld over de wederzijds erkenning van *VGB* en het equivalent van het betreffende andere land.
Multi-factor authenticatie	Een beveiligingsmaatregel die meerdere factoren vereist om de identiteit van een *Gebruiker* vast te stellen voordat toegang kan worden verleend tot een *Systeem* of *Compartiment*.
NAVO	Noord Atlantische Verdragsorganisatie
NBIV	Nationaal Bureau Industrieveiligheid. De uitvoeringsorganisatie die is belast met het bevorderen van maatregelen ten aanzien van de beveiliging van gegevens en materiaal die de nationale veiligheid raken. *NBIV* biedt in dit kader ondersteuning aan *Opdrachtgever* bij het toezien op de naleving van *ABRO 2026* met betrekking tot *Bijzondere Opdrachten*, geïnitieerd door *Opdrachtgever(s)*.
Need-to-Be	Het uitgangspunt dat een persoon alleen fysieke of digitale toegang heeft tot een omgeving wanneer dit noodzakelijk is voor de uitvoering zijn of haar werkzaamheden.
Need-to-Know	Het uitgangspunt dat een persoon alleen kennis neemt van of toegang heeft tot bepaalde informatie wanneer dit noodzakelijk is voor de uitvoering zijn of haar werkzaamheden.
Need-to-Use	Het uitgangspunt dat een persoon alleen fysiek of digitaal gebruik kan maken van *Middelen* of informatie wanneer dit noodzakelijk is voor de uitvoering zijn of haar werkzaamheden.
Netwerk	Een samenstelling van onderling verbonden *Systemen*, apparaten, en andere componenten die communiceren en gegevens uitwisselen.
Netwerkapparatuur	Elektronische apparatuur die met behulp van bekabeling of draadloze verbindingen een *Netwerk* tot stand brengen, zoals een switch of een firewall.
Noodvernietigingsplan	Onderdeel van het *Beveiligingsplan* waarin heldere procedures en instructies zijn beschreven voor noodvernietiging van een *Te Beschermen Belang*. Van noodvernietiging is enkel sprake in buitengewone omstandigheden, waarbij de staatsveiligheid in gevaar is. In zulke gevallen wordt afgeweken van de voorgeschreven vernietigingsprocedures.

Offensief cyberprogramma	De vanuit een overheid georganiseerde of gestimuleerde inzet van cyberaanvallen om haar eigen belangen te dienen. Het betreft hier onder andere landen die als zodanig zijn genoemd in de meest recente jaarverslagen van de *MIVD* en de *AIVD*.
Onderaannemer	Een *Leverancier* waaraan *Opdrachtnemer* bepaalde werkzaamheden in het kader van de *Bijzondere Opdracht* heeft uitbesteed, waarbij de betreffende *Leverancier* toegang krijgt tot of kennis kan nemen van een *Te Beschermen Belang*. Ook wanneer een *Leverancier* niet direct toegang krijgt tot of kennis kan nemen van een *Te Beschermen Belang*, maar wel een cruciale rol vervult in het kader van een *Bijzondere Opdracht*, kan deze worden aangemerkt als *Onderaannemer.*
Onderhoud op afstand	Het uitvoeren van onderhoudswerkzaamheden vanaf een werkstation of *Mobiel apparaat* dat via een extern *Netwerk* verbinding maakt de lokale IT-Infrastructuur die is ingericht ten behoeve van een *Bijzondere Opdracht*.
Opbergmiddel	Een object ontworpen voor het veilig en georganiseerd bewaren van materialen of documenten met passende beveiligingsmaatregelen conform relevante NEN-standaarden, zoals een kluis.
Opdrachtgever	Het ministerie, agentschap, Politie die *Opdrachtnemer* inhuurt voor het uitvoeren van een *Bijzondere Opdracht.* Het kan tevens gaan om een buitenlandse overheidsorganisatie of internationale organisatie waar een internationaal verdrag aan ten grondslag ligt. Bij de toepassing van *ABRO* 2026 op een *Onderaannemer* waarbij het beoogde beveiligingsdoel van een eis betrekking heeft op de samenwerking tussen *Opdrachtnemer* en *Onderaannemer* in het kader van de *Bijzondere Opdracht* geldt dat voor de term *Opdrachtgever* de *Opdrachtnemer* verondersteld wordt.
Opdrachtnemer	Het bedrijf of organisatie dat als leverancier is geselecteerd is om een gevraagde dienst of goederen te leveren in het kader van een *Bijzondere Opdracht.* Bij de toepassing van *ABRO* 2026 op een *Onderaannemer* waarbij het beoogde beveiligingsdoel van een eis betrekking heeft op de samenwerking tussen *Opdrachtnemer* en *Onderaannemer* in het kader van de *Bijzondere Opdracht* geldt dat voor de term *Opdrachtnemer* de *Onderaannemer* verondersteld wordt.
Opnamen	Een op een medium vastgelegde representatie van een situatie of object op basis van akoestische, visuele of andere soorten signalen.
OSI Model-lagen	Het OSI-model (Open Systems Interconnection) is een ISO gestandaardiseerd referentiemodel om de communicatie tussen systemen te categoriseren. Lagen 2, 3 en 4 verwijzen respectievelijk naar de Datalink-, Netwerk- en Transportlaag.
PaaS	Platform as a Service. Een dienst geleverd aan een *CSC* waarbij een door de *CSC* gecreëerde of verworven applicatie is geïnstalleerd op de cloudinfrastructuur van de *CSP* met behulp van programmeertalen, code libraries, en applicaties die ondersteund worden door de *CSP.* De *CSC* heeft geen directe controle over, noch beheert de *CSC* de onderliggende cloudinfrastructuur, inclusief *Netwerk*, server, besturingssysteem, opslag, maar heeft wel controle over de geïnstalleerde applicatie en mogelijk de configuratie instellingen van de applicatie-hostingomgeving.
PAC	Particuliere Alarm Centrale. Een meldkamer van een derde partij waar de signalen bij alarmering worden ontvangen vanuit het *IDSS* en andere detectiesystemen en van waaruit alarmopvolging wordt georganiseerd en gecoördineerd.
PAM	Privileged Access Management. Een beveiligingsmethode en technologie die gericht is op het beheren en controleren van toegang tot *Systemen* en gevoelige informatie door *Gebruikers* met geprivilegieerde (verhoogde) *Rechten* binnen een organisatie.
Patch(ing)	Het proces van het toepassen van een specifieke update aan software of *Systemen* waarbij nieuwe of gewijzigde softwarecode (*Patches*) wordt toegevoegd om beveiligingsproblemen op te lossen, bugs te verhelpen of functionaliteit te verbeteren.
Penetratietest(s)	Een toets op fysieke en digitale kwetsbaarheden van een *Systeem* of applicatie met als doel de gevonden kwetsbaarheden te gaan verhelpen of mitigeren.

Private Cloud	Een cloudinfrastructuur die beschikbaar is gesteld voor het exclusieve gebruik door een enkele organisatie met meerdere *Gebruikers* (bijvoorbeeld afdelingen). Deze kan het eigendom zijn van, beheerd worden of geëxploiteerd worden door diezelfde organisatie, een derde partij of een combinatie daarvan.
Proxy	Een computersysteem of applicatie die als een intermediair functioneert tussen verzoeken van werkstations en resources van servers.
PSC(C)	Personnel Security Clearance (Certificate). De verklaring dat een persoon is geautoriseerd voor toegang tot of kennisname van een *Te Beschermen Belang* (waaronder *Bijzondere Informatie*) in internationale context.
PSI	Project Security Instruction. Een document waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van een buitenlandse opdracht.
Public Cloud	Een cloudinfrastructuur die beschikbaar is gesteld aan een groot publiek of meerdere organisaties. Alle gerelateerde hardware, software en ondersteunende infrastructuur zijn eigendom van de *Leverancier*.
RASCI	Responsible, Accountable, Support, Consulted en Informed. Dit betreft een tabel waarin vastgelegd is welke functies welke rol vervullen per activiteit binnen een proces.
Rechten	De aan een *Gebruikers-* of *Beheerdersaccount* toegekende (toegangs)*Rechten* en permissies om specifieke handelingen uit te kunnen voeren binnen een *Systeem* of toegang te hebben tot informatie, zoals het beheren van *Gebruikers-* of systeemconfiguraties of het aanpassen van informatie elementen.
RfV	Request for Visit. Het verzoek aan de betrokken veiligheidsautoriteiten om toestemming voor een bezoek aan een overheidsorganisatie of een bedrijf in het buitenland.
Rijksoverheid	De *Rijksoverheid* wordt gevormd door alle ministeries, uitvoeringsorganisaties en inspecties die onder de verantwoordelijkheid van een minister vallen en de Hoge Colleges van Staat.
Risicoanalyse	Het proces van het gestructureerd vaststellen van de kans op en gevolgen van gebeurtenissen op de belangen van een organisatie. Dit proces bestaat minimaal uit het identificeren (wat kan er gebeuren), het beoordelen (hoe waarschijnlijk is het en wat zijn de gevolgen) en evalueren van risico's.
Risicoland	Een land dat, door zijn intenties, beleid of acties een (potentiële) bedreiging vormt voor de belangen van de Staat, van zijn bondgenoten of van één of meerdere ministeries. Ter informatie kan ook gekeken worden naar de landen die zijn benoemd in de Staatscourant en in de recente jaarverslagen van de *AIVD* en *MIVD*.
RPO	Recovery Point Objective. De maximaal acceptabele hoeveelheid dataverlies die een organisatie kan tolereren na een uitval, inbreuk of ontwrichtende gebeurtenis.
RTO	Recovery Time Objective. De maximale duur van de uitval van een *Systeem* of *Netwerk* die een organisatie kan tolereren.
Rubricering	Het *Rubriceringsdomein en - niveau* dat is vastgesteld voor de betreffende *Bijzondere Informatie* door de eigenaar van de informatie, zoals Departementaal VERTROUWELIJK, Staatsgeheim GEHEIM of NATO SECRET.
Rubriceringsdomein	Aanduiding van een afgebakende omgeving met een eigenaar, zoals *NAVO*, NLD, UK, *EU* of *ESA*, waarvoor de *Bijzondere Informatie* bestemd is.

