

Ongerubriceerd en ongemerkt

ABDO

Ministerie van Defensie

**In de tekst gecursiveerd opgenomen afkortingen en begrippen worden
in hoofdstuk 5 nader verklaard.**

Voorwoord

Regelmatig blijkt dat buitenstaanders grote interesse hebben in kennis, informatie, materieel, goederen en objecten van het Ministerie van Defensie en de kennisinstituten en bedrijven die voor Defensie werken. Onoorbare praktijken en heimelijke middelen worden niet geschuwd om te trachten hierop de hand te leggen of hieromtrent gegevens te vergaren. Het is dus noodzakelijk een en ander goed te beveiligen.

Ook uw organisatie beschikt over waardevolle zaken die u niet wilt prijsgeven aan onbevoegden. Helaas is niet iedereen zich daarvan in voldoende mate bewust en dat, in combinatie met een (te) laag niveau van beveiliging, maakt een organisatie kwetsbaar. De beveiliging van kennis, informatie, materieel en goederen, alsmede van het object waar e.e.a. wordt geproduceerd, verwerkt dan wel opgeslagen, verdient dan ook de nodige aandacht.

Onder andere het Voorschrift Informatiebeveiliging Rijksdienst (VIR) geeft regels voor de beveiliging van (bijzondere) Informatie bij de Rijksoverheid, opdat ongewenste verspreiding van en onrechtmatige toegang tot die informatie wordt voorkomen. Ook wordt beschreven hoe te handelen indien zich een beveiligingsincident heeft voorgedaan. Voor ieder ministerie zijn deze regels nader uitgewerkt in beveiligingsbeleid. Voor Defensie is dat het Defensie Beveiligingsbeleid (DBB).

De werking van het VIR en andere voorschriften is in beginsel beperkt tot de Rijksoverheid. Het kan echter noodzakelijk zijn de betreffende informatie, materieel, goederen of zelfs een object – met andere woorden een Te Beschermen Belang (TBB) – buiten het Ministerie van Defensie te brengen,

bijvoorbeeld bij een bedrijf dat een TBB nodig heeft voor de uitvoering van een contract. Dit is alleen toegestaan als voldoende zekerheid bestaat dat een adequate beveiliging is gewaarborgd. Dit document bevat de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO), die Defensie oplegt aan instellingen en bedrijven met betrekking tot het beveiligen van een TBB. De ABDO 2017 zijn een afgeleide van de eerder genoemde regelgeving, waar nodig aangevuld met nieuwe algemene beveiligingseisen en uitvoeringsbepalingen.

De volledig herziene ABDO 2017 vervangen de ABDO 2006 en zijn ten opzichte daarvan ingrijpend gewijzigd. Vooral het hoofdstuk over IT-beveiliging is, gezien de toegenomen dreiging, fors uitgebreid en aangepast aan de huidige technologische ontwikkelingen. De toegankelijkheid is verbeterd door de modulaire opzet. Daarmee voorziet de ABDO 2017 in de behoefte van het Ministerie van Defensie aan een modern stelsel van beveiligingseisen. Toepassing daarvan draagt bij aan adequate beveiliging van niet alleen het overgedragen TBB van het Ministerie van Defensie, maar ook van de bedrijfseigen “kroonjuwelen”.

De ABDO 2017 treden in werking per 1 juni 2017.

Namens de minister van Defensie,
de Hoofddirecteur Bedrijfsvoering/Beveiligingsautoriteit,



Ir. M.G.L.H. Tossings
Schout-bij-nacht

Inhoudsopgave

Voorwoord	2
Algemeen	4
1. Bestuur en organisatie.....	10
Inleiding.....	10
Eisen	11
2. Personeel	17
Inleiding	17
Eisen	18
3. Fysiek	21
Inleiding.....	21
Eisen 22	
4. Cyber.....	33
Inleiding.....	33
Eisen	34
5. Verklaring gebruikte afkortingen en begrippen..	55
6. Inhoudsopgave bijlagen.....	65

Algemeen

1 *Te Beschermen Belangen*

Onder alle omstandigheden moet men kunnen rekenen op de betrouwbaarheid (*Beschikbaarheid, Integriteit, Vertrouwelijkheid*) van personeel, *Informatie, Materieel, Goederen* en *Objecten*. Deze staan echter voortdurend bloot aan dreigingen zoals criminaliteit, extremisme, sabotage, terrorisme en spionage. Economische, strategische, militaire en technisch wetenschappelijke spionage vormen een actuele dreiging. Vitale sectoren zoals energie en telecommunicatie kunnen worden getroffen door (digitale) extremistische of terroristische aanslagen.

Beveiligingsmaatregelen dragen bij aan de weerstand tegen deze dreigingen. Het niveau van de maatregelen hangt af van de aard van de *Informatie*, het *Materieel*, de *Goederen* en de *Objecten* in relatie tot de specifieke dreiging. Het Ministerie van Defensie hanteert daartoe een *Rubricering-* en *Merking*-systeem. Defensie heeft alle te beschermen *Informatie, Materieel, Goederen* en *Objecten* ingedeeld in vier categorieën *Te Beschermen Belang (TBB)*, met *TBB 1* als strengst te *Beveiligen* categorie).

2 *Risicomanagement ABDO*

Het doel van risicomanagement is het identificeren van dreigingen jegens een TBB, het onderkennen van de daaraan verbonden risico's en deze risico's vervolgens door beveiligingsmaatregelen wegnemen of tot een aanvaardbaar restrisico reduceren.

Hierbij wordt risico gedefinieerd als het product van de kans dat een dreiging zich daadwerkelijk manifesteert en het effect daarvan op het voortzettingsvermogen van Defensie. Kortweg: $\text{risico} = \text{kans} \times \text{effect}$.

Voor de vaststelling van het restrisico heeft Defensie alle *Informatie, Materieel, Goederen* en *Objecten* op basis van een risicoanalyse ingedeeld in TBB. Op basis van de door Defensie gestelde betrouwbaarheidseisen, de ingeschatte dreiging en een kosten/baten afweging is in de *ABDO 2017* per TBB-categorie een set beveiligingsmaatregelen opgenomen die moet voorkomen dat bedrijfsprocessen van Defensie stagneren en dat de Staat of zijn bondgenoten onaanvaardbare schade lijden.

Omdat omstandigheden en dreigingen voortdurend aan wijzigingen onderhevig zijn, is risicomanagement een cyclisch proces. Dergelijke wijzigingen kunnen aanleiding zijn het beveiligingsniveau bij te stellen. Afhankelijk van het bedrijf, de aard van opdracht en de locatie kunnen andere combinaties van maatregelen nodig zijn om aan hetzelfde niveau van beveiliging te voldoen. *BIV / MIVD* geeft per situatie aan welke eisen van toepassing zijn en welke maatregelen dienen te worden genomen.

3 *Bijzondere Informatie en Informatie voorzien van een Merking*

Informatie die is voorzien van een *Rubricering* wordt *Bijzondere Informatie (BI)* genoemd. *BI* wordt onderscheiden in Staatsgeheime en niet-Staatsgeheime *BI*. Er is sprake van een Staatsgeheim als belangen van de Staat of zijn bondgenoten in het geding zijn en indien kennisname door niet-gerechtigden kan leiden tot schade aan deze belangen. Er is sprake van niet-Staatsgeheime *BI* indien kennisname door niet-gerechtigden kan leiden tot nadeel voor het belang van één of meer ministeries. Ook *BI* valt, afhankelijk van de hoogte van de *Rubricering*, in een *TBB*-categorie.

In de volgende tabel zijn de vier mogelijke *Rubriceringen* opgenomen met de overeenkomstige *TBB*-categorie. Informatie die van één van deze *Rubriceringen* is voorzien, wordt *BI* genoemd. Opgemerkt wordt dat, in tegenstelling tot *BI*, een *TBB* niet gerubriceerd hoeft te zijn.

NL Rubricering	TBB categorie	Betekenis
Stg. ZEER GEHEIM	TBB 1	Kennisname door niet-gerechtigden kan zeer ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.
Stg. GEHEIM	TBB 2	Kennisname door niet-gerechtigden kan ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.
Stg. CONFIDENTIEEL	TBB 3	Kennisname door niet-gerechtigden kan schade toebrengen aan het belang van de Staat of zijn bondgenoten.
DEPARTEMENTAAL VERTROUWELIJK	TBB 4	Kennisname door niet-gerechtigden kan nadeel toebrengen aan het belang van één of meer ministeries.

Informatie kan ook zijn voorzien van een *Merking* (al dan niet in combinatie met een *Rubricering*). Een *Merking* heeft als doel de kring van tot kennisname gerechtigden te beperken tot een specifieke groep. Ook kan een *Merking* een specifieke behandeling en beveiliging tot doel hebben. **Bijlage 1** bevat een tabel met de meest voorkomende *Merkingen* en hun betekenis, gekoppeld aan de *TBB*-categorie. Ongerubriceerde *Informatie* van Defensie die wel voorzien is van een *Merking* (zoals Intern Gebruik Defensie, Intern Beraad, NLD -Eyes - Only) dient als *TBB 4* te worden beveiligd. Ongerubriceerde en ongemerkte informatie dient te worden behandeld op basis van “Need-to-Know”.

Een verzameling ter beschikking gestelde, personeelsgevoelige (bijvoorbeeld medische gegevens, of gegevens over operationele inzetbaarheid van personeel) *Informatie* dient minimaal als *TBB 4* te worden beveiligd. Indien het gaat om een grote verzameling van gerubriceerde en/of gemerkte *Informatie*, kan hieraan een (hogere) *TBB* worden toegekend, en dus *TBB 4* overstijgen. De schade die bij *Compromittatie* van de verzameling ontstaat, is immers groter dan bij *Compromittatie* van een enkelvoudig gegeven.

Informatie, *Materieel*, *Goederen* en *Objecten* kunnen ook een *Vitaal* karakter hebben. Op grond daarvan kan een *TBB*-categorie worden toegekend ook zonder dat sprake is van een *Rubricering* of *Merking*. Een niet correcte uitvoering van de in de *ABDO 2017* gestelde eisen heeft nadelige invloed op de bedrijfsvoering van het Ministerie van Defensie, Staat of zijn bondgenoten en veroorzaakt schade aan de veiligheid of overige gewichtige belangen van de Staat.

4 Bijzondere Opdrachten

Aan productie, behandeling, verwerking, opslag en vernietiging van een *TBB* worden specifieke beveiligingseisen gesteld. Indien het voor een goede uitvoering van een opdracht noodzakelijk is een dergelijk *TBB* vanuit Defensie (de *Opdrachtgever*) over te dragen aan een bedrijf (de *Opdrachtnemer*), of wanneer wordt voorzien dat de *Opdrachtnemer* zelf een *TBB* bezit of genereert, is sprake van een *Bijzondere Opdracht (BO)*. Overdracht van een *TBB* kan op vele manieren plaatsvinden: mondeling, schriftelijk, digitaal of *Materieel*. Er dient te worden gewaarborgd dat bij de *Opdrachtnemer* het juiste beveiligingsregime wordt toegepast. Bij een *BO* wordt de *Opdrachtnemer* contractueel verplicht tot implementatie van beveiligingsmaatregelen als beschreven in deze *ABDO 2017*.

5 Advies en controle

In de *Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv)*¹ artikel 7 is de *Militaire Inlichtingen- en Veiligheidsdienst (MIVD)* aangewezen maatregelen te treffen ter bescherming van *TBB* van Defensie, waarvan de *Compromittatie* de krijgsmacht of zijn bondgenoten kan schaden. Bij de *MIVD* is het *Bureau Industrieveiligheid (BIV)* verantwoordelijk voor controle op de uitvoering van de vereiste beveiliging bevorderende maatregelen bij *Opdrachtnemers* in het kader van een *BO*. Hiertoe brengt *BIV / MIVD* op meerdere momenten een bezoek aan de *Opdrachtnemers*, die verplicht zijn medewerking te verlenen, met als doel:

- inschakeling en autorisatie: op verzoek van de inkoper van Defensie beoordeelt *BIV / MIVD* of een potentiële *Opdrachtnemer* bereid en in staat is te voldoen aan *ABDO 2017*. Bij voorgenomen gunning volgt controle op implementatie en toereikendheid van de beveiligingsmaatregelen. Bij positieve beoordeling wordt de inkoper geautoriseerd tot gunning van het contract. Het bedrijf is daarmee geautoriseerd om *TBB* op te slaan en te verwerken. Deze autorisatie wordt, op enkele uitzonderingen na, per contract verleend en is derhalve geen algemene autorisatie. Een uitgebreide beschrijving van het inkoopproces is opgenomen in de leidraad “**procedure ABDO**”;
- advies: *BIV / MIVD* adviseert over de maatregelen die moeten worden getroffen om te voldoen aan de minimale beveiligingseisen van de *ABDO 2017*;

- controle: *BIV / MIVD* bezoekt de *Opdrachtnemer*, al dan niet aangekondigd, voor een tussentijdse beoordeling van de implementatie van de beveiligingsmaatregelen en beoordeelt of aan de gestelde normen is voldaan;
- audit: *BIV / MIVD* voert vooraf aangekondigd een formele integrale audit uit op de implementatie en toereikendheid van de beveiligingsmaatregelen. De resultaten worden vastgelegd in een auditrapport dat wordt vastgesteld door de Directeur *MIVD*;
- onderzoek: na melding van een (mogelijk) *Beveiligingsincident* verricht *BIV / MIVD* onderzoek naar mogelijke *Compromittatie* van een *TBB* en de gevolgen daarvan met als doel de schade te beperken en herhaling te voorkomen.