Rubriceringsniveau	Aanduiding van de verwachte nadelige gevolgen aan de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) de informatie bekend wordt bij niet-geautoriseerden. Binnen een *Rubriceringsniveau* kan onderscheid gemaakt worden tussen verschillende *Merkingen*, die als het betreffende *Rubriceringsniveau* behandeld worden.
SaaS	Software as a Service. Een dienst geleverd aan een *CSC* waarbij een applicatie beschikbaar is gesteld vanaf een cloudinfrastructuur. De applicatie is toegankelijk vanaf verschillende apparaten door middel van een thin client interface, zoals een webbrowser, of een programma interface. *CSC* heeft geen directe controle over, noch beheert de *CSC* de onderliggende cloud-infrastructuur, inclusief *Netwerk*, server, besturingssysteem, opslag, met uitzondering van beperkte gebruikersspecifieke configuratiemogelijkheden van de betreffende applicatie(s).
SAL	Security Aspect Letter. Een document waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van kleinere buitenlandse projecten.
SBOM	Software Bill of Materials. Een inventaris van alle softwarecomponenten, libraries en modules die worden gebruikt in de ontwikkeling van een softwaretoepassing. Het biedt een overzicht van de herkomst, versies en licentie-informatie van deze componenten, evenals hun onderlinge afhankelijkheden.
Scrubber	Een standalone *Systeem* dat *Verwijderbare gegevensdragers* controleert op de aanwezigheid van *Malware* en deze zo nodig in quarantaine plaatst.
Secure by default	Een beveiligingsprincipe waarbij een *Systeem*, product, of dienst standaard zo is ontworpen en geconfigureerd dat het de best mogelijke beveiliging biedt zonder dat *Gebruikers* aanvullende aanpassingen hoeven te maken. Dit betekent dat alle beveiligingsinstellingen en -maatregelen standaard geactiveerd zijn, waardoor de kans op beveiligingslekken door onopgemerkte of niet-geconfigureerde instellingen wordt geminimaliseerd.
Segment	Een deel van een groter *Netwerk* dat logisch of fysiek is gescheiden van andere delen van het *Netwerk*. In het geval van een fysieke scheiding, maakt elk *Segment* gebruik van afzonderlijke netwerkcomponenten, zoals switches, routers, bekabeling en firewalls, waardoor er geen gedeelde fysieke infrastructuur is.
Serviceaccount	Een type account dat gecreëerd is voor het uitvoeren van specifieke applicaties of diensten. Deze accounts zijn bedoeld om geautomatiseerde taken uit te voeren zonder menselijke tussenkomst, zoals het draaien van een databaseservice. Een *Serviceaccount* heeft in principe alleen de benodigde *Rechten* om de toegewezen taken uit te voeren.
Signatures	Eigenschappen van *Malware* op basis waarvan herkenning kan plaatsvinden.
Significante invloed	Een formeel of informeel belang in een organisatie waarbij wijzigingen in bedrijfsvoering, strategie of capaciteiten kunnen worden geïnitieerd en/of geïmplementeerd door of namens de belanghebbende.
SLA	Service Level Agreement. Formele afspraken tussen een dienstverlener en een klant dat de verwachte servicekwaliteit en -prestaties specificeert. Het bevat meetbare criteria om de geleverde diensten te beoordelen.
Staatsgeheim	*Bijzondere Informatie* waarvan de geheimhouding vanwege het belang van de Staat of zijn bondgenoten is geboden.
Systeem	Een samenstel van hardware, software, netwerkcomponenten, IT-infrastructuur en processen die samenwerken om specifieke taken of functies uit te voeren.

Systeemaccount	Een type account dat door het besturingssysteem zelf wordt gebruikt om systeemprocessen en -services uit te voeren (default account). Deze accounts zijn essentieel voor het functioneren van een *Systeem* en worden vaak door een *Systeem* aangemaakt tijdens de installatie van het besturingssysteem. *Systeemaccounts* hebben doorgaans uitgebreide *Rechten* binnen een *Systeem* om ervoor te zorgen dat ze alle noodzakelijke taken kunnen uitvoeren die vereist zijn voor het beheer en de werking van het besturingssysteem.
Systeemdocumentatie	Een document of set van documenten die de implementatie van een *Systeem* beschrijven om beheer te kunnen uitvoeren.
Te Beschermen Belang (TBB)	Personen, informatie, *Systemen*, materieel, goederen, imago en objecten, waarbij in geval van *Compromittatie*, of de mogelijkheid van *Compromittatie*, nadelige gevolgen, of een risico daarop, kunnen ontstaan voor de *Vertrouwelijkheid*, *Beschikbaarheid* en *Integriteit* van de primaire processen van de *Rijksoverheid*, delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries. *Te Beschermen Belangen* zijn ingedeeld in een viertal categorieën (TBB 1 tot en met TBB 4, waarbij TBB 1 de zwaarst te beveiligen categorie is).
Technische infrastructuur	Het geheel van *ICT-bedrijfsmiddelen* voor generiek gebruik, zoals servers, firewalls, *Netwerkapparatuur*, besturingssystemen voor *Netwerken* en servers, databasemanagement-systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
TEMPEST	Het tegengaan van mogelijk compromitterende emissie van elektronische systemen die kan leiden tot het onbevoegd opvangen, verwerken en reproduceren van data.
Tenant	Een afzonderlijke en geïsoleerde instantie binnen een gedeelde *Cloud* omgeving.
Toegang op afstand	Het benaderen van *Systemen*, *Netwerken* en gegevens vanaf een werkstation of *Mobiel apparaat* dat via een extern *Netwerk* verbinding maakt de lokale IT-Infrastructuur.
Transport	Fysiek en gecontroleerd vervoeren van een *Te Beschermen Belang* of *Bijzondere Informatie*, waarbij de *Betrouwbaarheid* gewaarborgd blijft.
Transportmiddel	Een fysiek hulpmiddel dat wordt gebruikt voor het verplaatsen (*Verzenden/Transport*) van een *Te Beschermen Belang*. Het *Transportmiddel* moet voldoen aan gestelde beveiligingsnormen en protocollen om *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid* (ook wel Exclusiviteit) van het *Te Beschermen Belang* te waarborgen.
Uitbesteding	Alle vormen van bedrijfsactiviteiten die direct bijdragen aan de te leveren dienst, waarbij geheel of gedeeltelijk gebruik wordt gemaakt van diensten van een derde partij. Hieronder valt ook het leveren van componenten wanneer *Compromittatie* van deze componenten een beveiligingsrisico vormen voor het *Te Beschermen Belang*.
Uitsteltijd	De opstelsom van het vertragende effect van organisatorische, bouwkundige en/of elektronische beveiligingsmaatregelen op een indringer. Bij de vaststelling van het *Beveiligingsrendement* betreft het de tijd tussen de detectie/verificatie van een inbraak en de *Compromittatie* van een *Te Beschermen Belang*. Maatregelen die een vertragend effect hebben op een indringer voordat detectie/verificatie heeft plaatsgevonden hebben geen effect op het *Beveiligingsrendement*.
Veiligheidsonderzoek	Het proces op basis van de Wet Veiligheidsonderzoeken dat leidt tot afgifte, weigering of intrekking van een *VGB*.
Verboden Plaats	Grote concentraties *Staatsgeheimen* op één locatie kunnen aanleiding zijn om die locatie bij Koninklijk Besluit te benoemen tot een *Verboden Plaats*. Een *Verboden Plaats* wordt op conform *TBB*-categorie 1 beveiligd. Personeel dat toegang moet hebben (‘*Need-to-Be*’), dient te beschikken over een veiligheidsmachtigingsniveau dat overeenkomt met de hoogst aanwezige *Rubricering*.