In het kader van een *BO* van *NAVO* of *EU* voeren ook deze organisaties reguliere inspecties uit. Een *Opdrachtnemer* is verplicht ook daaraan medewerking te verlenen.

6 Access to Site

Het is mogelijk dat aan medewerkers van een *Opdrachtnemer*, hoewel niet geplaatst op een *Vertrouwensfunctie*, frequent toegang moet worden verleend tot locaties, compartiment of systemen waar zich al dan niet gerubriceerde *TBB* bevinden. Het Ministerie van Defensie kan in zulke gevallen toch de *ABDO 2017* bedingen en tot *Screening* van de betrokken medewerkers overgaan.

¹ Momenteel wordt er gewerkt aan een nieuwe WIV. Zodra deze is afgerond, is de nieuwe WIV van toepassing.

7 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 *TBB* 1-niveau beveiligd. Personeel dat toegang moet hebben (*Need-to-be*), dient te beschikken over een *Veiligheidsmachtigingsniveau* dat overeenkomt met de hoogst aanwezige *Rubricering*.

8 Buitenlandse opdrachten

Bedrijven kunnen ook in aanmerking komen voor een *BO* van *NAVO*, *EU* of een buitenlandse overheid. Naast nationale *TBB* kan derhalve sprake zijn van *NAVO*-, *EU*- of buitenlandse *TBB*. Bij aan Defensie gerelateerde opdrachten treedt *BIV* / *MIVD* naar het betrokken bedrijf op als de aangewezen beveiligingsautoriteit namens die organisaties en landen. Bij civiele opdrachten vervult de *AIVD* die rol. Vaak is daarbij de voorwaarde dat daarover afspraken zijn vastgelegd in een Beveiligingsverdrag of een zogeheten *Memorandum of Understanding (MoU)*. *BIV* / *MIVD* vervult dan de rol van *Designated Security Authority (DSA)*.

9 Internationale Rubriceringen

In de tabel in **bijlage 2** zijn de met de nationale *Rubricering* overeenkomstige *NAVO*- en *EU-Rubriceringen* opgenomen, alsmede de meest voorkomende buitenlandse, nationale *Rubriceringen*. Voor internationaal gebruik kan de Nederlandse *Rubricering* eventueel worden uitgebreid met de internationaal meer bekende Engelstalige rubriceringsaanduiding, zoals *NLD CONFIDENTIAL* in aanvulling op *Stg. CONFIDENTIEEL*. Zie hiervoor tevens **bijlage 2**.

10 Export Controle

Indien bij een opdracht *Informatie*, *Materieel* en/of *Goederen* zijn betrokken die onderworpen zijn aan exportcontrolebeleid van het land van herkomst, kunnen separaat of aanvullend beveiligingseisen worden gesteld. Zo worden in het kader van een opdracht waarbij *Informatie*, *Materieel* en/of *Goederen* zijn betrokken die vallen onder de Amerikaanse wet- en regelgeving voor exportcontrole zoals de *International Traffic of Arms Regulations (ITAR)*, separaat beveiligingseisen gesteld. Dergelijke *Informatie*, *Materieel* en/of *Goederen* vallen doorgaans in de categorie *Controlled Unclassified Information /Item (CUI)*. Veelal worden hier door het betrokken bedrijf rechtstreeks afspraken gemaakt met de (buitenlandse) *Opdrachtgever* in een *Technical Assistance Agreement*. De *ABDO* 2017 zijn hierop feitelijk niet van toepassing maar kunnen wel een handvat bieden voor het beoogde beveiligingsregime. Als de opdracht wordt verstrekt door Defensie is de *ABDO* 2017 wel van toepassing op minimaal *TBB* 4 niveau.

11 Octrooien

Indien uit een *BO* een vinding voortvloeit waarop naar mening van de *Opdrachtnemer* octrooi moet worden aangevraagd, dient hij, alvorens daartoe over te gaan, de *Opdrachtgever* en *BIV* / *MIVD* hiervan in kennis te stellen. Mogelijk wordt aan de octrooiaanvraag, gezien het militaire karakter, een *Rubricering* toegekend (conform Hoofdstuk 2, paragraaf 3, artikel 40 - 46 van de Rijksoctrooiwet 1995). Alle aan de octrooiaanvraag gerelateerde *BI* dient conform de *ABDO* 2017 te worden beveiligd. Ook het octrooigemachtigde bureau waar de gerubriceerde octrooiaanvraag wordt ingediend, dient aan de *ABDO* 2017 te voldoen.

Het is ook mogelijk dat Defensie het octrooi aanvraagt, bijvoorbeeld als het intellectueel eigendom van de vinding bij Defensie berust.

12 Escrow

Als *BI* wordt gedeponereerd bij een door Defensie aangewezen *Escrow Agent* dient ook deze aan de *ABDO* 2017 te voldoen.

13 Verantwoording

De *ABDO* 2017 is mede gebaseerd op nationale en internationale wet- en regelgeving, zoals de voorschriften van de *NAVO* en de *EU* voor de beveiliging van gerubriceerde *Informatie*, *Defensiebeveiligingsbeleid (DBB)*, de *Wet op de inlichtingen- en veiligheidsdiensten 2002*, de *Wet veiligheidsonderzoeken*, de *Wet bescherming staatsgeheimen* en de *Archiefwet 1995*.

14 Tussentijdse wijziging van de eisen

Omstandigheden en dreigingen zijn voortdurend aan wijzigingen onderhevig. Dergelijke wijzigingen kunnen aanleiding zijn het beveiligingsniveau tijdens de uitvoering van het contract bij te stellen en nadere eisen te stellen. Over de eventuele gevolgen daarvan (kosten, termijnen) dient nader overleg plaats te vinden tussen *Opdrachtgever* en *Opdrachtnemer*.

15 Sancties

De *ABDO* 2017 vormen een integraal onderdeel van het contract tussen *Opdrachtgever* en *Opdrachtnemer*. Het niet naleven van de in de *ABDO*

2017 gestelde beveiligingseisen wordt derhalve als contractbreuk beschouwd. Dit kan leiden tot opschorting of intrekking van de verleende autorisatie tot verwerken en opslaan van *TBB*, hetgeen beëindiging van het contract tot gevolg kan hebben. Indien het niet naleven valt terug te voeren op een bepaald persoon kan intrekking van diens *Verklaring van Geen Bezwaar (VGB)* het gevolg zijn. Bij beëindiging van het contract dient het *TBB* te worden ingeleverd of vernietigd. Het moedwillig achterhouden of verstrekken of ter beschikkingstellen van een *TBB* aan een niet-gerechtigde, is een strafbaar feit conform het gestelde in het *Wetboek van strafrecht* (artikel 98, 98a, 98b, 98c, 272 en 273).

16 Overgangsregeling (ABDO 2006 naar ABDO 2017)

Met het in werking treden van deze *ABDO* 2017 worden de *ABDO* 2006 geheel vervangen. Dat betekent dat voor nieuwe contracten, sub-contracten, projecten, deelprojecten, opdrachten onder raamcontract etc. waarop de *ABDO* van toepassing zijn, onder *ABDO* de *ABDO* 2017 dient te worden verstaan. Op bestaande contracten blijven dus de *ABDO* 2006 van toepassing.

17 Aanhaling van de ABDO 2017

Deze beveiligingseisen kunnen worden aangehaald als '*Algemene Beveiligingseisen voor Defensieopdrachten 2017*', afgekort *ABDO* 2017.

18 Leeswijzer

Deze *ABDO* 2017 bevat de eisen voor de beveiliging van een *TBB* waaraan voldaan moet zijn. Op basis van risico inschatting kunnen de eisen proportioneel worden toegepast. Dit kan betekenen dat er een andere,

bijvoorbeeld minder stringente invulling aan een eis wordt gegeven dan letterlijk voorgeschreven. *BIV / MIVD* besluit hierover.

De eisen hebben betrekking op vier deelgebieden: bestuur en organisatie, personeel, fysiek en cyber. In de volgende hoofdstukken zijn de eisen per deelgebied in een kader verwoord. Waar nodig zijn eisen nader toegelicht of uitgewerkt in een bijlage. Bij tegenstrijdigheid tussen de eis in de tabel en de tekst in inleiding of bijlage prevaleert de eis in de tabel.

De van toepassing zijnde eisen worden aangegeven door een gesloten bolletje (●) in de kolom onder de van toepassing zijnde (hoogste) *Rubricering* of *TBB*-categorie. Als zich in deze kolom een open bolletje (○) bevindt, dient in overleg met *BIV / MIVD* te worden bepaald of, respectievelijk in welke mate, aan de eis moet worden voldaan.

1 Bestuur en Organisatie

Inleiding

Bescherming van een *Te Beschermen Belang (TBB)* begint met een breed gedragen en structureel gehandhaafd beveiligingsbeleid, bekrachtigd door het hoogste bestuursorgaan. Het vervolgens opgestelde beveiligingsplan en de implementatie van adequate beveiligingsmaatregelen vormen de basis voor succesvolle beveiliging. Daarbij is beveiligingsbewustzijn van groot belang. Pas als de gehele organisatie, van hoog tot laag, is doordrongen van de waarde van een *TBB*, kan een bedrijfscultuur ontstaan waarin een *TBB* ook daadwerkelijk door alle medewerkers als zodanig wordt behandeld. Daarbij moet zijn inbegrepen het besef dat *Disclosure* aan derden of publicatie van een *TBB* niet is toegestaan.

Veel aandacht is er in dit hoofdstuk voor bedrijfsstructuur, eigendom en *Zeggenschap* omdat hierdoor ongewenste invloed op het bedrijf en daarmee op de behandeling van een *TBB* mogelijk is. Een dergelijke invloed kan ook ontstaan als *Bijzondere Informatie (BI)* toegankelijk is voor personen met uitsluitend een andere dan de Nederlandse nationaliteit.

Voorts is het van belang dat in het kader van een *Bijzondere Opdracht (BO)* de gehele logistieke keten, inclusief *(Toe)Leveranciers* inzichtelijk is. Ook via levering van op zich onschuldige componenten of onderdelen is immers invloed op de te leveren dienst of het te leveren product mogelijk.

Tenslotte besteedt dit hoofdstuk aandacht aan de afhandeling van *Beveiligingsincidenten*.

Ook met betrekking tot bestuur en organisatie moet worden voldaan aan een aantal beveiligingseisen. Deze eisen zijn in het kader vanaf de volgende pagina verwoord. Waar nodig zijn eisen nader toegelicht of uitgewerkt in een bijlage. Bij tegenstrijdigheid tussen de eis in de tabel en de tekst in inleiding of bijlage prevaleert de eis in de tabel.

Deze *ABDO 2017* bevat de eisen voor de beveiliging van een *TBB* waaraan voldaan moet zijn. Op basis van risico inschatting kunnen de eisen proportioneel worden toegepast. Dit kan betekenen dat er een andere, bijvoorbeeld minder stringente invulling aan een eis wordt gegeven dan letterlijk voorgeschreven. *BIV / MIVD* besluit hierover.

De van toepassing zijnde eisen worden aangegeven door een gesloten bolletje (●) in de kolom onder de van toepassing zijnde (hoogste) *Rubricering* of *TBB*-categorie. Als zich in deze kolom een open bolletje (○) bevindt, bepaalt *BIV / MIVD* na overleg met de *Opdrachtnemer* of, respectievelijk in welke mate, aan de eis moet worden voldaan.