Vertrouwd(e)	In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau, bijvoorbeeld *Vertrouwde* zones of *Vertrouwde Netwerken*.
Vertrouwelijkheid	Waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwensfunctie	Een functie waarbinnen de mogelijkheid bestaat om de nationale veiligheid te schaden. Zie ook art. 3 lid 1 Wet veiligheidsonderzoeken.
Vertrouwensfunctionaris	Een persoon die op een *Vertrouwensfunctie* is geplaatst.
Verwijderbare gegevensdrager	Opslagmiddelen die eenvoudig kunnen worden verwijderd en meegenomen. Zoals CDROMs, USB sticks, verwijderbare harde schijven of tapes.
Verzenden	Het fysiek aanbieden van een *Te Beschermen Belang*, in het bijzonder *Bijzondere Informatie*, aan een postbedrijf dat zorgdraagt voor doorgaans ongecontroleerd vervoer naar de eindbestemming.
VGB	Verklaring van Geen Bezwaar. Een verklaring dat uit het oogpunt van de nationale veiligheid geen bezwaar bestaat tegen de vervulling van een bepaalde *Vertrouwensfunctie* door een bepaald persoon. Hierbij kan het ook gaan om een internationaal equivalent, mits hier internationale afspraken aan ten grondslag liggen voor de wederzijdse erkenning van dergelijke besluiten.
Virtualisatie	Een technologie die het mogelijk maakt om een of meerdere fysieke computersystemen (de host) op te splitsen in meerdere virtuele machines (VM's) of containers, die onafhankelijk van elkaar kunnen draaien. Een virtuele machine heeft zijn eigen besturingssysteem en applicaties, en functioneert alsof het een afzonderlijke fysieke computer is. Een container heeft een verzameling van software die nodig is om een applicatie te laten draaien.
VOG	Verklaring Omtrent het Gedrag. Een verklaring afgegeven door Justis van het Ministerie van Justitie en Veiligheid waaruit blijkt het gedrag van een persoon in het verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie. Hierbij kan het ook gaan om een internationaal equivalent, mits hier internationale afspraken aan ten grondslag liggen voor de wederzijdse erkenning van dergelijke verklaringen. Een *VOG* is minimaal vereist wanneer een medewerker toegang heeft tot en kennis kan nemen van een *Te Beschermen Belang* categorie 4 of Departementaal Vertrouwelijke informatie.
WAN	Wide Area Network. Een type *Netwerk* dat een groot geografisch gebied bestrijkt, vaak op nationale of zelfs internationale schaal. WAN's verbinden meerdere kleinere *Netwerken*, zoals LAN's (Local Area Networks) of MAN's (Metropolitan Area Networks), waardoor apparaten en *Gebruikers* op verschillende locaties met elkaar kunnen communiceren.
Zeggenschap	De mogelijkheid op grond van feitelijke of juridische omstandigheden invloed uit te oefenen op het beleid van een onderneming. Het hebben van relevante invloed op het beleid van een onderneming kan voortvloeien uit financiële, organisatorische en formele banden (benoemingsrechten, stemrechten op aandelen), directe dan wel indirecte banden (dochter- en zusterondernemingen), samenwerking in een groep of informele samenwerkingsverbanden.
Zelfinspectie	Kritische evaluatie van opzet, bestaan en werking van de beveiligingsmaatregelen door *Opdrachtnemer*.
Zero footprint	Het gebruik van mechanismes om te voorkomen dat gevoelige informatie lokaal wordt opgeslagen of op andere manieren te achterhalen is tijdens of na het gebruik van een apparaat.
Zoneringsmeting	De meting die wordt uitgevoerd om te bepalen welke *TEMPEST*-maatregelen benodigd zijn.

OVERZICHT BIJLAGEN

1. Inrichten beveiligingsorganisatie
2. Beveiligingsfunctionaris
3. Cryptobeheerder
4. Overzicht van Te Beschermen Belangen
5. Fysieke beveiliging
6. Bouwkundige maatregelen
7. Transport en verzenden
8. Labeling en vernietiging van gegevensdragers
9. Goedgekeurde middelen
10. Scrubber
11. Cloud

BIJLAGE 1: INRICHTEN BEVEILIGINGSORGANISATIE

Iedere *Opdrachtnemer* moet beschikken over een integraal beveiligingsbeleid, of een specifiek voor de *Bijzondere Opdracht* opgesteld beveiligingsbeleid. Tevens dient *Opdrachtnemer* een *Beveiligingsfunctionaris* aan te dragen bij *NBIV* (zie bijlage 2). In lijn met het beveiligingsbeleid wordt het *Beveiligingsplan* opgesteld door de *Beveiligingsfunctionaris*. Het ontwikkelen van het *Beveiligingsplan* start met een *Risicoanalyse*. Hierin is uitgewerkt met welke risico's *Opdrachtnemer* rekening moet houden bij het uitvoeren van de *Bijzondere Opdracht*.

Daarnaast wordt beschreven welke beveiligingsmaatregelen zijn gerealiseerd en welke nog gerealiseerd dienen te worden. Hiervoor kan de zelfinspectielijst worden gebruikt.

In het geval dat een bedrijf meerdere *Bijzondere Opdrachten* uitvoert, kan er gekozen worden om een integraal *Beveiligingsplan* op te stellen en per *Bijzondere Opdracht* of locatie sub-*Beveiligingsplannen* op te stellen. In het geval van een internationale opdracht dient er een *Project Security Instruction (PSI)* te worden opgesteld waarin de beveiligingseisen zijn vastgelegd.

In het *Beveiligingsplan* worden minimaal de volgende punten geadresseerd:

- Beschrijving van de lopende *Bijzondere Opdracht(en)* inclusief eenduidige beschrijving van de *Te Beschermen Belang(en)* op de bedrijfslocatie en het *Rubriceringsdomein* en *-niveau* van *Bijzondere Informatie* op de bedrijfslocatie;
- Rollen en verantwoordelijkheden ten aanzien van de *Bijzondere Opdracht(en)*, inclusief de contactgegevens van de *Beveiligingsfunctionaris* en indien van toepassing *sub-Beveiligingsfunctionaris, (sub-) Cyber-Beveiligingsfunctionaris* en *Cryptobeheerder*;
- *Risicoanalyse* ten aanzien van de *Bijzondere Opdracht(en)*;
- Uitgewerkte *Incident Response Procedure;*
- Per onderdeel van het *Beveiligingsplan* een referentie van *ABRO*-eisen waaraan wordt voldaan;
- Overzicht van en toelichting op *ABRO*-eisen waarvoor geen beveiligingsmaatregelen getroffen zijn of die nog gerealiseerd dienen te worden;
- Actuele zelfinspectielijst voorzien van een overzicht van benodigde aanpassingen in beveiligingsmaatregelen en het *Beveiligingsplan*;
- Beschrijving van de manier waarop invulling gegeven wordt aan de bewaartermijnen;
- Procedure(s) voor het uitgeven, vernieuwen en intrekken van digitale *Certificaten*.

Voor verschillende aspecten en procedures is goedkeuring van *NBIV* vereist. Deze goedkeuring kan plaatsvinden middels vastlegging in het *Beveiligingsplan* en goedkeuring daarvan door *NBIV*. Het gaat hierbij om de onderstaande eisen:

Paragraaf	Eisen
4.1 Beheer van ICT-bedrijfsmiddelen	4.1.9 en 4.1.10
4.3 Identificatie en authenticatie	4.3.18 en 4.3.41
4.4 Configuratiemanagement	4.4.3
4.5 Netwerkbeveiliging	4.5.11, 4.5.13, 4.5.23, 4.5.24, 4.5.25, 4.5.34 en 4.5.35

Paragraaf	Eisen
4.6 Endpoint beveiliging	4.6.12
4.7 Beheer van mobiele apparatuur	4.7.3 en 4.7.4
4.12 Onderhoud	4.12.7 en 4.12.8
4.14 Bedrijfscontinuïteit en herstel	4.14.7
4.15 Ontwikkeling en acquisitie	4.15.7

Minimaal jaarlijks evalueert de *Opdrachtnemer* het *Beveiligingsplan,* aan de hand van de zelfinspectie-lijst en een hernieuwde *Risicoanalyse*, om vast te stellen of het *Beveiligingsplan* nog voldoet of moet worden bijgesteld. Naast de jaarlijkse evaluatie kan ook een *Beveiligingsincident* of veranderend dreigingsbeeld een reden zijn om het *Beveiligingsplan* te herzien. Het *Beveiligingsplan* en eventuele (latere) wijzigingen die invloed hebben op de beveiliging worden ter goedkeuring voorgelegd aan *NBIV. Opdrachtnemer* houdt versie- en wijzigingsbeheer van het *Beveiligingsplan* bij.

BIJLAGE 2: BEVEILIGINGSFUNCTIONARIS

Beveiligingsfunctionaris

De *Beveiligingsfunctionaris* is namens zijn werkgever verantwoordelijk voor de beveiliging van de *Bijzondere Opdracht* en dient als primaire contactpersoon voor *NBIV*. Er is één *Beveiligingsfunctionaris* aangewezen. Ook is het mogelijk om één of meerdere sub-*Beveiligingsfunctionarissen* aan te wijzen, bijvoorbeeld als vervanger bij afwezigheid van de *Beveiligingsfunctionaris*. Daarnaast kan een *Cyber-Beveiligingsfunctionaris* worden aangewezen, die de *Beveiligingsfunctionaris* kan ondersteunen bij zaken ten aanzien van cybersecurity.

Aanstellen en ontheffen van een Beveiligingsfunctionaris

Een (sub-)(*Cyber-*)*Beveiligingsfunctionaris* wordt door het *Hoogste bestuursorgaan* van de *Opdrachtnemer* voorgedragen aan *NBIV*. Hiervoor wordt het formulier 'Aanstelling Beveiligingsfunctionaris' gebruikt. Na goedkeuring van *NBIV* wordt een (sub-)(*Cyber-*)*Beveiligingsfunctionaris* benoemd.

Er kunnen aanleidingen zijn dat een (sub-)(*Cyber-*)*Beveiligingsfunctionaris* wordt of moet worden ontheven uit zijn functie. Bijvoorbeeld bij de wijziging van functie of rol binnen de organisatie. *Opdrachtnemer* kan een verzoek tot ontheffing indienen middels het formulier 'Ontheffing Beveiligingsfunctionaris'.

Taken en verantwoordelijkheden

De *Beveiligingsfunctionaris* kan taken, zoals het afgeven van autorisaties voor de toegang tot een *Compartiment*, delegeren of zich laten ondersteunen door bijvoorbeeld een sub-*Beveiligingsfunctionaris*. De *Beveiligingsfunctionaris* blijft echter verantwoordelijk.