ABDO 2017 eisen						
HOOFDSTUK 1 BESTUUR EN ORGANISATIE			BEVEILIGINGSREGIME			
1.1	Algemeen	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	Opdrachtnemer voldoet aan de eisen van de ABDO 2017 aangaande de gerelateerde <i>Gerubriceerde Opdracht</i> .	Procedure ABDO	●	●	●	●
2	Bij beëindiging van het contract vervallen alle bijbehorende autorisaties, de LvV en de VGB. Hieraan voorafgaand dient de <i>Opdrachtnemer</i> de door <i>Opdrachtgever</i> verstrekte TBB te retourneren tenzij <i>Opdrachtgever</i> , eventueel in overleg met <i>BIV / MIVD</i> , schriftelijk toestemming heeft verleend de TBB te vernietigen of te behouden.	Procedure ABDO	●	●	●	●
1.2	Inrichten van de beveiligingsorganisatie	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	<i>Opdrachtnemer</i> beschikt over een organisatiebreed, structureel gehandhaafd en breed gedragen beveiligingsbeleid, bekrachtigd door het hoogste bestuursorgaan.	Bijlage 3	●	●	●	●
2	<i>Opdrachtnemer</i> beschikt over een beveiligingsplan, opgesteld door de <i>BF</i> , goedgekeurd door <i>BIV / MIVD</i> en ondertekend door het hoogste bestuur, waarin de beveiligingseisen uit de ABDO 2017 zijn uitgewerkt in duidelijke, hanteerbare maatregelen en procedures.	Bijlage: 3	●	●	●	●
3	<i>Opdrachtnemer</i> heeft de in het beveiligingsplan beschreven maatregelen en procedures eenduidig geïmplementeerd in de organisatie.	Bijlage 3	●	●	●	●
4	<i>Opdrachtnemer</i> heeft, met voorafgaande schriftelijke instemming van <i>BIV / MIVD</i> , een <i>beveiligingsfunctionaris (BF)</i> benoemd en zonodig één of meerdere sub- <i>BF</i> 'n, afhankelijk van de omvang van de <i>BO</i> , het aantal betrokken locaties en specialismen.	Bijlage 3	●	●	●	●

5	De <i>BF</i> beschikt ten minste over: - de Nederlandse nationaliteit en is in dienst van het desbetreffende bedrijf; - voldoende autonomie, bevoegdheden, slagkracht en senioriteit; - een <i>Verklaring Omtrent Gedrag (VOG)</i> of een <i>Verklaring van Geen Bezwaar (VGB)</i> op het hoogst geldende rubriceringsniveau van de <i>BO</i>; - rechtstreekse en onafhankelijke toegang tot alle bestuursorganen binnen de organisatie.	Bijlage 4	●	●	●	●
1.3	De Beveiligingsfunctionaris	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	De <i>BF</i> is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de <i>Opdrachtnemer</i> .	Bijlage 4	●	●	●	●
2	De <i>BF</i> toetst periodiek, doch minimaal eenmaal per jaar, het beveiligingsplan aan de praktijk. De resultaten hiervan zijn schriftelijk vastgelegd en aan het bestuur, in afschrift aan BIV / MIVD, gerapporteerd. Zonodig wordt het beveiligingsplan geactualiseerd.	Bijlage 3 en 37	●	●	●	●
3	(Beleids)wijzigingen die impact hebben op het security beleid van het bedrijf zijn aan BIV / MIVD ter beoordeling verstrekt en zijn verwerkt in het beveiligingsplan.	Bijlage 4	●	●	●	●
4	Noodzakelijke wijzigingen n.a.v. een verhoogd dreigingsbeeld of een <i>Beveiligingsincident</i> , zijn vastgelegd in het beveiligingsplan binnen de door BIV / MIVD gestelde termijn.	Bijlage 3 en 4	○	○	○	○
5	De <i>BF</i> draagt zorg voor volledige medewerking bij controles, audits en onderzoeken bij <i>Opdrachtnemer</i> door BIV / MIVD.	Bijlage 4	●	●	●	●
6	De <i>BF</i> stelt zich door middel van het onderhouden van contacten met de gemeente, omliggende bedrijven en de politie op de hoogte van zaken die de lokale beveiliging aangaan.	Bijlage 4	●	●	●	○
7	De <i>BF</i> voert voorts de taken uit als beschreven in bijlage 4: Taken en verantwoordelijkheden <i>BF</i> .	Bijlage 4	●	●	●	●

1.4	Zeggenschap en bedrijfsstructuur	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
Een melding van een <i>Opdrachtnemer</i> ten aanzien van de eisen van 1.4 kan aanleiding geven dit formeel schriftelijk aan de Directeur MIVD ter besluitvorming voor te leggen. Dit is ter beoordeling van BIV / MIVD.						
1	<i>Opdrachtnemer</i> heeft ten behoeve van de autorisatie een Verklaring van Eigendom, Zeggenschap en bedrijfsstructuur opgesteld en ter beschikking gesteld aan BIV / MIVD.	Bijlage 5	●	●	●	●
2	<i>Opdrachtnemer</i> meldt elke voorgenomen wijziging in eigendom/aandeelhouderschap van het bedrijf terstond schriftelijk aan BIV / MIVD.	Bijlage 5	●	●	●	●
3	<i>Opdrachtnemer</i> meldt voorgenomen wijzigingen in Zeggenschap, eigendom en aandeelhouderschap waarbij deze grotendeels of geheel in handen komt van één natuurlijke of rechtspersoon, of van één of meerdere buitenlandse natuurlijke of rechtspersonen, terstond schriftelijk aan BIV / MIVD.	Bijlage 5	●	●	●	●
4	<i>Opdrachtnemer</i> meldt voorgenomen benoemingen van bestuurders die niet beschikken over de Nederlandse nationaliteit, terstond schriftelijk aan BIV / MIVD.	Bijlage 5	●	●	●	●
5	<i>Opdrachtnemer</i> meldt voorgenomen samenwerking met buitenlandse bedrijven of overheden, terstond schriftelijk aan BIV / MIVD.	Bijlage 5	●	●	●	●
6	<i>Opdrachtnemer</i> meldt voorgenomen splitsing, strategische samenwerking of fusie, dreigende gedeeltelijke danwel volledige overname, bedrijfsbeëindiging, surseance van betaling of faillissement terstond schriftelijk aan BIV / MIVD.	Bijlage 5	●	●	●	●
7	<i>Opdrachtnemer</i> meldt voorgenomen wijziging van bedrijfsactiviteiten, locaties, sourcing, fusies of gedeeltelijke dan wel volledige overname terstond schriftelijk aan BIV / MIVD.	Bijlage 5	●	●	●	●
8	<i>Opdrachtnemer</i> verschaft duidelijkheid bij welk (onderdeel van het) bedrijf en op welke locatie de BO wordt belegd en streeft maximaal naar onderbrenging van alle BO bij één duidelijk herkenbaar en juridisch en organisatorisch af te schermen (onderdeel van het) bedrijf.	Bijlage 5	●	●	●	●
9	<i>Opdrachtnemer</i> is een Nederlands Rechtspersoon in geval van een BO waarbij een grote hoeveelheid (te bepalen door BIV / MIVD in overleg met <i>Opdrachtgever</i>) Bijzondere Informatie (BI) is overgedragen.	Bijlage 5	●	●	●	○

10	<i>Opdrachtnemer</i> garandeert dat een grote hoeveelheid <i>BI</i> (te bepalen door <i>BIV / MIVD</i> in overleg met <i>Opdrachtgever</i>) slechts op Nederlands grondgebied wordt gegenereerd, bewerkt en opgeslagen.	Bijlage 5	●	●	●	●
11	<i>Opdrachtnemer</i> plaatst slechts medewerkers met de Nederlandse nationaliteit op <i>Vertrouwensfuncties</i> waarbij toegang tot een grote hoeveelheid <i>BI</i> (te bepalen door <i>BIV / MIVD</i> in overleg met <i>Opdrachtgever</i>) is vereist.	Bijlage 5	●	●	●	○
1.5	Beveiligingsbewustzijn	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	<i>Opdrachtnemer</i> voert een programma uit ter bevordering van het beveiligingsbewustzijn waarbij deelname verplicht en meetbaar is.	Bijlage 6	●	●	●	●
2	De <i>BF</i> geeft voorlichting aan medewerkers die werken aan een <i>BO</i> , aangaande <i>ABDO 2017</i> procedures en de bijbehorende verantwoordelijkheden, bij aanstelling op een <i>Vertrouwensfunctie</i> , bij de start van een nieuwe <i>BO</i> en vervolgens periodiek, doch tenminste eenmaal per jaar.	Bijlage 6	●	●	●	●
3	De <i>BF</i> geeft waar nodig individueel advies en begeleiding aan medewerkers, die werken aan een <i>BO</i> , buitenlandse contacten hebben of op reis gaan naar risicolanden.	Bijlage 6 / 16	●	●	●	●
1.6	RAL / PSI / SAL	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	Een door de <i>Opdrachtgever</i> ingevulde <i>Rubriceringsaanduidingslijst (RAL)</i> is per <i>BO</i> aanwezig.	Bijlage 7	●	●	●	●
2	Een <i>Project Security Instruction (PSI)</i> of <i>Security Aspect Letter (SAL)</i> is aanwezig indien een (buitenlandse) <i>BO</i> specifieke aanvullende beveiligingseisen stelt.	Bijlage 7	●	●	●	●
3	<i>EU</i> en/of <i>NAVO TBB</i> wordt alleen vrijgegeven aan landen, organisaties of personeel die tot de <i>EU</i> en/of <i>NAVO</i> programma's behoren, behoudens vooraf vastgelegde uitzonderingen.	Bijlage 7	●	●	●	●
1.7	Logistieke keten	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	<i>Opdrachtnemer</i> meldt voorgenomen uitbesteding van werkzaamheden in het kader van een <i>BO</i> aan binnen- of buitenlandse <i>Subcontractors</i> vooraf aan <i>BIV / MIVD</i> . <i>BIV / MIVD</i> neemt hier een besluit over en verleent waar mogelijk toestemming.	Bijlage 8	●	●	●	●

2	Na toestemming van <i>BIV / MIVD</i> tot uitbesteding heeft <i>Opdrachtnemer</i> in het contract met <i>Subcontractors</i> die in aanraking komen met een <i>TBB</i> , de <i>ABDO 2017</i> bedongen. Een ingevulde <i>RAL</i> is hierbij verstrekt aan <i>BIV / MIVD</i> .	Bijlage 8	●	●	●	●
3	Na toestemming van <i>BIV / MIVD</i> (op basis van een door de buitenlandse <i>Partner</i> verstrekt <i>Facility Security Clearance</i>) tot uitbesteding heeft <i>Opdrachtnemer</i> in het contract met buitenlandse <i>Subcontractors</i> die in aanraking komen met een <i>TBB</i> , de in het betrokken land geldende beveiligingseisen bedongen. Een ingevulde <i>RAL</i> is hierbij verstrekt aan <i>BIV / MIVD</i> .	Procedure <i>ABDO</i>	●	●	●	●
4	Op (toe)leveranties van systeemonderdelen die op grond van hun kritische / vitale functie een zekere mate van bescherming verdienen, heeft <i>Opdrachtnemer</i> de <i>ABDO 2017</i> bedongen.	Bijlage 8	○	○	○	○
5	Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan een <i>BO</i> zijn de werkzaamheden aan een <i>TBB</i> zoveel mogelijk gecentraliseerd. (<i>Opdrachtnemer</i> draagt de verantwoordelijkheid voor het voldoen aan de eisen van <i>ABDO 2017</i> de bedrijven die hij als <i>Subcontractor</i> onder zijn hoede neemt).	Bijlage 8	●	●	●	●
6	<i>Opdrachtnemer</i> meldt het voornemen een buitenlandse <i>Subcontractor</i> in te schakelen voor een <i>BO</i> vooraf aan <i>BIV / MIVD</i> voor toestemming. Voor inschakeling van een buitenlands bedrijf is toestemming van <i>Opdrachtgever</i> en autorisatie door <i>BIV / MIVD</i> vereist.	Bijlage 8	●	●	●	●
1.8	Pers, internet, sociale media, publicatie, opnamen, etc.	Verwijzing	<i>TBB 1/ZG</i>	<i>TBB 2/G</i>	<i>TBB 3/C</i>	<i>TBB4/DV</i>
1	<i>Opdrachtnemer</i> en zijn medewerkers maken zonder uitdrukkelijke voorafgaande toestemming van <i>Opdrachtgever</i> en <i>BIV / MIVD</i> op geen enkele wijze publiekelijk bekend welke <i>BO</i> zij voor de Nederlandse overheid, buitenlandse overheid en/of <i>NAVO / EU</i> uitvoeren.	Bijlage 3 / 6	●	●	●	●
2	Het maken van opnamen van een <i>TBB</i> , anders dan noodzakelijk voor de uitvoering van de <i>BO</i> , is ongeacht het middel, niet toegestaan zonder voorafgaande schriftelijke goedkeuring van de <i>Opdrachtgever</i> in overleg met <i>BIV / MIVD</i> .	Bijlage 6	●	●	●	●
3	<i>Opdrachtnemer</i> en zijn medewerkers maken contactgegevens en afspraken met de <i>MIVD</i> op geen enkele wijze publiekelijk bekend.	Bijlage 6	●	●	●	●

1.9	Beveiligingsincidenten	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	Er is een <i>Incident Response Procedure (IRP)</i> opgesteld voor het behandelen van <i>Beveiligingsincidenten</i> . Deze is bekend bij allen die werken aan of toegang hebben tot een <i>TBB</i> .	Bijlage 9	●	●	●	●
2	<i>Beveiligingsincidenten</i> dienen binnen de normstelling genoemd in tabel "Classificatie" met behulp van de <i>IRP</i> aan <i>BIV / MIVD</i> te zijn bekend gesteld.	Bijlage 9	●	●	●	●
3	Gegevens t.a.v. toegang tot en inzicht in een <i>TBB</i> zijn vastgelegd en worden gedurende de aangegeven periode bewaard om achteraf onderzoek naar vermoede <i>Beveiligingsincidenten</i> mogelijk te maken.	Bijlage 9	6 maanden	6 maanden	3 maanden	3 Maanden
4	<i>Informatie</i> aangaande vastgestelde <i>Beveiligingsincidenten</i> wordt gedurende de aangegeven periode door de <i>BF</i> bewaard.	Bijlage 9	3 jaar	3 jaar	3 jaar	2 jaar
5	Werknemers dienen zwakke plekken in de beveiliging binnen de aangegeven termijn aan de <i>BF</i> te rapporteren.	Bijlage 9	direct	direct	werkdag	week
6	Er is een evaluatiemechanisme gedefinieerd waarmee men specifieke lessen (lessons learned) identificeert en deze verwerkt in het beveiligingsbeleid.	Bijlage 4 / 9	●	●	●	●
7	Er zijn disciplinaire maatregelen mogelijk tegen veroorzakers van <i>Beveiligingsincidenten</i> .		●	●	●	●

2 Personeel

Inleiding

Personele beveiliging betreft maatregelen gericht op het verkrijgen van een bepaalde mate van zekerheid dat een persoon de belangen van Defensie niet schaadt. Hieronder wordt niet begrepen de fysieke beveiliging van personeel of persoonsbeveiliging. Er worden betrouwbaarheidseisen gesteld aan het personeel van Defensie, alsmede aan het personeel in dienst van bedrijven die *Bijzondere Opdrachten (BO)* uitvoeren.

Personele beveiliging in relatie tot het kennisnemen van, werken met, produceren van of in aanraking komen met een *TBB* richt zich met name op het *Veiligheidsonderzoek* dat wordt uitgevoerd ter verkrijging van een *VGB*. In een aantal gevallen kan worden volstaan met een *VOG*, af te geven door Dienst Justis van het Ministerie van Veiligheid en Justitie.

Daarnaast is het zaak aandacht te besteden aan het beveiligingsbewustzijn bij medewerkers, zodat zij zich bij voortduring

bewust zijn van de risico's en zich nut en noodzaak realiseren van gedegen beveiligingsmaatregelen. Dit speelt ook een belangrijke rol bij reizen naar het buitenland.

De eisen met betrekking tot personele beveiliging zijn in het kader vanaf de volgende pagina verwoord. Waar nodig zijn de eisen nader toegelicht of uitgewerkt in een bijlage. Bij tegenstrijdigheid tussen de eis in de tabel en de tekst in inleiding of bijlage prevaleert de eis in de tabel.

Deze *ABDO 2017* bevat de eisen voor de beveiliging van een *TBB* waaraan voldaan moet zijn. Op basis van risico inschatting kunnen de eisen proportioneel worden toegepast. Dit kan betekenen dat er een andere, bijvoorbeeld minder stringente invulling aan een eis wordt gegeven dan letterlijk voorgeschreven. *BIV / MIVD* besluit hierover.

De van toepassing zijnde eisen worden aangegeven door een gesloten bolletje (●) in de kolom onder de van toepassing zijnde (hoogste) *Rubricering* of *TBB*-categorie. Als zich in deze kolom een open bolletje (○) bevindt, bepaalt *BIV / MIVD* na overleg met de *Opdrachtnemer* of, respectievelijk in welke mate, aan de eis moet worden voldaan.

ABDO 2017 eisen						
HOOFDSTUK 2 PERSONEEL			BEVEILIGINGSREGIME			
2.1	Het Veiligheidsonderzoek, VGB en VOG	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	Er is een formele <i>Lijst van Vertrouwensfuncties (LvV)</i> vastgesteld door de MIVD.	Bijlage 10	●	●	●	○
2	<i>Veiligheidsonderzoeken</i> worden aanvraagd op basis van een formeel vastgestelde LvV.	Bijlage 10	●	●	●	○
3	Een geldige VGB voor het vervullen van een <i>Vertrouwensfunctie</i> op A-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar.	Bijlage 11	●			
4	Een geldige VGB voor het vervullen van een <i>Vertrouwensfunctie</i> op B-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar.	Bijlage 11		●		
5	Een geldige VGB voor het vervullen van een <i>Vertrouwensfunctie</i> op C-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar.	Bijlage 11			●	
6	Een geldige VOG voor vervullen van een functie op DV-niveau is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 4 jaar.	Bijlage 11				●
7	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een VGB op A-niveau.	Bijlage 11	●	●		
8	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een VGB op minimaal B-niveau.	Bijlage 11			●	●
9	De BF van de <i>Opdrachtnemer</i> vraagt tenminste drie maanden voor het verstrijken van de periode van vijf jaar na de afgifte van de meest recente VGB een hernieuwd Veiligheidsonderzoek aan.	Bijlage 11	●	●	●	○
10	Bij tussentijdse aanleiding, bijvoorbeeld bij wijziging persoonlijke omstandigheden, vraagt de BF een hernieuwd <i>Veiligheidsonderzoek</i> aan.	Bijlage 14	●	●	●	○
11	Plaatsing op een <i>Vertrouwensfunctie</i> van een medewerker die niet beschikt over de Nederlandse nationaliteit, is voorafgaande aan de aanvraag van het <i>Veiligheidsonderzoek</i> goedgekeurd door BIV / MIVD.	Bijlage 13	●	●	●	○

12	<i>Opdrachtnemer</i> plaatst slechts medewerkers met de Nederlandse nationaliteit op <i>Vertrouwensfuncties</i> waarbij toegang tot een grote hoeveelheid <i>BI</i> (te bepalen door <i>BIV / MIVD</i> in overleg met <i>Opdrachtgever</i>) is vereist.	Bijlage 13	●	●	●	●
13	Een overzicht van alle de <i>VGB</i> , de <i>VOG</i> en verklaringen van bekendheid met de geheimhoudingsplicht is bij de <i>BF</i> aanwezig.	Bijlage 4	●	●	●	●
2.2	Geheimhoudingsverklaring	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	De <i>BF</i> heeft de (<i>Vertrouwens</i>) <i>functionaris</i> gewezen op de verplichtingen die voortvloeien uit het bekleden van een (<i>Vertrouwens</i>) <i>functie</i> .	Bijlage 10 / 12	●	●	●	●
2	Een door een <i>Vertrouwensfunctionaris</i> getekende ‘Verklaring van bekendheid met de geheimhoudingsplicht voor (<i>Vertrouwens</i>) <i>functionarissen</i> ’ is aanwezig en niet ouder dan vijf jaar.	Bijlage 12	●	●	●	
3	Een door een <i>functionaris</i> getekende ‘Verklaring van bekendheid met de geheimhoudingsplicht voor (<i>Vertrouwens</i>) <i>functionarissen</i> ’ is aanwezig.	Bijlage 12				●
4	Een door een <i>Vertrouwensfunctionaris</i> , die kennis moet nemen van crypto, crypto-security of CCI-gemerkte <i>Informatie</i> of materiaal, getekende ‘Verklaring van bekendheid met de geheimhoudingsplicht voor <i>Vertrouwensfunctionarissen</i> in het kader van een <i>Cryptofunctie</i> ’ is aanwezig en niet ouder dan vijf jaar.	Bijlage 12	●	●	●	
2.3	Ontheffing uit een <i>Vertrouwensfunctie</i>	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	De <i>BF</i> meldt ontheffing uit een <i>Vertrouwensfunctie</i> aan <i>BIV / MIVD</i> bij: - functiewijziging van een <i>Vertrouwensfunctionaris</i> ; - ontslag van een <i>Vertrouwensfunctionaris</i> ; - overtreding van beveiligingsregels door een <i>Vertrouwensfunctionaris</i> .	Bijlage 15	●	●	●	○
2	Een door de medewerker getekende ontheffingsverklaring bij ontheffing uit een <i>Vertrouwensfunctie</i> respectievelijk <i>Cryptofunctie</i> is aanwezig.	Bijlage 15	●	●	●	○
3	De <i>BF</i> heeft een toelichting gegeven op de ontheffingsverklaring, de (kopie) <i>VGB</i> ingenomen en zeker gesteld dat de medewerker geen <i>TBB</i> in bezit heeft.	Bijlage 15	●	●	●	○
4	Indien de <i>Vertrouwensfunctionaris</i> de beveiligingsregels van de <i>Opdrachtnemer</i> bewust of onbewust negeert of overtreedt, dient de <i>BF</i> passende maatregelen	Bijlage 15	●	●	●	○

	te nemen en <i>BIV / MIVD</i> hierover te informeren. Grove nalatigheid of bewuste <i>Compromittatie</i> van <i>Staatsgeheime</i> of <i>Vitale Informatie</i> of <i>Materieel</i> kan aanleiding zijn tot strafrechtelijke vervolging.					
5	Na het beëindigen van de overeenkomst zijn alle digitale TBB teruggegeven aan de Opdrachtgever. In het Beveiligingsplan is het proces hiervan beschreven		●	●	●	●
2.4	Reizen naar het buitenland	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	Een <i>Vertrouwensfunctionaris</i> heeft een voorgenomen reis naar het buitenland in het kader van een <i>BO</i> onverwijld gemeld aan de <i>BF</i> .	Bijlage 16	●	●	●	○
2	Een <i>Vertrouwensfunctionaris</i> heeft een voorgenomen reis naar een risicoland onverwijld gemeld aan de <i>BF</i> .	Bijlage 16	●	●	●	○
3	Indien bij een zakelijke reis een <i>Request for Visit</i> benodigd is, dient de <i>Vertrouwensfunctionaris (RfV)</i> , via de <i>BF</i> , een (elektronische) <i>RfV</i> ter goedkeuring in bij <i>BIV / MIVD</i> . Zonder goedgekeurd <i>RfV</i> kan de reis niet plaatsvinden.	Bijlage 16	●	●	●	○
4	De <i>BF</i> brieft en debrieft <i>Vertrouwensfunctionarissen</i> die voorgenomen reizen naar risicolanden aan de <i>BF</i> hebben gemeld.	Bijlage 16	●	●	●	○
5	De <i>BF</i> meldt aan <i>BIV / MIVD</i> het zakelijk of privéverblijf van een <i>Vertrouwensfunctionaris</i> of diens <i>Partner</i> in het buitenland langer dan drie aaneengesloten maanden.	Bijlage 16	●	●	●	○
6	De <i>BF</i> meldt, d.m.v. het formulier in bijlage 16 , aan <i>BIV / MIVD</i> zakelijk reizen en/of privéverblijf van een <i>Vertrouwensfunctionaris</i> naar of resp. in een risicoland.	Bijlage 16	●	●	●	○

3 Fysiek

Inleiding

Als op de eigen locatie van de *Opdrachtnemer* sprake is van opslag, verwerking of transport van een *TBB*, al dan niet in een daartoe aangewezen compartiment op die locatie (bijvoorbeeld een fysieke ruimte in een gebouw), zal die locatie c.q. het compartiment fysiek beveiligd moeten worden. Ook is het mogelijk dat een compartiment beveiligd moet worden waar besprekingen en/of presentaties plaatsvinden op gerubriceerd niveau ondanks dat daar normaliter geen opslag of verwerking plaatsvindt.

Fysieke beveiligingsmaatregelen worden onderscheiden in maatregelen van Organisatorische (O), Bouwkundige (B), Elektronische (E) en Reactieve (R) (OBER) aard. Een afgewogen selectie uit deze OBER-maatregelen moet onrechtmatige toegang tot een *TBB* onmogelijk maken, of pogingen daartoe in elk geval tijdig signaleren. Organisatorische maatregelen zijn er voornamelijk om onrechtmatige toegang tot een *TBB* te voorkomen. Met elektronische maatregelen moet vooral tijdige signalering van (pogingen tot) onrechtmatige toegang worden bewerkstelligd. Voorts dienen bouwkundige maatregelen de *Uitsteltijd* zodanig te vergroten dat tijdige *Interventie* kan plaatsvinden door de gebruiker, een beveiligingsbedrijf, politie of, indien het *ABDO*-bedrijf beschikt over een Verboden Plaats of gevestigd is op een defensielocatie, door Defensie. *Uitsteltijd* wordt gerealiseerd met bouwkundige maatregelen zoals stevige wanden,

vloeren en plafonds, geschikte deuren, ramen en dergelijke. Het is van belang om voor alle *TBB* een goede tijdpadanalyse te maken om zo vast te stellen wat het bewakingsrendement is. Voor een *TBB* 1 en een *TBB* 2 is de norm dat er sprake moet zijn van positief bewakingsrendement. Dat betekent dat te allen tijde *Interventie* plaatsvindt voordat de dader het *TBB* heeft kunnen compromitteren. De optelsom van de *Uitsteltijd* die door de OBER-beveiligingsschillen wordt opgebouwd moet dus worden vergeleken met de tijd die het een dader kost om het *TBB* te compromitteren.

Deze *ABDO* 2017 bevat de eisen voor de beveiliging van een *TBB* waaraan voldaan moet zijn. Op basis van risico inschatting kunnen de eisen proportioneel worden toegepast. Dit kan betekenen dat er een andere, bijvoorbeeld minder stringente invulling aan een eis wordt gegeven dan letterlijk voorgeschreven. *BIV* / *MIVD* besluit hierover. Een *Opdrachtnemer* conformeert zich aan de eisen uit hoofdstuk Fysiek wanneer er sprake is van opslag van *TBB* op eigen locatie.

De eisen met betrekking tot fysieke beveiliging zijn in het kader vanaf de volgende pagina verwoord. Waar nodig zijn eisen nader toegelicht of uitgewerkt in een bijlage. Bij tegenstrijdigheid tussen de eis in de tabel en de tekst in inleiding of bijlage prevaleert de eis in de tabel.