De *Beveiligingsfunctionaris* is onder andere verantwoordelijk voor:

- Opstellen en minimaal jaarlijks of bij wijzigingen actualiseren van het *Beveiligingsplan*;
- Coördinatie van en toezicht houden op de beveiliging van de *Bijzondere Opdracht*;
- Uitvoeren en minimaal jaarlijks actualiseren van een *Risicoanalyse* voor de *Bijzondere Opdracht*;
- Uitvoeren en minimaal jaarlijks herhalen van een *Zelfinspectie* met behulp van de zelfinspectielijst;
- Rechtstreeks, onafhankelijk en feitelijk informeren en adviseren van het *Hoogste bestuursorgaan* van *Opdrachtnemer* over beveiligingszaken aangaande de *Bijzondere Opdracht*;
- Bijhouden van een actuele registratie van *Te Beschermen Belangen* (inclusief kopieën);
- Vastleggen van gegevens ten aanzien van toegang tot en inzicht in een *Te Beschermen Belang* en het bewaren van deze gegevens om achteraf onderzoek naar *Beveiligingsincidenten* mogelijk te maken;
- Toezien op de actualiteit van de registratie van *Bijzondere Opdracht(en)* en de *Betrokken Medewerker(s)*;
- Medewerking verlenen bij nalevingscontroles en onderzoeken door of in afstemming met *NBIV* die raken aan een *Bijzondere Opdracht*;
- Melden en onderzoeken van *Beveiligingsincidenten* in afstemming met *NBIV* en treffen van mogelijke additionele beveiligingsmaatregelen;

- Het toezien op de naleving van de vastgestelde voorschriften voor het *Transport* en *Verzenden* van een *Te Beschermen Belang*;
- Verzorgen van voorlichting, training en begeleiding ten aanzien van beveiligingsbewustzijn;
- Afstemmen van internationale bezoeken met *NBIV* gerelateerd aan de *Bijzondere Opdracht;*
- Bijhouden van een actueel overzicht van de gehele keten van *(Toe)leveranciers* en *Onderaannemers* betrokken bij de *Bijzondere Opdracht;*
- Op regelmatige wijze de eventuele sub-*Beveiligingsfunctionaris* of *Cyber-Beveiligingsfunctionaris* op de hoogte stellen van procedures en *Beveiligingsincidenten,* zodat zij deze taken kunnen uitvoeren bij afwezigheid van de *Beveiligingsfunctionaris*.

De *Cyber-Beveiligingsfunctionaris* ondersteunt de *Beveiligingsfunctionaris* bij *Cyber* gerelateerde beveiligingsvraagstukken. Voorbeelden hiervan zijn:

- Bijhouden van een actuele registratie van digitale *Bijzondere Informatie;*
- Toezien op implementatie van benodigde *Cyber* beveiligingsmaatregelen om de *Betrouwbaarheid* van een *Te Beschermen Belang* te waarborgen;
- Toezien op de *Betrouwbaarheid* van de digitale infrastructuur van *Opdrachtnemer;*
- Coördineren van de registratie en afhandeling van *Cyber* gerelateerde *Beveiligingsincidenten;*
- Toezien op geordende en traceerbare procedures bij wijzigingen in *Cyber* beveiligingsmaatregelen of de digitale infrastructuur van *Opdrachtnemer;*
- Regelmatig de *Beveiligingsfunctionaris* op de hoogte stellen van lopende zaken zoals de afhandeling van *Cyber-Beveiligingsincidenten*.

BIJLAGE 3: CRYPTOBEHEERDER

Cryptobeheerder

Een *Cryptobeheerder* is belast met de zorg voor *Cryptografische beveiligingsoplossingen*. Een *Cryptobeheerder* dient te beschikken over gecertificeerde kennis van cryptografie. Het *Hoogste bestuursorgaan* van de *Opdrachtnemer* draagt een kandidaat *Cryptobeheerder* aan bij *NBIV* middels het daartoe bestemde formulier 'Aanstelling Cryptobeheerder'. Het is mogelijk om de *Beveiligingsfunctionaris* tevens de rol van *Cryptobeheerder* te laten vervullen. In dat geval dienen beide formulieren, 'Aanstelling Beveiligingsfunctionaris' en 'Aanstelling Cryptobeheerder', ingediend te worden.

Wanneer *Opdrachtnemer* cryptografische sleutels ontvangt in het kader van een *Bijzondere Opdracht* via de Nationale Distributie Autoriteit of *Opdrachtgever*, zijn er minstens twee *Cryptobeheerders* benoemd, tenzij met *NBIV* anders is overeengekomen.

Indien bij een internationale opdracht nationaliteitseisen worden vastgesteld door *Opdrachtgever*, worden deze door *Opdrachtnemer* nageleefd. Dit kan ook gelden voor een *Cryptobeheerder* en wordt aangegeven door *Opdrachtgever*.

Taken en verantwoordelijkheden

Ten aanzien van *Cryptografische beveiligingsoplossingen* in het kader van *Bijzondere Opdracht* is de *Cryptobeheerder* verantwoordelijk voor:

- Opvolgen van de aansluitvoorwaarden van *Opdrachtgever*, het inzetadvies en adviezen van de fabrikant en de opvolging documenteren in het *Beveiligingsplan;*
- Overhandigen van beheerdersinstructies en opleiden van *Beheerders*;
- Overhandigen van gebruikersinstructies en opleiden van *Gebruikers*;
- *Autoriseren* van *Gebruikers* en *Beheerders* van *Cryptografische beveiligingsoplossingen;*
- Documenteren in het *Beveiligingsplan* van overeenkomsten, wetten en voorschriften waaraan *Cryptografische beveiligingsoplossingen* moeten voldoen en deze implementeren in cryptografische technieken;
- Vastleggen van het proces, de actoren en hun verantwoordelijkheden (conform *RASCI*) ten aanzien van het beheer van *Cryptografische beveiligingsoplossingen* in het cryptografiebeleid als onderdeel van het *Beveiligingsplan*;
- Ziet toe op de geldigheid van cryptografische sleutels conform het cryptografiebeleid als onderdeel van het *Beveiligingsplan*;
- Melden en opvolgen van de procedure bij (mogelijk) gecompromitteerde *Cryptografische beveiligingsoplossingen* in afstemming met *NBIV* en de eigenaar van de cryptografische sleutel(s);
- Optreden als primair contactpersoon voor de eigenaar van de cryptografische sleutel(s);
- Registreren van in gebruik zijnde *Cryptografische beveiligingsoplossingen;*
- Beheren, uitgeven, laden en periodiek tellen van sleutels evenals het inventariseren van *Cryptografische beveiligingsoplossingen;*
- Opslag, verpakking en *Transport* van *Cryptografische beveiligingsoplossingen;*
- Afvoer en vernietigen van *Cryptografische beveiligingsoplossingen.*

BIJLAGE 4: OVERZICHT VAN TE BESCHERMEN BELANGEN

Het overzicht van *Te Beschermen Belangen* wordt voorafgaand aan de *Bijzondere Opdracht* opgesteld door *Opdrachtgever* en vervolgens overgedragen aan de *Opdrachtnemer*. Hierin wordt voor informatie, informatiesystemen, materieel, goederen en objecten ten aanzien van de *Bijzondere Opdracht* weergegeven welke *TBB*-categorie of *Rubriceringsniveau* van toepassing is. Daarnaast wordt het belang van de *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid* van de informatie, informatiesystemen, materieel, goederen en objecten inzichtelijk gemaakt. Een Rubriceringsaanduidingslijst (RAL) is een manier om de *Te Beschermen Belangen* en bijbehorende *TBB*-categorieën of *Rubriceringsniveaus* in kaart te brengen.

Het overzicht van *Te Beschermen Belangen* geeft daarmee inzicht in de van toepassing zijnde niveau(s) van het *Te Beschermen Belang(en)* in het kader van de *Bijzondere Opdracht*. Daarnaast geeft het *Opdrachtnemer* inzicht in de deelgebieden, en daarmee de *ABRO 2026* hoofdstukken, die van toepassing zijn voor de *Bijzondere Opdracht*. Aan de hand van dit overzicht past *Opdrachtnemer* in afstemming met *NBIV* de benodigde beveiligingsmaatregelen toe in lijn met de vanuit *ABRO 2026* voorgeschreven eisen.

Overzicht van Te Beschermen Belangen bij Uitbesteding

Wanneer een *Opdrachtnemer* werkzaamheden voor de *Bijzondere Opdracht Uitbesteedt* aan een of meerdere *Onderaannemer(s)*, dient *Opdrachtnemer* een overzicht van *Te Beschermen Belangen* op te stellen voor de werkzaamheden die door de betreffende *Onderaannemer(s)* worden uitgevoerd. Het opstellen van een overzicht van *Te Beschermen Belangen* gebeurt in afstemming met *Opdrachtgever* en *NBIV*. Hierdoor hebben *Opdrachtgever* en *NBIV* blijvend inzicht in de *Onderaannemer(s)* die toegang hebben tot een *Te Beschermen Belang*.

Buitenlandse equivalent

Bedrijven kunnen ook in aanmerking komen voor een *Bijzondere Opdracht* van *NAVO*, *EU* of een buitenlandse overheidsorganisatie. Naast nationale *Te Beschermen Belangen* kan derhalve sprake zijn van *NAVO*- of *EU*- of buitenlandse *Te Beschermen Belangen*. *NBIV* treedt naar het betrokken bedrijf op als de aangewezen Designated Security Authority (DSA) namens die organisaties en landen. Vaak is daarbij de voorwaarde dat daarover afspraken zijn vastgelegd in een *Beveiligingsverdrag* of een zogenaamd *Memorandum of Understanding (MoU)*.

NAVO- en *EU*-regelgeving en vaak ook internationale verdragen schrijven voor dat in de contracten met *NAVO*, *EU* en buitenlandse overheidsorganisaties voor de beveiligingseisen van grote projecten een specifieke “Project Security Instruction” (*PSI*) wordt opgenomen. Voor kleinere projecten wordt in dit verband vaak een “Security Aspect Letter” (*SAL*) gebruikt. Inhoudelijk vertonen een *PSI* en *SAL* veel overeenkomsten met *ABRO 2026*. Zo kennen de *PSI* en de *SAL* een “Security Classification Guide” en een “Security Classification Checklist”, het equivalent van het overzicht van *Te Beschermen Belangen* uit *ABRO 2026*. Bedrijven die werken aan dergelijke *Bijzondere Opdrachten*, worden gecontroleerd op basis van *ABRO 2026*.