De van toepassing zijnde eisen worden aangegeven door een gesloten bolletje (●) in de kolom onder de van toepassing zijnde (hoogste) *Rubricering* of *TBB*-categorie. Als zich in deze kolom een open bolletje (○) bevindt, bepaalt *BIV* / *MIVD* na overleg met de *Opdrachtnemer* of, respectievelijk in welke mate, aan de eis moet worden voldaan.

ABDO 2017 eisen						
Hoofdstuk 3 Fysiek			BEVEILIGINGSREGIME			
3.1	Organisatorische maatregelen	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	De fysieke beveiligingsmaatregelen zijn volgens een schillenstructuur opgebouwd met toepassing van het "Need-to-Be" principe.	Bijlage 17 en 18	●	●	●	●
2	Bij het samenstellen van de fysieke maatregelen worden de "Need-to-Be" en "Need-to-Know" principes toegepast.	Bijlage 18	●	●	●	●
3	TBB moet worden beveiligd zodat <i>Compromittatie</i> wordt voorkomen.	Bijlage 19	●	●	●	●
4	Fysieke toegang tot het compartiment met een TBB is tot op individueel niveau controleerbaar.	Bijlage 19	●	●	●	○
5	Toegang tot het TBB of compartiment is alleen door middel van <i>Two-factor Authenticatie</i> verleend.	Bijlage 19	●	●	○	
6	Alleen een <i>Geautoriseerd</i> persoon kan zelfstandig toegang krijgen tot een TBB of tot een compartiment waarin zich een TBB bevindt.	Bijlage 18	●	●	●	
7	De BF zorgt voor <i>Autorisatie</i> van het personeel betreffende de toegang tot een TBB en de daarbij behorende infrastructuur.	Bijlage 18	●	●	●	
8	Periodiek, doch minimaal 1x per jaar, wordt het betrokken personeel en bewakingspersoneel getraind in het uitvoeren van beveiligingsmaatregelen.	Bijlage 18	●	●	●	●
9	Toegang van personen zonder <i>Autorisatie</i> (zoals bezoekers) is vooraf gemeld aan de BF.	Bijlage 18	●	●	●	
10	Personen met een <i>Autorisatie</i> zijn binnen het compartiment herkenbaar door middel van een zichtbaar gedragen pas. Op de pas staan tenminste de naam van de persoon en een pasfoto.	Bijlage 18	●	●	●	

11	Personen zonder <i>Autorisatie</i> (zoals bezoekers) zijn binnen het compartiment herkenbaar door middel van een zichtbaar gedragen pas. Op de pas staat voor een ieder goed zichtbaar "bezoeker" vermeld.	Bijlage 18	●	●	●	○
12	Bij toegang van personen zonder <i>Autorisatie</i> is het personeel in een compartiment waar gewerkt wordt met of aan een <i>TBB</i> vooraf geïnformeerd. Het personeel neemt hierop maatregelen om <i>Compromittatie</i> te voorkomen.	Bijlage 18	●	●	●	
13	In alle compartimenten met een <i>TBB</i> wordt personeel zonder <i>Autorisatie</i> (zoals bezoekers) begeleid door personeel met een <i>Autorisatie</i> . Van personen zonder <i>Autorisatie</i> is vooraf de identiteit vastgesteld en geregistreerd. De registratie hiervan wordt minimaal een jaar bewaard en op aanvraag aan <i>BIV / MIVD</i> verstrekt.	Bijlage 18	●	●	●	●
14	Toegang tot een compartiment met een <i>TBB</i> door bezoekers zonder <i>Autorisatie</i> die <u>niet</u> beschikken over de Nederlandse nationaliteit is minimaal vijf werkdagen voor het bezoek gemeld via de <i>BF</i> aan <i>BIV / MIVD</i> . Zonder toestemming van <i>BIV / MIVD</i> kan het bezoek niet plaatsvinden.	Bijlage 18	●	●	●	●
15	Er vindt toegangscontrole plaats bij elke beveiligingsschil.	Bijlage 17	●	●	●	
16	Aan de buitenzijde van het compartiment met een <i>TBB</i> zijn algemene beveiligingsinstructies bevestigd. In het beveiligingsplan is een overzicht van deze instructies opgenomen.	Bijlage 3 / 4 / 18	●	●	●	
17	De uitgifte van sleutels voor toegang tot compartimenten en opbergmiddelen met een <i>TBB</i> is geregistreerd. Bij de uitgifte van sleutels is gecontroleerd of men over een <i>Autorisatie</i> beschikt. De registratie hiervan wordt minimaal een jaar bewaard. Sleutels zijn voor zo min mogelijk personen toegankelijk.	Bijlage 18	●	●	●	●
18	Er zijn uitsluitend gecertificeerde sleutels gebruikt.	Bijlage 19	●	●	○	
19	De <i>BF</i> beheert certificaten, cijfercombinaties en reservesleutels van opbergmiddelen en compartimenten. Deze zijn opgeborgen in een ander opbergmiddel met <i>Two-factor Authenticatie</i> . Daarbij wordt het beveiligingsniveau gehanteerd van het <i>TBB</i> .	Bijlage 4 / 18	●	●	○	

20	Cijfercombinaties van sloten worden, zonder dat een eerder gebruikte combinatie wordt gekozen, veranderd: - indien een nieuw opbergmiddel of slot in gebruik wordt genomen; - indien een medewerker die de combinatie kent, wordt overgeplaatst; - indien wordt vermoed of vaststaat dat <i>Compromittatie</i> heeft plaatsgevonden; - uiterlijk zes maanden na de laatste wijziging van de combinatie.	Bijlage 18	●	●	●	
21	Alvorens een <i>TBB</i> buiten het reguliere, in het beveiligingsplan beschreven, proces te plaatsen, is hier toestemming voor verkregen van <i>BIV / MIVD</i> . De beveiliging van het <i>TBB</i> wordt hierbij op hetzelfde niveau gehouden.	Bijlage 18	●	●	●	●
22	Het " <i>Clear Desk</i> principe" en " <i>clear screen</i> principe" is toegepast in alle compartimenten waar zich een <i>TBB</i> bevindt of kan bevinden. Een <i>TBB</i> wordt niet onbeveiligd achter gelaten.	Bijlage 18	●	●	●	●
23	Beheer- en instandhoudingsmaatregelen zijn getroffen om beveiligingsmaatregelen blijvend te laten functioneren.	Bijlage 18	●	●	●	●
24	Het verlies van een authenticatiemiddel, zoals (elektronische) sleutel, dient behandeld te worden als een <i>Beveiligingsincident</i> .	Bijlage 18	●	●	●	○
25	Er zijn niet meer compartimenten dan strikt noodzakelijk.	Bijlage 18/19	●	●	●	●
26	Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan een opdracht worden de compartimenten zoveel mogelijk gecentraliseerd.	Bijlage 18/19	●	●	●	●
27	Het compartiment met een <i>TBB</i> bevindt zich in een zone die met toegangscontrole is afgeschermd van de openbare ruimte of van ruimten die niet onder controle staan.	Bijlage 18/19	●	●	●	
28	Beveiligingspersoneel heeft de beschikking over alarmeringsmiddelen.	Bijlage 20	●	●	●	○
29	Bij het verlaten van een compartiment met een <i>TBB</i> is een sluitronde gemaakt, waarbij de deur van het opbergmiddel, het compartiment en zo mogelijk het gebouw is afgesloten. Ramen en deuren zijn afgesloten en het <i>Indringer Detectie- en Signaleringssysteem (IDSS)</i> is geactiveerd. Tevens is een controle op insluiping en de verzegeling van nooddeuren uitgevoerd.	Bijlage 18/20	●	●	●	○

30	Bij afwezigheid van <i>Geautoriseerd</i> personeel blijft positief bewakingsrendement gewaarborgd.	Bijlage 18	●	●		
3.2	Bouwkundige maatregelen	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	Compartimenten met een <i>TBB</i> zijn afsluitbaar.	Bijlage 19	●	●	●	●
2	In het beveiligingsplan is een sluit- en sleutelplan opgenomen. Ramen, deuren en opbergmiddelen zijn afgesloten bij afwezigheid van <i>Geautoriseerd</i> personeel. Sleutels worden op hetzelfde niveau beveiligd als het <i>TBB</i> waar de sleutel toegang toe geeft.	Bijlage 18/19	●	●	●	●
3	Een compartiment waarin een <i>TBB</i> is opgeborgen is afgesloten met een slot voorzien van een gecertificeerde cilinder en sleutels. Wanneer een slot met een cilinder niet kan worden toegepast, wordt een gelijkwaardig gecertificeerd of getest mechanisme gebruikt, waardoor onbevoegd betreden niet mogelijk is zonder sporen van braak.	Bijlage 19	●	●	○	
4	Toegangsdeuren met een <i>Elektronisch Toegangsbeheer Systeem (ETS)</i> zijn voorzien van een deurdranger en een (elektronisch en akoestisch) alarm tegen te lang openstaan.	Bijlage 19 / 20	●	●	●	
5	Nooddeuren in het compartiment zijn alleen naar buiten toe te openen en te verzegelen. Bij openen klinkt een elektronisch of akoestisch signaal.	Bijlage 19	●	●	●	
6	Het gebouw waarin zich een <i>TBB</i> bevindt, is tegen opklimmen beveiligd. Losse opklimmogelijkheden zijn verwijderd zoals (afval) containers en ladders. Hemelwaterafvoeren, lage muren e.d. zijn van opklimbeveiliging conform NEN1887 voorzien.	Bijlage 19	●	●	●	
7	Gevelopeningen groter dan 15 cm moeten zijn beveiligd conform NEN-EN 5096 en NEN-EN-1627 die geldt voor het compartiment.	Bijlage 19	●	●	●	
8	Kelderramen en dergelijke zijn afgeschermd met traliewerk of strekmetaal conform NEN-EN 5096 en NEN-EN-1627 die geldt voor het compartiment.	Bijlage 19	●	●	●	○
9	Lichtkoepels, indien niet slagvast, zijn voorzien van traliewerk of strekmetaal conform NEN-EN 5096 en NEN-EN-1627 die geldt voor het compartiment.	Bijlage 19	●	●	●	○
10	Het compartiment met een <i>TBB</i> of een opbergmiddel met een <i>TBB</i> , zijn op alle vlakken (drie dimensionaal) van inbraakwerende maatregelen voorzien conform de normen uit de tabel in bijlage 19.	Bijlage 19	●	●	●	○

11	Wanneer het compartiment met een <i>TBB</i> of een opbergmiddel met een <i>TBB</i> zich bevindt op een hoogte van meer dan 5,5 meter en niet van buiten is te benaderen, gelden voor de breekwerendheid van de buitengevel de eisen van het niveau <i>TBB 4</i> .	Bijlage 19	●	●	●	
12	Ramen en gevelopeningen die open kunnen, zijn voorzien van breekwerend gaas.	Bijlage 19	●	●	●	
13	Opbergmiddelen tot 1000 kilogram zijn chemisch verankerd.	Bijlage 19	●	●		
13	Opbergmiddelen tot 1000 kilogram zijn verankerd.	Bijlage 19			●	
14	Bevestigingspunten van opbergmiddelen die van buitenaf bereikbaar zijn, zijn voorzien van beveiligde schroeven, bouten of moeren.	Bijlage 19	●	●	●	
15	Opbergmiddelen zijn voorzien van <i>Two-factor Authenticatie</i> .	Bijlage 19	●	●	●	
16	Opbergmiddelen zijn dusdanig afsluitbaar dat breek achteraf kan worden vastgesteld.	Bijlage 19	●	●	●	●
17	Opbergmiddelen voldoen aan de NEN-normering.	Bijlage 19	●	●	●	
18	Rondom het gebouw of terrein met een <i>TBB</i> staat een terreinafscheiding met toegangscontrole.	Bijlage 19	●	●	●	
19	Er is beveiligingsverlichting toegepast rondom het gebouw met een <i>TBB</i> .	Bijlage 19	●	●	●	
21	Bij de aanleg van cultuurtechnische infrastructuur is rekening gehouden met inbraakpreventie doormiddel van het creëren van een overzichtelijk geheel, zodat de indringer niet ongezien te werk kan gaan.	Bijlage 19	●	●	●	
22	De ramen en glazen wanden in een compartiment met een <i>TBB</i> zijn voorzien van inkijk beperkende maatregelen.	Bijlage 19	●	●	●	
23	Er zijn voorzieningen getroffen om elektronische apparatuur die niet strikt noodzakelijk zijn voor het uitvoeren van werkzaamheden buiten de compartimenten te houden.	Bijlage 19	●	●	○	