BIJLAGE 5: FYSIEKE BEVEILIGING

Om te voorkomen dat een niet-geautoriseerd persoon fysieke toegang krijgt tot een *Te Beschermen Belang*, worden fysieke beveiligingsmaatregelen getroffen. Het *Te Beschermen Belang* moet worden beveiligd zodat enerzijds *Compromittatie* wordt voorkomen en anderzijds *Compromittatie* wordt gedetecteerd en/of gesignaleerd. Om dit te realiseren wordt een combinatie van Organisatorische-, Bouwkundige-, Elektronische- en Reactieve- (OBER) maatregelen getroffen.

- **Organisatorische maatregelen:**
  Bij organisatorische maatregelen kan worden gedacht aan toegangscontrole en het proces van identificatie, *Authenticatie* en *Autorisatie* van personen. Hierbij wordt te allen tijde rekening gehouden met de principes '*Need-to-Know*' en '*Need-to-Be*'.
- **Bouwkundige maatregelen:**
  Bouwkundige maatregelen vormen de ruggengraat van de fysieke beveiligingsmaatregelen. Voorbeelden zijn inbraakwerende muren, inbraakwerend glas en versterkt hang- en sluitwerk (zie ook bijlage 6).
- **Elektronische maatregelen:**
  Elektronische maatregelen omvatten alle materiële voorzieningen op elektronisch, elektrotechnisch of optisch gebied, die een observerende, sturende, signalerende of alarmerende functie hebben. Voorbeelden zijn camerasystemen (CCTV), toegangsbeheersystemen (zoals *ETS*) en diverse soorten detectoren (zoals *IDSS*).
- **Reactieve maatregelen:**
  Voor de beveiliging van een *Te Beschermen Belang* is de reactie op (vermeende) *Beveiligingsincidenten* essentieel. Voorbeelden van reactieve maatregelen zijn procedures voor alarmopvolging, alarmverificatie en *Interventie*.

Bij het bepalen van de benodigde maatregelen wordt van binnen naar buiten geredeneerd, met het *Te Beschermen Belang* als startpunt. Een *Te Beschermen Belang* moet in een *Compartiment* zijn geplaatst. Daarnaast moet een *Compact Te Beschermen Belang* – zoals een laptop, maar ook grotere objecten die redelijkerwijs fysiek opgeborgen kunnen worden – in een daartoe geschikt *Opbergmiddel* geplaatst worden. Vervolgens moeten passende Organisatorische, Bouwkundige, Elektronische of Reactieve beveiligingsmaatregelen getroffen worden om *Compromittatie* van het *Te Beschermen Belang* tegen te gaan, te detecteren en *Interventie* tijdig te laten plaatsvinden.

Fysieke beveiligingsmaatregelen worden altijd georganiseerd volgens een schillenstructuur, bijvoorbeeld door een *Te Beschermen Belang* in een *Opbergmiddel* te plaatsen en dit *Opbergmiddel* in een afgesloten ruimte of bijvoorbeeld *Compartiment* te plaatsen. Het gelaagd opbouwen van fysieke beveiligingsmaatregelen zorgt ervoor dat *Uitsteltijd* wordt gerealiseerd. Daarnaast maakt het dat het doorbreken van één beveiligingsmaatregel niet direct leidt tot *Compromittatie* van het *Te Beschermen Belang*.

Beveiligingsrendement

Het Beveiligingsrendement vormt de basis voor het bepalen van de benodigde fysieke beveiligingsmaatregelen. Het *Beveiligingsrendement* komt voort uit de *Uitsteltijd* en de *Interventietijd*. Om de benodigde *Uitsteltijd* te bepalen, is inzicht nodig in de fysieke dreigingen en risico's ten aanzien van de *Bijzondere Opdracht* en het *Te Beschermen Belang*. Hiertoe dient een *Risicoanalyse* uitgevoerd te worden.

Daarnaast is het van belang inzicht te krijgen in de middelen die een potentiële dader ter beschikking heeft, hiertoe kan het daderprofiel worden gebruikt. Deze kan op verzoek door *NBIV* beschikbaar worden gesteld.

Het vereiste *Beveiligingsrendement* is in *ABRO 2026* vastgelegd voor de verschillende *TBB*-categorieën, zie ook de onderstaande tabel.

TBB-categorie	Beveiligingsrendement
TBB 1 en TBB 2	*Te Beschermen Belangen* in deze categorie vereisen een positief *Beveiligingsrendement*. Dit betekent dat *Interventie* altijd moet plaatsvinden voordat *Compromittatie* heeft plaatsgevonden (*Interventietijd* < *Uitsteltijd*).
TBB 3	*Te Beschermen Belangen* in deze categorie vereisen een *Beveiligingsrendement* van maximaal 120 minuten. Dit betekent dat *Interventie* altijd moet plaatsvinden binnen 120 minuten na *Compromittatie* (*Interventietijd* - *Uitsteltijd* < *120* minuten).
TBB 4	*Te Beschermen Belangen* in deze categorie vereisen geen *Beveiligingsrendement*. *Compromittatie* of pogingen daartoe moeten gedetecteerd worden, maar daaraan is geen termijn verbonden. Na constatering van *Compromittatie* wordt binnen 48 uur een *Melding* gemaakt bij het *NBIV*.

Voorbeeld voor TBB 1 en 2

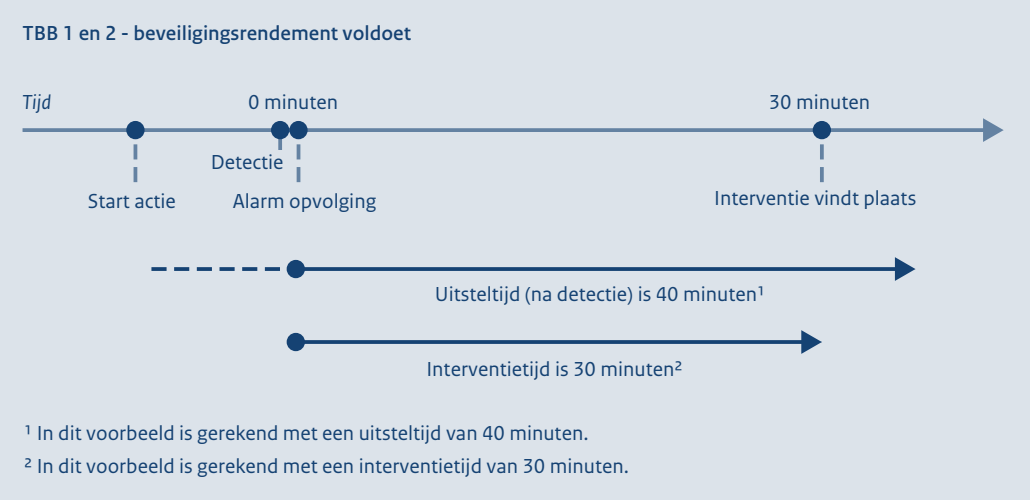
Voor het realiseren van een positief *Beveiligingsrendement* moet dus gekeken worden welke maatregelen nodig zijn om een dader zodanig te vertragen na alarmering dat *Interventie* altijd eerder plaatsvindt dan *Compromittatie*. Dat hangt af van de *Interventietijd*. Wanneer de *Interventietijd* 15 minuten is zijn er minder (zware) maatregelen nodig om een dader te vertragen dan wanneer de *Interventietijd* 30 minuten is.

In het onderstaand voorbeeld is de *Interventietijd* 30 minuten. Om een positief *Beveiligingsrendement* te realiseren dienen de fysieke beveiligingsmaatregelen tezamen dus een *Uitsteltijd* van minimaal 30 minuten te realiseren. Dit kan door bijvoorbeeld trildetectie op het *Opbergmiddel* te plaatsen en een *Opbergmiddel* te gebruiken dat conform NEN-normeringen in bijlage 6 voldoende *Uitsteltijd* oplevert.

De *Uitsteltijd* is afhankelijk van de middelen die een dader redelijkerwijs kan gebruiken. Op basis van de NEN-normeringen en de beschikbare middelen van de dader kan de *Uitsteltijd* van een fysieke beveiligingsmaatregel bepaald worden. Het is ook mogelijk om detectie al buiten het *Compartiment* plaats te laten vinden. Hierdoor zal een dader na detectie eerst nog de bouwkundige afscherming van het *Compartiment* moeten doorbreken en vervolgens nog het *Opbergmiddel* moeten forceren. Stel dat het *Compartiment* zorgt voor 10 minuten *Uitsteltijd*, dan volstaat een *Opbergmiddel* dat 20 minuten *Uitsteltijd* oplevert, aangezien dit gezamenlijk voor 30 minuten *Uitsteltijd* zorgt.

In beide opties is een dader na detectie nog 30 minuten bezig om daadwerkelijke toegang te krijgen tot het *Te Beschermen Belang*. Aangezien *Interventie* in dit voorbeeld binnen 30 minuten plaatsvindt, zal de dader gehinderd worden voordat het *Te Beschermen Belang* gecompromitteerd wordt.

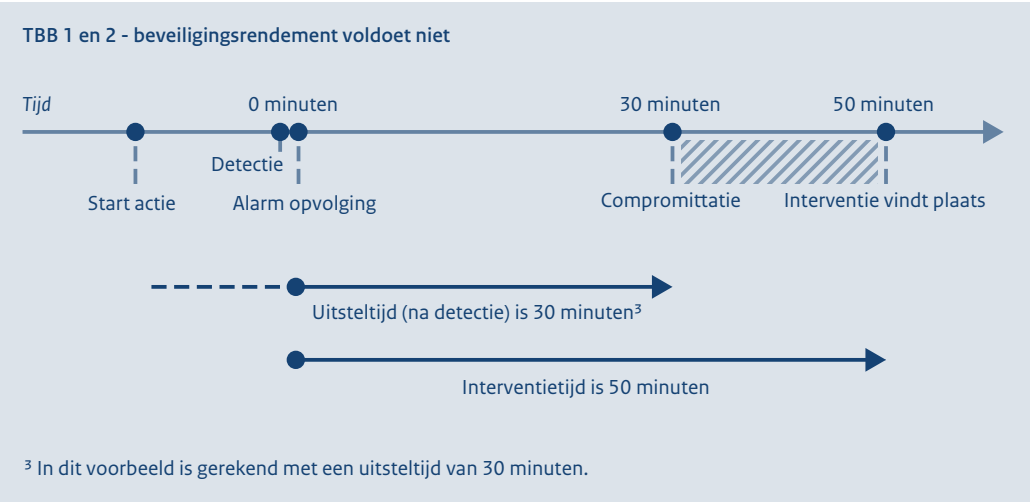
Opdrachtnemer stemt met *NBIV* af welke fysieke beveiligingsmaatregelen getroffen dienen te worden. Een schematische weergave van een rekenvoorbeeld is te vinden in figuur 1.



Figuur 1: Rekenvoorbeeld TBB 1 en 2

In het voorbeeld in figuur 1 is een *Uitsteltijd* van 40 minuten gegenereerd. De *Interventietijd* is 30 minuten na detectie. Daardoor wordt het vereiste positief *Beveiligingsrendement* gerealiseerd. In deze situatie vindt er dus geen *Compromittatie* van het *Te Beschermen Belang* plaats.

De fysieke beveiligingsmaatregelen dienen zodanig te worden ingericht dat een positief *Beveiligingsrendement* wordt gerealiseerd. Onderstaand ter illustratie nog een tijdslijn waarbij dit niet het geval is (figuur 2). In dit voorbeeld is de *Interventietijd* 50 minuten na detectie. De gerealiseerde *Uitsteltijd* is 30 minuten. Hierdoor heeft de dader 20 minuten ongeautoriseerde toegang tot het *Te Beschermen Belang*.



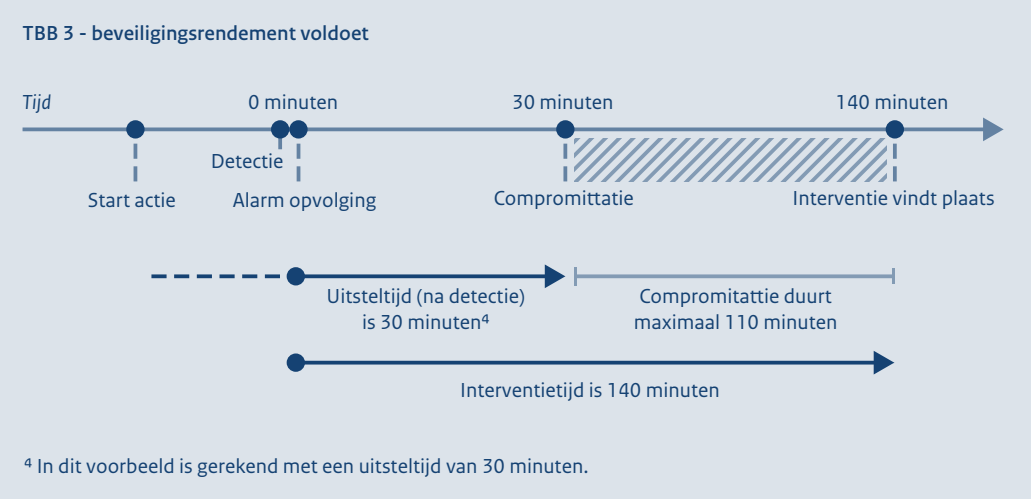
Figuur 2: Rekenvoorbeeld waarbij positief beveiligingsrendement niet is gerealiseerd

Voorbeeld voor TBB 3

In het onderstaande voorbeeld bieden de fysieke beveiligingsmaatregelen een *Uitsteltijd* van 30 minuten (figuur 3). Dit houdt in dat 30 minuten na detectie een niet-geautoriseerde toegang heeft tot of kennis kan nemen van een *Te Beschermen Belang*. Voorbeelden van beveiligingsmaatregelen om *Uitsteltijd* te genereren zijn het plaatsen van een *Te Beschermen Belang* in een *Opbergmiddel*, zoals een kluis.

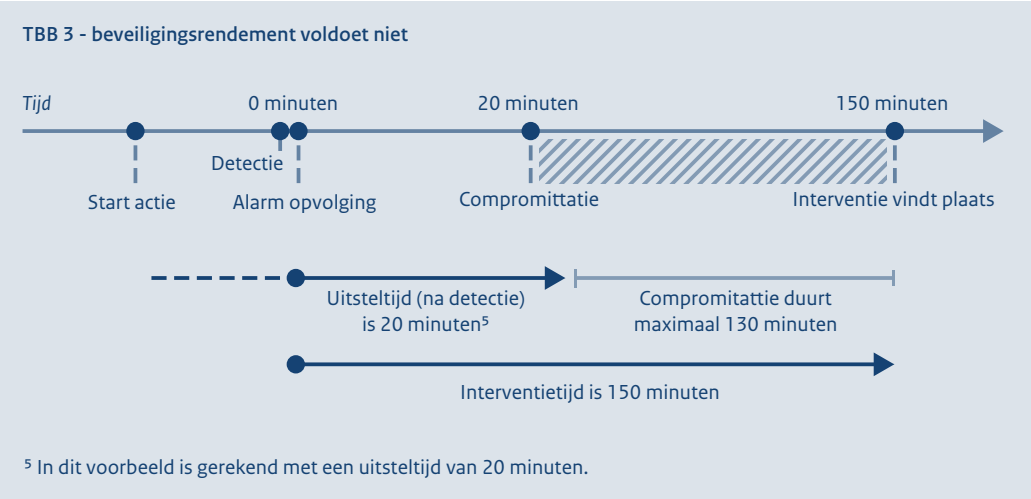
TBB 3 vereist dat *Interventie* uiterlijk 120 minuten na *Compromittatie* moet plaatsvinden. De kluis in dit voorbeeld heeft een *Uitsteltijd* van 30 minuten. Dat betekent dat een dader 30 minuten nodig heeft om de kluis te forceren. De kluis in dit voorbeeld is uitgerust met trildetectie, dus zodra de dader begint met het forceren van de kluis vindt alarmering plaats en wordt de *Interventie* in gang gezet. De *Interventietijd* in dit voorbeeld is 140 minuten. De *Beveiligingsfunctionaris* of het aanwezige *Beveiligingspersoneel* zijn dus uiterlijk 140 minuten na alarmering ter plaatse. Aangezien de dader 30 minuten nodig heeft om de kluis te forceren, heeft de dader maximaal 110 minuten toegang tot het *Te Beschermen Belang* en is er dus sprake van *Compromittatie*, alvorens *Interventie* plaatsvindt.

In het onderstaande voorbeeld volgt de *Interventie* binnen 110 minuten na *Compromittatie*. Hiermee is het *Beveiligingsrendement* 110 minuten, hetgeen binnen de vereiste 120 minuten valt. Ook in dit geval stemt *Opdrachtnemer* af met *NBIV* welke fysieke beveiligingsmaatregelen getroffen dienen te worden. Een schematische weergave van dit voorbeeld is te vinden in onderstaand figuur (figuur 3).



Figuur 3: Rekenvoorbeeld TBB 3

Voor TBB 3 is het realiseren van een *Beveiligingsrendement* van 120 minuten vereist. Onderstaand is ter illustratie nog een tijdslijn opgenomen waarbij dit niet het geval is (figuur 4). In dit voorbeeld is de *Interventietijd* 150 minuten na detectie. De gerealiseerde *Uitsteltijd* is 20 minuten. Dit resulteert in een *Beveiligingsrendement* van 130 minuten, hetgeen meer is dan de benodigde 120 minuten.



Figuur 4: Rekenvoorbeeld waarbij vereiste Beveiligingsrendement niet is gerealiseerd

BIJLAGE 6: BOUWKUNDIGE MAATREGELEN

Bouwkundige beveiligingsmaatregelen vormen een belangrijk onderdeel van de OBER-maatregelenmix. Het is derhalve van belang om adequate bouwkundige maatregelen op het vereiste beveiligingsniveau tijdig te adresseren in nieuwbouwplannen of wijzigingen. In het geval van bestaande bouw stemt *Opdrachtnemer* met *NBIV* af welke fysieke beveiligingsmaatregelen getroffen moeten worden. Voorbeelden van bouwkundige maatregelen zijn:

- Inbraakwerende muren;
- Versterkte deuren;
- Inbraakwerend glas;
- Versterkt hang- en sluitwerk;
- Hekwerken en andere terreinaanpassingen.

Bouwkundige maatregelen vormen een belangrijke barrière tegen niet-geautoriseerde personen die proberen fysieke toegang te krijgen tot een *Te Beschermen Belang*. Denk daarbij aan inbraak, met als doel veelal diefstal, spionage of sabotage, maar ook aan abusievelijke toegang van niet-geautoriseerde medewerkers. Om de benodigde bouwkundige maatregelen te bepalen, kan gebruik gemaakt worden van relevante NEN-normeringen. Een overzicht hiervan is opgenomen in de tabel op de volgende pagina.

Een *Te Beschermen Belang* moet in een (bouwkundig) *Compartiment* worden geplaatst. Wanneer het gaat om een *Compact Te Beschermen Belang* (zoals een laptop of *Bijzondere Informatie*) dient het *Compact Te Beschermen Belang* in een *Opbergmiddel* te worden geplaatst.

Visueel en akoestisch beperkende maatregelen

Tevens zijn visuele (inkijkbeperkende) en akoestische (geluidsbeperkende) beveiligingsmaatregelen noodzakelijk. Deze maatregelen moeten voorkomen dat niet-geautoriseerde personen, al dan niet met gebruik van hulpmiddelen, van buiten het *Compartiment* kennis kunnen nemen van het *Te Beschermen Belang*.