3.3	Elektronische maatregelen	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	Het compartiment waarin een opbergmiddel met een <i>TBB</i> is geplaatst, is voorzien van een <i>IDSS</i> .	Bijlage 20	●	●	●	
2	De aanliggende compartimenten van het compartiment met een <i>TBB</i> zijn voorzien van <i>IDSS</i> of een opbergmiddel met een <i>TBB</i> is zelf voorzien van <i>IDSS</i> .	Bijlage 20	●	●	●	
3	Het activeren en deactiveren van een <i>IDSS</i> kan alleen door middel van een <i>Two-factor Authenticatie</i> .	Bijlage 20	●	●	●	
4	Het <i>IDSS</i> functioneert 24 uur per dag en 7 dagen per week, tenzij <i>Geautoriseerd</i> personeel aanwezig is in het compartiment.	Bijlage 18/20	●	●	●	
5	<i>IDSS</i> -onderdelen zijn zodanig geplaatst dat <i>Compromittatie</i> van een <i>TBB</i> of pogingen daartoe worden ontdekt en een alarm genereren.	Bijlage 20	●	●	●	
6	De ruimte met een <i>TBB</i> is binnen het <i>IDSS</i> als aparte zone opgenomen. Deze zone is actief wanneer er geen <i>Geautoriseerd</i> personeel is in de ruimte.	Bijlage 18/20	●	●	●	
7	Doormelding van een <i>IDSS</i> voldoet aan de kwaliteit zoals gesteld in bijlage 19.	Bijlage 19	●	●	●	
8	Een alarm van een <i>IDSS</i> leidt tot een alarmopvolging binnen de in bijlage 21 gestelde <i>Interventie</i> tijd.	Bijlage 21	●	●	●	
9	Het <i>IDSS</i> signaleert en registreert uitval van de stroomvoorziening van de <i>IDSS</i> .	Bijlage 20	●	●	●	
10	Het <i>IDSS</i> beschikt over een gegarandeerde stroomvoorziening.	Bijlage 20	●	●	●	
11	Het <i>IDSS</i> is niet onopgemerkt te saboteren c.q. een <i>Compromittatie</i> wordt opgemerkt. Pogingen hiertoe zijn als een werkelijk alarm te presenteren.	Bijlage 20	●	●	●	
12	Detectie vindt onder alle (klimatologische) omstandigheden plaats.	Bijlage 20	●	●	●	
13	Bewegingsmelders beschikken over anti-masking maatregelen.	Bijlage 20	●	●	●	
14	Alleen elektronische apparatuur die essentieel is voor het uitvoeren van de opdracht is toegestaan binnen de ruimten van het <i>TBB</i> . Een lijst van de	Bijlage 18/19/20	●	●	○	

	apparatuur is opgenomen in het beveiligingsplan.					
15	In een ruimte met een <i>TBB</i> zijn geen camera's, smartphones, microfoons of andere opnameapparatuur aanwezig.	Bijlage 20	●	●	○	
16	Beveiligingssystemen zijn geïnstalleerd en periodiek onderhouden door een gecertificeerd bedrijf conform NEN-EN 50130. Daarbij zijn de beveiligingssystemen periodiek, doch minimaal 1x per jaar, gecontroleerd.	Bijlage 19	●	●	●	
17	Een beveiligingscamera met zicht op de toegang van een compartiment is buiten het compartiment aangebracht.	Bijlage 20	●	●	○	
18	De bewaartermijn voor camerabeelden is 3 maanden. Camerabeelden met incidentdata dienen 1 jaar bewaard te zijn.		●	●	●	
19	Er is een <i>ETS</i> voor gecontroleerde toegang tot het compartiment geïnstalleerd en in werking.	Bijlage 20	●	●	○	
20	Als gebruik is gemaakt van elektronische sloten, zijn maatregelen getroffen om te detecteren dat toegang "onder dwang" is verleend.	Bijlage 18	●	●		
21	Een <i>ETS</i> is uitgerust met een Anti Pass Back (APB) systeem.	Bijlage 20	●	●		
22	Een <i>ETS</i> is voorzien van <i>Logging</i> , waarbij de logs tenminste een jaar worden bewaard.	Bijlage 20	●	●		
23	Een <i>ETS</i> is zodanig uitgevoerd dat, wanneer het systeem uitschakelt of uitvalt, alle toegangen tot het compartiment mechanisch worden afgesloten of elektronisch afgesloten blijven.	Bijlage 20	●	●		
24	Een <i>ETS</i> is dusdanig uitgevoerd dat een noodknopbediening of mechanische paniekontgrendeling binnen het compartiment op zodanige wijze is aangebracht dat bij calamiteiten het <i>Object</i> snel in het kader van veiligheid kan worden verlaten.	Bijlage 20	●	●		
25	De noodknopbediening of mechanische paniekontgrendeling is van buitenaf niet bereikbaar. Na gebruik van de noodknopbediening of mechanische paniekontgrendeling dienen adequate veiligheidsmaatregelen te worden getroffen ter bescherming van het <i>TBB</i> .	Bijlage 20	●	●		

26	Wanneer een beveiligingssysteem (<i>ETS</i> of <i>IDSS</i>) gekoppeld is aan een gebouwbeheersysteem, gelden de beveiligingsmaatregelen van het beveiligingssysteem ook voor het gebouwbeheersysteem.	Bijlage 20	●	●		
3.4	Reactieve maatregelen	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	Meldingen uit het <i>IDSS</i> en het <i>ETS</i> moeten leiden tot tijdige <i>Interventie</i> .	Bijlage 21	●	●	●	
2	<i>Interventie</i> vindt plaats door daartoe aangewezen en opgeleid personeel binnen de gestelde <i>Interventietijd</i> .	Bijlage 21	●	●	●	●
3	Als alleen een alarm afgaat in een compartiment en niet bij de daaromheen liggende beveiligingsschillen is te handelen alsof de omliggende alarmen ook zijn afgegaan.	Bijlage 21	●	●	●	
4	Beveiligingspersoneel informeert bij een geconstateerde <i>Compromittatie</i> van een <i>TBB</i> terstond de <i>BF</i> .	Bijlage 21	●	●	●	●
5	Reactie op (technische) storingen moet leiden tot het herstellen van het gewenste beveiligingsrendement.	Bijlage 21	●	●	●	●
6	Na een alarm vindt controle van het compartiment met een <i>TBB</i> plaats door de <i>BF</i> of diens gemandateerde.	Bijlage 21	●	●	●	○
7	Alarmverificatie vindt aan de buitenzijde van het compartiment met een <i>TBB</i> plaats. Hierbij zijn alle toegangen, gevelopeningen, daken e.d. gecontroleerd.	Bijlage 21	●	●	●	●
8	Personeel dat alarmverificatie uitvoert, heeft ten tijde van de alarmverificatie niet de beschikking over sleutels of codes die toegang geven tot het <i>TBB</i> .	Bijlage 21	●	●	●	●
9	Een Particuliere Alarm Centrale beschikt over een justitiële erkenning en voldoet aan de NEN-EN 50518 norm.	Bijlage 21	●	●	●	●
3.5	Transport en verzenden	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	Een <i>TBB</i> wordt uitsluitend buiten het compartiment gebracht als dit voor de voortgang van de werkzaamheden absoluut noodzakelijk is.	Bijlage 22	●	●	●	●
2	De <i>BF</i> stelt conform bijlage 22 voorschriften op voor het transporteren en verzenden van een <i>TBB</i> en houdt hier toezicht op.	Bijlage 22	●	●	●	●

3	Een <i>TBB</i> mag nooit mee naar huis worden genomen.	Bijlage 22	●	●	●	○
4	Transport van <i>TBB</i> is vooraf gemeld aan <i>BIV / MIVD</i> .	Bijlage 22	●	●	●	
3.6	Transport en verzenden binnenland	Verwijzing	<i>TBB 1 / ZG</i>	<i>TBB 2 / G</i>	<i>TBB 3 / C</i>	<i>TBB 4 / DV</i>
1	Transport van een <i>TBB</i> geschiedt uitsluitend door tussenkomst van <i>BIV / MIVD</i> .	Bijlage 22	●			
2	Een <i>TBB</i> is uitsluitend mee te nemen in een door <i>BIV / MIVD</i> goedgekeurd afsluitbaar transportmiddel.	Bijlage 22	●	●	●	
3	Transport van een <i>TBB</i> vindt plaats: - handcarried, al dan niet met eigen vervoer, door 1 <i>Geautoriseerde</i> medewerker, of - met inschakeling van een door <i>BIV / MIVD</i> goedgekeurd transport- / koeriersbedrijf.	Bijlage 22		●	●	
4	Een <i>TBB</i> is uitsluitend mee te nemen in een afsluitbaar transportmiddel.	Bijlage 22				●
5	Transport van een <i>TBB</i> vindt plaats: - handcarried, al dan niet met eigen vervoer, door een <i>Geautoriseerde</i> medewerker, of - met inschakeling van een door <i>BIV / MIVD</i> goedgekeurd transport- / koeriersbedrijf, of - met inschakeling van een transport-/koeriersbedrijf	Bijlage 22				●
6	Het transport-/koeriersbedrijf waaraan het <i>TBB</i> zonder toezicht of begeleiding door een vertrouwensfunctionaris wordt toevertrouwd, is als <i>Subcontractor</i> aangemeld bij <i>BIV / MIVD</i> .	Bijlage 22		●	●	○
7	Transport van een <i>TBB</i> gaat via de kortst mogelijke weg zonder onderbrekingen. Het <i>TBB</i> blijft onder toezicht, voertuigen worden niet onbeheerd gestald.	Bijlage 22		●	●	
8	Verzenden van <i>BI</i> per post is <u>niet</u> toegestaan.	Bijlage 22	●			

9	Verzending van <i>BI</i> per post is uitsluitend toegestaan binnen Nederland wanneer dit aangetekend met een track en trace nummer wordt verstuurd in dubbele verpakking volgens bijlage 22 met een onmiddellijke ontvangstbevestiging	Bijlage 22		●	●	
10	Verzending van <i>BI</i> per post is uitsluitend binnen Nederland toegestaan wanneer dit in dubbele verpakking volgens bijlage 22 wordt verstuurd.	Bijlage 22				●
3.7	Transport en verzenden buitenland	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	Transport van een <i>TBB</i> geschiedt uitsluitend door tussenkomst van <i>BIV</i> / <i>MIVD</i> .	Bijlage 22	●			
2	Een <i>TBB</i> mag zonder toestemming van <i>BIV</i> / <i>MIVD</i> niet worden meegenomen naar het buitenland.	Bijlage 22		●	●	●
3	Internationaal transport van een <i>TBB</i> vindt plaats na goedkeuring van het transportplan door <i>BIV</i> / <i>MIVD</i> .	Bijlage 22		●	●	●
4	Voor transport van <i>BI</i> naar het buitenland kan worden teruggevallen op <i>BIV</i> / <i>MIVD</i> ("Government-to-Government"-procedure).	Bijlage 22		●	●	●
5	Verzenden van <i>BI</i> per post is <u>niet</u> toegestaan.	Bijlage 22	●	●	○	
6	Verzenden van <i>BI</i> per post is toegestaan, met gebruikmaking van aangetekende post met track en trace nummer, in dubbele verpakking en met onmiddellijke ontvangstbevestiging.	Bijlage 22			○	●
3.8	Fysieke opslag, verwerking en ontwikkeling	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
1	De <i>BF</i> of een daartoe aangewezen en geautoriseerd persoon dient een actueel overzicht te hebben van alle <i>BO</i> binnen het bedrijf.	Bijlage 23	●	●	●	●
2	Geregistreerd is wie <i>BI</i> onder zijn berusting heeft.	Bijlage 23	●	●	●	
3	Geregistreerd is wie werkzaamheden aan <i>BI</i> heeft uitgevoerd of <i>BI</i> heeft ingezien.	Bijlage 23	●	●		
4	<i>Informatie</i> geproduceerd door het bedrijf, waarbij de steller vermoedt dat bij <i>Compromittatie</i> voor de Staat schade kan ontstaan, is <i>Gerubriceerd</i> . De <i>Rubricering</i> is door de (sub-) <i>BF</i> vastgesteld en geregistreerd.	Bijlage 23	●	●	●	
5	<i>BI</i> is geregistreerd en van een kenmerk (labeling) voorzien.	Bijlage 23	●	●	●	●

6	BI is geregistreerd en van een uniek exemplaarnummer voorzien.	Bijlage 23	●	●		
7	Rubriceringen en Merkingen zijn conform bijlage 23 aangebracht.	Bijlage 23	●	●	●	●
8	De reproductie van <i>Informatie</i> geschiedt alleen met toestemming van degene die de <i>Rubricering</i> heeft vastgesteld.	Bijlage 23	●	●	●	
9	Gemaakte reproducties zijn geregistreerd.	Bijlage 23	●	●	●	
10	Het maken van reproducties is voorbehouden aan daartoe aangewezen geautoriseerd personeel dat ook zorgdraagt voor de registratie hiervan.	Bijlage 23	●	●	●	
11	Reproducties kennen dezelfde <i>Rubricering</i> als het origineel, ook als slechts delen van het origineel is gebruikt.	Bijlage 23	●	●	●	●
12	Er zijn niet meer reproducties gemaakt dan strikt noodzakelijk is.	Bijlage 23	●	●	●	●
13	Reproducties maken, is alleen toegestaan met door BIV / MIVD toegestane middelen.	Bijlage 23	●	●	●	
14	Reproductiemiddelen worden beschouwd als een <i>Informatiesysteem</i> en worden minimaal op hetzelfde niveau beveiligd als de verwerkte informatie.	Bijlage 23	●	●	●	●
15	In geval van vernietiging wordt door de BF of een aangewezen medewerker met de juiste <i>Autorisatie</i> een proces verbaal van vernietiging opgemaakt.	Bijlage 23	●	●	●	
16	Vernietigen van <i>Informatie</i> geschiedt conform bijlage 23.	Bijlage 23	●	●	●	●

4 Cyber

Periodiek wordt in nauwe samenwerking tussen publieke en private partijen het Nationaal Cyber Security Beeld Nederland (CSBN) opgemaakt. Eén van de kernbevindingen in het CSBN is dat staten en cybercriminelen een grote dreiging vormen voor Nederland. Dit uit zich in een groeiend aantal digitale aanvallen op Defensie, de defensie-industrie en bondgenootschappelijke netwerken. De aanvallen worden steeds complexer en zijn agressief van aard. De verwachting is dat deze tendens zich de komende jaren zal voortzetten. Actuele en strengere maatregelen zijn vereist om de digitale weerbaarheid te waarborgen.