Inkijkbeperkende beveiligingsmaatregelen voorkomen dat niet-geautoriseerde personen van buiten de werkruimte kennis kunnen nemen van een *Te Beschermen Belang*. Deze maatregelen zijn noodzakelijk ongeacht de *Rubricering* en/of *Merking*. Geluidsbeperkende beveiligingsmaatregelen voorkomen dat niet-geautoriseerde personen, al dan niet met gebruik van auditieve hulpmiddelen, door waarnemen (afluisteren) van buiten de werkruimte kennis kunnen nemen van een *Te Beschermen Belang*. Deze maatregelen zijn niet noodzakelijk voor TBB 4.

Dergelijke beveiligingsmaatregelen worden getroffen in vergaderzalen, briefingrooms en werkruimten waarin een *Te Beschermen Belang* wordt besproken of behandeld.

Bijlage 6.1: Overzicht NEN-normeringen

Onderstaande tabel toont een overzicht van relevante NEN-normeringen ten aanzien van fysieke beveiliging.

NEN-EN 5096	Inbraakwerendheid • Dak of gevelelementen met deuren, ramen, luiken en vaste vullingen • Eisen, classificatie en beproevingsmethoden
NEN-EN 1143	Waardeberging • Eisen, classificatie en beproevingsmethoden van de weerstand tegen inbraak
NEN-EN 1627	Deuren, ramen, vliesgevels, traliehekken en luiken • Inbraakwerendheid • Eisen en classificatie
NEN-EN 50131	Alarmsystemen • Inbraak- en overvalsystemen
NEN-EN 50136	Alarmsystemen, specifiek alarmtransmissiesystemen en -apparatuur
NEN-EN-IEC 62676	Video surveillance systems for use in security applications

BIJLAGE 7: TRANSPORT EN VERZENDEN

Tijdens *Transport* of *Verzending* is een *Te Beschermen Belang* kwetsbaarder dan wanneer het zich op een beveiligde locatie bevindt. Men kan immers niet terugvallen op de OBER-maatregelen die het *Te Beschermen Belang* beschermen in de normale situatie binnen het *Compartiment*. De verhoogde kwetsbaarheid houdt een verhoogde kans op *Compromittatie* van het *Te Beschermen Belang* in. Bij internationaal *Transport* en *Verzending* neemt de kwetsbaarheid nog verder toe.

Een belangrijk uitgangspunt is dat *Transport* dan wel *Verzenden* van een *Te Beschermen Belang* tot een minimum moet worden beperkt. Indien het voor de uitvoering van de *Bijzondere Opdracht* noodzakelijk is om een *Te Beschermen Belang* buiten het *Compartiment* te brengen, dient de *Beveiligingsfunctionaris* hier vooraf goedkeuring voor te geven. Daarnaast is het van belang om na te gaan of de ontvangende partij, bijvoorbeeld een *Onderaannemer*, de juiste beveiligingsmaatregelen getroffen heeft om het vereiste beveiligingsniveau van het *Te Beschermen Belang* te kunnen waarborgen.

De *Beveiligingsfunctionaris* beschrijft in het *Beveiligingsplan* op welke wijze om wordt gegaan met *Transport* en *Verzenden* van een *Te Beschermen Belang*. Hierin staan ten minste de volgende punten:

- (Aanvullende) relevante wet- en regelgeving;
- Internationale afspraken, zoals vastgelegd in een *PSI* of *SAL*;
- *Risicoanalyse* ten aanzien van *Transport* en *Verzenden*, inclusief bijbehorende dreigingen;
- Rol van *Opdrachtgever* bij *Transport* en *Verzenden*;
- Omgang met praktische zaken, zoals overslag, wachttijden en overnachtingen.

Indien zich gedurende het *Transport* of *Verzenden* onverhoopt een *Beveiligingsincident* voordoet, dient onmiddellijk de *Incident Response Procedure* te worden opgestart.

Verzenden

Onder *Verzenden* wordt verstaan: het fysiek aanbieden van een *Te Beschermen Belang*, in het bijzonder *Bijzondere Informatie*, aan een postbedrijf dat zorgdraagt voor doorgaans ongecontroleerd vervoer naar de eindbestemming. Enkel TBB 4/Departementaal VERTROUWELIJK mag worden verzonden.

Voorafgaand aan *Verzenden* dient het betreffende *Te Beschermen Belang* verpakt te worden zodat de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is. Daarnaast is een onmiddellijke ontvangstbevestiging vereist.

Daarnaast is bij *Verzenden* van een *Te Beschermen Belang* een ontvangstbevestiging noodzakelijk. In zo'n geval wordt bij het verpakken van het *Te Beschermen Belang* een ontvangstbevestiging bijgevoegd. De ontvanger zendt de ondertekende ontvangstbevestiging, ten minste voorzien van een handtekening en datum, terug naar de afzender. De afzender ziet er op toe dat de ontvangstbevestiging binnen een redelijke termijn wordt ontvangen. Onder redelijke termijn wordt verstaan:

- Binnen Nederland: 2 weken;
- Binnen Europa: 3 weken;
- Buiten Europa: 1 maand.

Wanneer de ontvangstbevestiging niet binnen bovenstaande termijn plaatsvindt, doet afzender navraag bij de ontvanger. Als dit geen resultaat heeft, stelt de afzender de *Beveiligingsfunctionaris* op de hoogte. Indien het *Transport* niet is aangekomen, dient dit als *Beveiligingsincident* te worden behandeld.

Transport

Onder *Transport* wordt verstaan het fysiek en gecontroleerd vervoeren van een *Te Beschermen Belang* of B*ijzondere Informatie* waarbij de *Betrouwbaarheid* gewaarborgd blijft. Voor het *Transport* van een *Te Beschermen Belang* is veelal maatwerk nodig, en worden beveiligingsmaatregelen vastgesteld door *Opdrachtgever*.

Voorafgaand aan een *Transport* van *Bijzondere Informatie* van TBB 3, TBB 2 en TBB 1 dient een transportplan opgesteld te worden conform formulier 'Transportplan' en in afstemming met *NBIV* ter goedkeuring te worden voorgelegd aan *Opdrachtgever*. Het transportplan beschrijft de daadwerkelijke inrichting van het *Transport* in lijn met de richtlijnen uit het *Beveiligingsplan*. *Transport* van een TBB 1 vindt enkel plaats met voorafgaande goedkeuring van *Opdrachtgever*.

Voor *Transport* van *Bijzondere Informatie* met TBB 2, 3 en 4 binnen Nederland heeft *Opdrachtnemer* een aantal opties:

- *Transport*-/koeriersbedrijf met *ABRO-Verklaring*;
- *Transport* door *Geautoriseerde Medewerkers*.

Voorafgaand aan *Transport* dient de *Bijzondere Informatie* zorgvuldig te worden verpakt. In het transportplan wordt beschreven hoe de *Bijzondere Informatie* wordt verpakt.

Internationaal Transport

Voor internationaal *Transport* dient het transportplan ten minste 10 werkdagen voorafgaand aan *Transport* in afstemming met *NBIV* ter goedkeuring voorgelegd te worden aan *Opdrachtgever*. Naast de eisen en maatregelen voor beveiliging van *Transport* uit *ABRO* 2026 kunnen specifieke bi- of multilaterale afspraken zijn gemaakt voor internationaal *Transport* van een (buitenlands) *Te Beschermen Belang*. Dit is doorgaans vastgelegd in een *PSI* of *SAL*.

BIJLAGE 8: LABELING EN VERNIETIGING VAN GEGEVENSDRAGERS

Het is van belang dat een *Gegevensdrager* wordt voorzien van een label met de *Rubricering* en/of *Merking* die aangeven op welke wijze de *Gegevensdrager* behandeld en opgeslagen moet worden. Wanneer de *Bijzondere Opdracht* is beëindigd of een *Gegevensdrager* niet meer benodigd is voor de *Bijzondere Opdracht*, dient deze te worden vernietigd.

Labeling van Gegevensdragers

	Toepassing	Rubriceringstekst	Methode van aanbrenging	Plaats rubricering/merking
Document	Gehele document is gerubriceerd en/of gemerkt	*Rubricering* en/of *Merking* in hoofdletters (alleen op eerste pagina of in colofon: vermelding van vaststeller *Rubricering*, datum vaststelling en de geldigheidsduur).	• Handgeschreven • Geprint • Gestempeld	• Boven- en onderkant van elke bladzijde • Op omslag • Op bijlagen (Aanbrengen exemplaar- en bladzijdenummering)
Document	Bijlage is hoger gerubriceerd en/of gemerkt dan hoofd-document	Hoogste *Rubricering* en/of *Merking* in hoofdletters. (In colofon: vermelding van vaststeller *Rubricering*, datum vaststelling en de geldigheidsduur)	• Handgeschreven • Geprint • Gestempeld	Op de omslag hoofddocument: <hoogste *Rubricering/Merking*> met toevoeging zonder bijlage (x) <*Rubricering/Merking*> of <ongerubriceerd/ongemerkt>. Op de bijlage(n) aan de boven- en onderkant van elke bladzijde. (Aanbrengen exemplaar- en bladzijdenummering).
Document	Verschillende *Rubriceringen* in één document.	(Stg-ZG): alinea met *Stg.* ZEER GEHEIM gerubriceerde informatie (Stg-G): alinea met *Stg.* GEHEIM gerubriceerde informatie (Stg-C): alinea met *Stg.* CONFIDENTIEEL gerubriceerde informatie (DV) alinea met Departementaal VERTROUWELIJK gerubriceerde informatie	• Handgeschreven • Geprint • Gestempeld	Hoogste *Rubricering* aan boven- en onderkant van elke bladzijde. Afkorting *Rubricering* aanbrengen aan het begin van iedere alinea. (Aanbrengen exemplaar- en bladzijdenummering).