Vanaf het ABDO 2017 worden de maatregelen in het digitale domein Cybermaatregelen genoemd. De term *Cyber* omvat naast de IT-infrastructuur ook het stelsel van activiteiten (o.a. bedrijfsvoering) wat met de infrastructuur mogelijk wordt gemaakt. Het zijn juist die activiteiten die beschermd moeten worden. Een gedegen *Beveiliging* van informatie vormt daarbij de basis van Cybersecurity. In dit ABDO worden informatiebeveiligingseisen aangevuld met eisen ten aanzien van de Cyberbeveiligingsorganisatie, incidentmanagement, *Logging* en *Monitoring* om snel te kunnen reageren op dreigingen tegen de Cyberactiviteiten.

Het ABDO 2017 vereist dat de organisatie een functionaris aanstelt die de rol van *Cyber-Beveiligingsfunctionaris* (Cyber-BF) vervult. De Cyber-BF heeft het overzicht van de Cyberactiviteiten die binnen de organisatie worden uitgevoerd ten behoeve van het Ministerie van Defensie en de

maatregelen om deze te beschermen. De *Cyber-BF* is de contactpersoon voor *BIV / MIVD* waar het gaat om het Cyberdomein.

Niet alleen de toenemende dreiging vereist nieuwe eisen, maar ook de innovaties in het digitale domein die nieuwe functionaliteiten bieden. Dit hoofdstuk stelt ook eisen ten aanzien van *Cloudcomputing* en het gebruik daarvan, *bring / choose your own device* (BYOD / CYOD) en *Virtualisatie*.

Deze ABDO 2017 bevat de eisen voor de *Beveiliging* van een TBB waaraan voldaan moet zijn. Op basis van risico inschatting kunnen de eisen proportioneel worden toegepast. Dit kan betekenen dat er een andere, bijvoorbeeld minder stringente invulling aan een eis wordt gegeven dan letterlijk voorgeschreven. *BIV / MIVD* besluit hierover.

De eisen met betrekking tot Cybersecurity zijn in de volgende tabel uiteengezet. Waar nodig zijn eisen nader toegelicht of uitgewerkt in een bijlage. De tabel met eisen kent globaal dezelfde structuur als de ISO27000-serie en is inhoudelijk afgestemd op het Defensie beveiligingsbeleid. Bij tegenstrijdigheid tussen de eis in de tabel en de tekst in inleiding of bijlage prevaleert de eis in de tabel.

De van toepassing zijnde eisen worden aangegeven door een gesloten bolletje (●) in de kolom onder de van toepassing zijnde (hoogste) *Rubricering* of TBB-categorie. Als zich in deze kolom een open bolletje (○) bevindt, bepaalt *BIV / MIVD* na overleg met de *Opdrachtnemer* of, respectievelijk in welke mate, aan de eis moet worden voldaan.

ABDO 2017 eisen						
Hoofdstuk 4 Cyber			BEVEILIGINGSREGIME			
4.1	Informatiebeveiligingsbeleid	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
4.1	Beleidsregels voor <i>Informatiebeveiliging</i>					
1	Er is beleid ten aanzien van cybersecurity.		○	○	○	○
4.2	Organiseren van <i>Informatiebeveiliging</i>	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
4.2	Interne organisatie					
1	Er is een <i>Cyber Beveiligingsfunctionaris</i> (Cyber-BF) aangesteld. De Cyber-BF heeft, net als de BF, rechtstreeks toegang tot de Directie van de organisatie. De Cyber-BF kan de taken door derden binnen de organisatie laten uitvoeren.	Bijlage 24	●	●	●	●
2	De Cyber-BF is namens de directie bevoegd tot het (laten) nemen van gepaste beveiligingsmaatregelen op het gebied van <i>Cyber-security</i> .	Bijlage 24	●	●	●	●
3	De Cyber-BF houdt, namens de directie, toezicht op een veilige inrichting van de digitale infrastructuur binnen de organisatie.	Bijlage 24	●	●	●	●
4	De Cyber-BF verstrekt de aan de organisatie toebehorende externe IP adressen en domeinnamen aan BIV / MIVD.	Bijlage 24	●	●	●	●
5	De Cyber-BF houdt door middel van een registratie toezicht op de locatie, uitgifte, inname en herkomst van alle door de organisatie in ontvangst of beheer genomen digitale TBB.	Bijlage 24	●	●	●	
6	De Cyber-BF heeft te allen tijde inzicht in de gebruikte digitale TBB.	Bijlage 24				●
7	De Cyber-BF voert voorts de taken uit als beschreven in de bijlage.	Bijlage 24	●	●	●	●
8	De Cyber-BF draagt zorg voor volledige medewerking bij controles van, audits op en onderzoeken aan de IT infrastructuur van de <i>Opdrachtnemer</i> door BIV / MIVD.	Bijlage 24	●	●	●	●
4.2	Scheiding van taken					

9	De rechten van een gebruiker omvatten niet een gehele cyclus van handelingen in een kritisch <i>Informatiesysteem</i> .	Bijlage 31	●	●	●	●
10	Er is een scheiding tussen IT-beheertaken en gebruikerstaken.	Bijlage 31	●	●	●	●
11	Voordat de verwerking van configuratiegegevens die de <i>Integriteit</i> van informatiesystemen kunnen aantasten zijn deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie is een log bijgehouden.	Bijlage 31	●	●	●	●
12	Verantwoordelijkheden voor IT-beheer en <i>Wijziging</i> van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (IT-beheerders)rol.	Bijlage 31	●	●	●	●
4.2	Mobiele apparatuur en telewerken					
13	Een <i>TBB</i> dat is opgeslagen op mobiele apparatuur is alleen toegestaan met toepassing van door <i>BIV / MIVD</i> goedgekeurde procedures en middelen: - een goedgekeurde <i>Vercijfering</i> ; - heeft alleen de hoogst noodzakelijke hoeveelheid informatie in opslag; - mag niet gebruikt worden in publieke ruimten.	Bijlage 22 / 25	●	●	●	
14	Een <i>TBB</i> dat is opgeslagen op mobiele apparatuur is alleen toegestaan met toepassing van door <i>BIV / MIVD</i> goedgekeurde procedures en middelen: - een goedgekeurde <i>Vercijfering</i> ; - heeft alleen de hoogst noodzakelijke hoeveelheid informatie in opslag; - mag niet gebruikt worden in publieke ruimten; - een door <i>BIV / MIVD</i> goedgekeurde koppeling.	Bijlage 22 / 25				●
15	Voor het gebruik van mobiele apparatuur en telewerken zijn gebruikersinstructies opgesteld.					●
16	Een mobiel apparaat bevat geen kenmerken die direct herleidbaar zijn tot het Ministerie van Defensie.					●
17	Er zijn voorzieningen om de actualiteit van anti- <i>Malware</i> programmatuur op mobiele apparaten te garanderen.		●	●	●	●
18	Na melding van verlies of diefstal is direct de communicatiemogelijkheid met de centrale applicaties afgesloten.					●
19	Mobiele apparatuur in het kader van <i>BYOD</i> of <i>CYOD</i> zijn alleen na goedkeuring van <i>BIV / MIVD</i> toegestaan.	Bijlage 25 / 28				●
20	Opslag, verwerking en transport van data op <i>BYOD / CYOD</i> -apparatuur vindt plaats op basis van gelijke condities gesteld aan <i>DV</i> netwerken. Bij lokale opslag	Bijlage 25 / 28				●

	van data is door <i>BIV / MIVD</i> goedgekeurde <i>Vercijfering</i> toegepast.					
4.2	Telewerken					
21	Telewerken is niet toegestaan.		●	●	●	
22	Telewerkvoorzieningen op basis van een terminal server verbinding zijn zo ingericht dat op de werkplek geen bedrijfsinformatie is opgeslagen ("zero footprint") en mogelijke <i>Malware</i> vanaf de werkplek niet in het vertrouwde deel terecht kan komen.					●
23	Indien toegang tot een <i>TBB</i> via een remote inlogvoorziening mogelijk is, is een procedure hiervoor in het <i>Beveiligingsplan</i> opgenomen.					●
24	Voor remote toegang is gebruik gemaakt van de door <i>BIV / MIVD</i> goedgekeurde oplossing(en) en middelen.					●
4.3	Vellig personeel	Verwijzing	<i>TBB 1 / ZG</i>	<i>TBB 2 / G</i>	<i>TBB 3 / C</i>	<i>TBB 4 / DV</i>
4.3	Bewustzijn, opleiding en training ten aanzien van <i>Informatiebeveiliging</i>					
1	Het personeel dat betrokken is bij de behandeling van een <i>TBB</i> doorloopt jaarlijks een <i>Cyber security-awareness</i> training met goed gevolg. Zie bijlage 26 voor een overzicht met aandachtspunten.	Bijlage 26	●	●	●	●
2	De BF, <i>Cyber-BF</i> , IT-beheer en het overige personeel dat betrokken is bij de behandeling van een digitale <i>TBB</i> bezitten de benodigde ervaring, competenties en kennis door relevante opleiding en training.		●	●	●	●
4.3	Beëindiging of Wijziging van verantwoordelijkheden van het dienstverband					
3	Er is een procedure vastgesteld voor verandering/beëindiging van functie/dienstverband, contract/project of overeenkomst waarin minimaal aandacht besteed is aan het intrekken van toegangsrechten, innemen van <i>ICT-bedrijfsmiddelen</i> en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.		●	●	●	●
4.4	Beheer van bedrijfsmiddelen	Verwijzing	<i>TBB 1 / ZG</i>	<i>TBB 2 / G</i>	<i>TBB 3 / C</i>	<i>TBB 4 / DV</i>
4.4	Inventariseren van <i>ICT-bedrijfsmiddelen</i>					
1	Er is een actuele registratie van <i>ICT-bedrijfsmiddelen</i> . Zie bijlage voor een overzicht van te registreren gegevens.	Bijlage 27	●	●	●	●
2	Er is een actuele beschrijving van de <i>ICT</i> -infrastructuur beschikbaar.	Bijlage 27	●	●	●	●

3	Alle apparatuur en systemen zijn in een netwerk- of configuratietekening bijgehouden. Hierin is duidelijk aangegeven de locatie en de functie van de componenten.	Bijlage 27	●	●	●	●
4.4	Eigendom van ICT-bedrijfsmiddelen					
4	Voor elk bedrijfsproces, applicatie, gegevensverzameling en overige <i>ICT-bedrijfsmiddelen</i> is een verantwoordelijke lijnmanager benoemd.	Bijlage 27	●	●	●	●
4.4	Aanvaardbaar gebruik van ICT-bedrijfsmiddelen					
5	Er zijn regels vastgesteld en gedocumenteerd voor gebruik van <i>ICT-bedrijfsmiddelen</i> en deze zijn ter kennis gesteld aan de gebruikers. De regels zijn als bijlage opgenomen in het <i>Beveiligingsplan</i> .		●	●	●	●
6	Alleen applicaties die door IT-Beheer op een systeem geplaatst zijn, zijn gebruikt.		●	●	●	●
4.4	Classificatie van informatie					
7	De opsteller van de informatie doet een voorstel tot <i>Rubricering</i> en/of <i>Merking</i> en brengt deze aan op de informatie. De <i>Cyber-BF</i> stelt de <i>Rubricering</i> van de informatie vast.	Bijlage 23 / 30	●	●	●	
8	De opsteller van de informatie bepaalt de <i>Rubricering</i> en/of <i>Merking</i> en brengt deze aan op de informatie.	Bijlage 23 / 30				●
4.4	Informatie labelen					
9	De hoogste <i>Rubricering</i> en <i>Merking</i> van Informatie is vermeld op verwijderbare en mobiele gegevensdragers.	Bijlage 23 / 30	●	●	●	●
4.4	Behandelen van ICT-bedrijfsmiddelen					
10	Systeemdocumentatie, wanneer deze specifieke informatie bevat over beveiligingsmaatregelen van de <i>TBB</i> welke zich op het systeem bevinden, is op het zelfde niveau beveiligd als deze <i>TBB</i> .		●	●	●	●
11	Er is systeemdokumentatie aanwezig die een implementatie van een systeem beschrijft om beheer te kunnen uitvoeren.	Bijlage 29	●	●	●	●
12	Er zijn procedures vastgesteld en in werking gesteld voor verwijderen van een <i>TBB</i> en de vernietiging hiervan.		●	●	●	●
13	Na beëindigen van de opdracht of bij het afvoeren zijn de gegevensdragers fysiek vernietigd. Een proces-verbaal van vernietiging is opgesteld.	Bijlage 23	●	●	●	
14	Het wissen van gegevensdragers is alleen toegestaan indien gebruik is gemaakt van door <i>BIV / MIVD</i> goedgekeurde middelen.		●	●	●	●