	Toepassing	Rubriceringstekst	Methode van aanbrenging	Plaats rubricering/merking
Verwijderbare gegevens-dragers	Alle *Rubriceringen* en/of *Merkingen*.	Hoogste niveau van *Rubriceringen* en/of *Merkingen* in hoofdletters.	*Gegevensdrager* graveren, inbranden of beschrijven met watervaste stift, of sticker met *Rubricering / Merking*, kleur of lint/label.	Stickers of (graveer-) tekst zichtbaar plaatsen. Zo mogelijk beide zijden van een sticker of (graveer-) tekst voorzien.
Werkstations	Alle *Rubriceringen* en/of *Merkingen*.	Hoogste niveau van *Rubriceringen* en/of *Merkingen* in hoofdletters.	Sticker met *Rubricering / Merking*.	Stickers zichtbaar plaatsen op systeemkast en bovenzijde beeldscherm.
Laptops	Alle *Rubriceringen* en/of *Merkingen*.	Hoogste niveau van *Rubriceringen* en/of *Merkingen* in hoofdletters.	Sticker met *Rubricering / Merking*.	Stickers zichtbaar plaatsen op buitenzijde scherm/klep.

Wanneer het ongewenste aandacht kan trekken om een *Gegevensdrager* op bovenstaande manier te labelen, kan gebruik gemaakt worden van onderstaand kleurensysteem. Wanneer hiervan gebruik wordt gemaakt, wordt de tabel met gebruikersinstructies beschreven in het *Beveiligingsplan*.

Labeling van Gegevensdragers middels kleurensysteem

	Rood	TBB 1	*Stg.* ZEER GEHEIM
	Blauw	TBB 2	*Stg.* GEHEIM
	Groen	TBB 3	*Stg.* CONFIDENTIEEL
	Geel	TBB 4	Departementaal VERTROUWELIJK
	Wit		Ongerubriceerd

Vernietiging van Gegevensdragers

	TBB 4 DV	TBB 3 Stg. C	TBB 2 Stg. G	TBB 1 Stg. ZG
Papier	Versnipperen L < 30mm B < 5mm	Versnipperen L < 25mm B < 3mm	Versnipperen L < 25 mm B < 3mm	Versnipperen L < 25 mm B < 3mm en verbranden
Papier i.h.k.v. internationale opdracht	Versnipperen max. 25mm2	Versnipperen max. 25mm2	Versnipperen max. 25mm2	Versnipperen max. 25mm2
Film	Versnipperen	Versnipperen (vernietigingsklasse P4*, max. 160mm2)	Versnipperen (vernietigingsklasse P5*, max. 30mm2)	Versnipperen (vernietigingsklasse P5*, max. 30mm2) en verbranden

	TBB 4 DV	TBB 3 Stg. C	TBB 2 Stg. G	TBB 1 Stg. ZG
Optische gegevensdragers (CD/DVD)	Breken	Versnipperen (vernietigingsklasse O4*, max. 30mm2)	Versnipperen (vernietigingsklasse O5*, max. 10mm2)	Versnipperen (vernietigingsklasse O5*, max. 10mm2) en verbranden
Tapes	Versnipperen	Versnipperen (vernietigingsklasse T4*, max. 160mm2)	Versnipperen (vernietigingsklasse T5*, max. 30mm2)	Versnipperen (vernietigingsklasse T5*, max. 30mm2) en verbanden
Harde schijf	Doorboren	Versnipperen (vernietigingsklasse H4*, max. 2000mm2)	Versnipperen (vernietigingsklasse H5*, max. 320mm2)	Versnipperen (vernietigingsklasse H5*, max. 320mm2) en verbanden
USB stick	Doorboren	Versnipperen (vernietigingsklasse E4*, max. 30mm2)	Versnipperen (vernietigingsklasse E5*, max. 10mm2)	Versnipperen (vernietigingsklasse E5*, max. 10mm2) en verbranden
Overig	Breken	Versnipperen	Versnipperen	Versnipperen en verbranden

*Conform DIN 66399

BIJLAGE 9: GOEDGEKEURDE MIDDELEN

In verschillende eisen wordt verwezen naar het gebruik van *Goedgekeurde Middelen*. In veel gevallen gaat het hier over *Cryptografische beveiligingsoplossingen* of specifieke software voor het beveiligen van verbindingen. Voor zowel een Nederlandse als internationale *Bijzondere Opdracht* wordt een limitatieve selectie van geëvalueerde producten gehanteerd. De inzet van deze *Middelen* is enkel toegestaan bij gebruik van de geëvalueerde versie en volledige naleving van het inzetadvies. Dit inzetadvies kan via *NBIV* worden opgevraagd.

Internationaal

Voor internationale *Bijzondere Opdrachten* geldt dat geëvalueerde producten worden gebruikt, bijvoorbeeld vanuit de *NAVO* of *EU* of op basis van internationale verdragen (*MoU,* GSA). Inzet van deze *Middelen* gebeurt te allen tijde in afstemming met *NBIV*.

Nationaal

Voor alle *Rubriceringsniveaus* is de lijst met geëvalueerde producten van de Unit Weerbaarheid van de *AIVD* leidend. De lijst van de Unit Weerbaarheid is op de website van de *AIVD* beschikbaar.

In bepaalde situaties kan het voorkomen dat de selectie van geëvalueerde producten ontoereikend is. In uitzonderlijke gevallen kan een aanvraag worden ingediend via *NBIV* om onder strikte voorwaarden te komen tot de goedkeuring voor het gebruik van een niet-geëvalueerd product. Daarnaast dient er te worden voldaan aan de van toepassing zijnde *ABRO*-eisen, zoals dat de producten niet voortkomen uit, noch afhankelijk zijn van landen met een gekend *Offensief cyber-programma* tegen de Nederlandse Staat.

BIJLAGE 10: SCRUBBER

Doel van een Scrubber

Verwijderbare gegevensdragers worden voor gebruik gecontroleerd met een speciaal voor dit doel ingerichte *Scrubber.* Een *Scrubber* is een losstaand *Systeem* dat *Verwijderbare gegevensdragers* controleert op de aanwezigheid van *Malware* en deze zo nodig in quarantaine plaatst.

Een *Scrubber* voldoet minimaal aan de volgende eigenschappen:

- Het is een volledig geïsoleerd systeem, zonder enige verbinding met andere *Netwerken*, en alle draadloze verbindingen zijn uitgeschakeld;
- Het is beveiligd op het niveau van het hoogste *Rubriceringsniveau* van de data;
- Er wordt geen data achtergelaten op een *Scrubber* wat betekent dat data na verwerking volledig wordt verwijderd;
- Er worden minimaal 2 verschillende typen anti-*Malware* software gebruikt die anders zijn dan anti-*Malware* software die is toegepast in het *Netwerk* waarop de *Verwijderbare gegevensdrager* uiteindelijk wordt gebruikt;
- De gebruikte indicatoren, zoals virusdefinities en *Signatures,* zijn maximaal 7 dagen oud en er is een proces beschreven om deze indicatoren tijdig te vernieuwen.

Wanneer deze vernieuwing niet wordt uitgevoerd, dan wordt de *Scrubber*, totdat de virusdefinities en *Signatures* vernieuwd zijn, uitgeschakeld en wordt gebruik onmogelijk gemaakt. Bij detectie van *Malware* wordt de *(Cyber-)Beveiligingsfunctionaris* geïnformeerd.

Praktische voorbeelden van werking

Onderstaand worden een aantal voorbeeldsituatie beschreven voor het gebruik van een *Scrubber*:

1. Wanneer een goedgekeurde USB-stick binnenkomt, wordt deze eerst ontsleuteld en gescand door de *Scrubber* voordat deze in een *Netwerk* met *Te Beschermen Belangen* wordt geplaatst. Vervolgens wordt de USB-stick naar het *Vertrouwde Netwerk* verplaatst.

2. Wanneer een versleuteld bestand binnenkomt via een onvertrouwd *Netwerk*, wordt het eerst op de *Scrubber* ontsleuteld en gescand. Vervolgens wordt het bestand op een goedgekeurde USB-stick verplaatst naar een *Vertrouwd Netwerk*.

3. Wanneer data verstuurd wordt, is het aanbevolen om deze eerst door de *Scrubber* te laten scannen voordat deze op een goedgekeurde USB-stick wordt geplaatst.

BIJLAGE 11: CLOUD

Hoofdstuk 5 beschrijft de eisen die specifiek van toepassing zijn op *Cloudoplossingen*. Daarnaast zijn er ook een aantal specifieke eisen uit H3 en H4 van toepassing op *Cloudoplossingen*. Deze zijn opgenomen in de onderstaande tabel.

Relevante eisen voor Cloudoplossingen uit H3 en H4

	Hoofdstuk 3 - Fysiek	Hoofdstuk 4 - Cyber
Specifieke eisen	3.1.10 3.1.11 3.1.12 3.1.13	4.5.20 4.13.8 4.13.9 4.15.20
Paragraaf*		4.6 Endpoint beveiliging 4.7 Beheer van mobiele apparatuur 4.8 Cryptografie

* Cryptografie, Endpoint beveiliging en Beheer van mobiele apparatuur

Afhankelijk van de exacte inrichting van de te leveren *Clouddienst* zijn ook de voorgeschreven eisen in de paragrafen Cryptografie, Endpoint beveiliging en Beheer van mobiele apparatuur uit H4 van toepassing.

- De eisen die voorgeschreven zijn in de sectie Cryptografie zijn van toepassing op een *Cloudoplossing* wanneer *CSP* verantwoordelijk is voor sleutelbeheer.
- De eisen die voorgeschreven zijn in de sectie Endpoint beveiliging en Beheer van *Mobiele apparatuur* zijn van toepassing op een *Cloudoplossing* wanneer de werkstations of *Mobiele apparatuur* die door *Opdrachtgever* gebruikt worden om de *Cloudoplossing* te gebruiken niet beheerd worden door *Opdrachtgever.*

Dit document is een uitgave van:

Rijksoverheid

Januari 2026