4.4	Beheer van Verwijderbare Gegevensdragers					
15	<i>Verwijderbare Gegevensdragers</i> zijn niet onbeheerd achtergelaten.		●	●	●	●
16	In het geval dat gegevensdragers een kortere verwachte levensduur hebben dan de gegevens die ze bevatten, zijn de gegevens gekopieerd wanneer 75% van de levensduur van de gegevensdrager is verstreken.		●	●	●	●
4.5	Toegangsbeveiliging	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
4.5	Beleid voor toegangsbeveiliging					
1	Alleen geautoriseerde gebruikers hebben toegang.	Bijlage 31	●	●	●	●
2	Het systeem voorkomt ongeautoriseerde toegang.		●	●	●	●
3	Toegang door derden uit hoofde van toezicht, inspectie en of audit is goedgekeurd door <i>BIV / MIVD</i> .		●	●	●	●
4	In het <i>Beveiligingsplan</i> is beschreven op welke wijze gebruikers toegang hebben.		●	●	●	●
5	Er is één basisadministratie van authenticatiegegevens van gebruikers, op basis waarvan de gebruikers vooraf zijn geïdentificeerd en geautoriseerd.		●	●	●	●
4.5	Toegang tot netwerken en netwerkdiensten					
6	<i>Beheer op afstand</i> is niet toegestaan.		●	●	●	
7	Er is een procedure vastgesteld waarbij <i>onderhoud op afstand</i> alleen toegankelijk is als het strikt noodzakelijk is en een verbinding uitsluitend geactiveerd kan worden door een bevoegd functionaris (conform <i>Beveiligingsplan</i>).					●
8	De toegang voor <i>onderhoud op afstand</i> door een <i>Leverancier</i> is alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.					●
9	<i>Beheer op afstand</i> van apparatuur is alleen toegestaan indien gebruik is gemaakt van door <i>BIV / MIVD</i> goedgekeurde middelen.	Bijlage 25				●
4.5	Registratie en afmelden van gebruikers					
10	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding is toegepast en welke toegangsrechten zijn gegeven. De risicoafweging, resultaten en maatregelen zijn weergegeven in het <i>Beveiligingsplan</i> .		●	●	●	●

11	Het accountmechanisme garandeert dat handelingen zijn herleid naar een natuurlijk persoon.		●	●	●	●
12	Een account mag geen indicatie geven van het privilegenniveau of de naam van de gebruiker.		●	●	●	●
13	Bij uitgifte van authenticatiemiddelen is de identiteit van de gebruiker vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.		●	●	●	●
4.5	Beheren van speciale toegangsrechten					
14	Gebruikers hebben alleen bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (" <i>Need-to-know</i> ", " <i>need-to-use</i> ").		●	●	●	●
15	Gebruikers hebben alleen toegang tot een voor de functie noodzakelijk geachte set van applicaties en commando's.		●	●	●	●
16	Systeemprocessen draaien onder een eigen gebruikersnaam, voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.		●	●	●	●
17	Autorisaties en gebruikersrollen zijn per gebruiker verstrekt conform een vaste autorisatieprocedure.		●	●	●	●
18	Er is een noodprocedure zodat in noodgevallen een beheerdersaccount met bijbehorend wachtwoord toegankelijk is. Hierin moet beschreven zijn wie er toestemming geeft voor gebruik van dit account.		●	●	●	●
19	Op het wachtwoord voor een beheerdersaccount zijn de eisen van toepassing die één (1) rubriceringsniveau hoger liggen dan het systeem dat er mee beheerd wordt, met als hoogste rubriceringsniveau STG. ZEER GEHEIM.		●	●	●	●
20	Er zijn maatregelen getroffen om het ongeautoriseerde gebruik van i/o-poorten (zoals de parallelle, seriële, USB en firewire poorten) op de werkplek(sessie) tegen te gaan.		●	●	●	●
21	Indien een gebruiker ingelogd is op een werkplek(sessie), dan vindt het overnemen van de werkplek(sessie) alleen plaats na toestemming van de gebruiker. Er moet een mogelijkheid zijn om overname van de werkplek(sessie) zelf te beëindigen of er moet een melding komen dat de werkplek(sessie) is beëindigd.		●	●	●	●
22	Administrator- of rootrechten zijn aan een beperkte groep IT-beheerders toegekend. Van deze IT-beheerders is een register bijgehouden.		●	●	●	●
23	De IT-beheerders administreren het gebruik van de beheerdersaccounts.		●	●	●	●

24	Het systeem geeft aan welke autorisaties zijn verleend aan personen en/of systemen.		●	●	●	●
4.5	Beheer van geheime <i>Authenticatie</i>-informatie van gebruikers					
25	Ten aanzien van wachtwoorden geldt: - wachtwoorden zijn op een veilige manier uitgegeven (controle identiteit van de gebruiker evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel); - tijdelijke wachtwoorden zijn bij eerste gebruik vervangen door een ander wachtwoord; - wachtwoorden mogen niet tegelijkertijd met het gebruikersaccount zijn verstrekt; - wachtwoorden die standaard in software zijn meegegeven, zijn bij installatie gewijzigd.		●	●	●	●
26	Op het wachtwoord voor een gebruikersaccount zijn de eisen van toepassing die gelijk zijn aan het rubriceringsniveau van het systeem waartoe toegang is verkregen.		●	●	●	●
4.5	Beoordeling van toegangsrechten van gebruikers					
27	Toegangsrechten van gebruikers zijn periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het <i>Beveiligingsplan</i> .					●
28	Toegangsrechten van gebruikers zijn periodiek, minimaal driemaandelijks, geëvalueerd. Het interval is beschreven in het <i>Beveiligingsplan</i> .			●	●	
29	Toegangsrechten van gebruikers zijn periodiek, minimaal maandelijks, geëvalueerd. Het interval is beschreven in het <i>Beveiligingsplan</i> .		●			
30	Accounts die meer dan 60 dagen niet zijn gebruikt, zijn geblokkeerd.		●	●	●	●
31	Een geblokkeerd account is vrijgegeven door tussenkomst van de <i>Cyber-BF</i> .		●	●	●	
4.5	Geheime <i>Authenticatie</i>-informatie gebruiken					

32	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: - wachtwoorden zijn niet opgeschreven; - gebruikers delen hun wachtwoord nooit met anderen; - een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde; - wachtwoorden zijn niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).		●	●	●	●
33	De minimale lengte van wachtwoorden is voor (TBB1:12, TBB2 en 3:10,TBB4:9) karakters.		●	●	●	●
34	Wachtwoorden zijn elke (TBB1:60, TBB2:90,TBB3:90,TBB4:90) dagen gewijzigd. Daarbij zijn de laatste 10 gebruikte wachtwoorden niet hergebruikt.		●	●	●	●
35	<i>Authenticatie</i> van gebruikers is op basis van wachtwoorden.		●	●	●	●
36	<i>Two-factor Authenticatie</i> in aanvulling op wachtwoorden is gebruikt.		●	●	●	
37	<i>Two-factor Authenticatie</i> in aanvulling op wachtwoorden is gebruikt bij het toepassen van externe toegang.					●
38	Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount draaien.		●	●	●	●
39	Indien tokens of biometrische toepassingen zijn gebruikt, is het niet mogelijk deze toepassingen eenvoudig buiten werking te stellen.		●	●	●	●
40	Wachtwoorden bestaan uit tenminste drie van de volgende elementen: hoofd- en kleine letters, leestekens en cijfers.		●	●	●	●
4.5	Beperking toegang tot informatie					
41	Bij het toekennen van autorisaties is tenminste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.		●	●	●	●
42	Hardware van een <i>TBB</i> -systeem is fysiek vast toegewezen aan dat systeem.		●	●	●	●
4.5	Beveiligde inlogprocedures					
43	Voorafgaand aan het aanmelden is aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.		●	●	●	●

44	Het aantal actieve sessies (werkplekken) per gebruiker is beperkt tot twee.					●
45	Het aantal actieve sessies (werkplekken) per gebruiker is beperkt tot één.		●	●	●	
46	Nadat voor een gebruikersaccount vijf maal een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockoutperiode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.					●
47	Nadat voor een gebruikersaccount drie maal een verkeerd wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten. De <i>Cyber-BF</i> verleent daartoe toestemming.				●	
48	Nadat voor een gebruikersaccount drie maal een verkeerd wachtwoord gegeven is, wordt het account geblokkeerd totdat de gebruiker verzoekt de lockout op te heffen of het wachtwoord te resetten. De <i>Cyber-BF</i> verleent daartoe toestemming.		●	●		
49	Nadat voor een beheerdersaccount drie maal een verkeerd wachtwoord gegeven is, wordt het account geblokkeerd totdat de IT-beheerder verzoekt de lockout op te heffen of het wachtwoord te resetten. De <i>Cyber-BF</i> verleent daartoe toestemming.		●	●	●	●
50	Het is niet toegestaan om gebruik te maken van groepsaccounts om gegevens te wijzigen in bedrijfskritieke applicaties die zelf geen <i>Identificatie-, Authenticatie-</i> en autorisatiemechanisme hebben.					●
51	Het is niet toegestaan om gebruik te maken van groepsaccounts.		●	●	●	

52	Groepsaccounts zijn toegestaan onder de volgende voorwaarden: - een groepsaccount is alleen in gebruik als er een grote operationele noodzaak is en het gebruik van persoonlijke accounts zeer ondoelmatig is; - de <i>Cyber-BF</i> verleent toestemming voor het gebruik van een groepsaccount; - het gebruik van een groepsaccount is te herleiden naar een natuurlijk persoon; - het is niet toegestaan om via externe toegang gebruik te maken van een groepsaccount; - het is niet toegestaan om toegang te hebben tot externe systemen (bijvoorbeeld het internet) met behulp van een groepsaccount; - het is niet toegestaan om persoonlijke of niet-werkgerelateerde informatie te verwerken met behulp van een groepsaccount.					●
53	Systeemaccounts zijn toegestaan onder de volgende voorwaarden: - het is niet toegestaan om via externe toegang gebruik te maken van een systeemaccount; - het is niet toegestaan om toegang te hebben tot externe systemen (bijvoorbeeld het internet) met behulp van een systeemaccount; - het is niet toegestaan om persoonlijke of niet-werkgerelateerde informatie te verwerken met behulp van een systeemaccount.		●	●	●	●
4.5	Systeem voor wachtwoordbeheer					
54	Er is automatisch gecontroleerd op het voldoen aan de wachtwoordpolicy.		●	●	●	●
55	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.		●	●	●	●
56	Wachtwoorden die gereset zijn en initiële wachtwoorden zijn uniek en niet hergebruikt.		●	●	●	
57	Gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende: - voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd; - ter voorkoming van typfouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.		●	●	●	●
58	Wachtwoorden zijn niet in originele vorm (plaintext) opgeslagen of verstuurd.		●	●	●	●
59	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het besturingssysteem.		●	●	●	

4.5	Speciale systeemhulpmiddelen gebruiken					
60	Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst, zijn afgesloten.		●	●	●	●
61	Alle onnodige programmatuur, services, protocollen en accounts zijn uitgeschakeld, evenals alle onnodige functionaliteiten zoals scripts, drivers, bestandssystemen en systeemhulpmiddelen.		●	●	●	●
62	De door de fabrikant van de gebruikte apparatuur minimaal voorgeschreven en aangeraden beveiligingsmaatregelen zijn uitgevoerd (<i>Hardening</i>).		●	●	●	●
4.5	Toegangsbeveiliging op programmabroncode					
63	De toegang tot <i>Broncode</i> is beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.		●	●	●	●
4.6	Cryptografie	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
4.6	Beleid inzake het gebruik van cryptografische beheersmaatregelen					
1	Voor de <i>Beveiliging</i> van TBB zijn door BIV / MIVD goedgekeurde cryptografische beveiligingsvoorzieningen, componenten en procedures gebruikt.		●	●	●	●
2	Er is een Cryptobeherder aangesteld. De Cryptobeherder voert voorts de taken uit als beschreven in de bijlage.	Bijlage 40	●	●	●	●
3	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Dit is vastgelegd in het <i>Beveiligingsplan</i> .		●	●	●	●
4.6	Sleutelbeheer					
4	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.		●	●	●	●
5	De geldigheidsduur van cryptografische sleutels is bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid als onderdeel van het <i>Beveiligingsplan</i> .		●	●	●	●
6	De <i>Vertrouwelijkheid</i> van cryptografische sleutels is gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.		●	●	●	●
7	Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.		●	●	●	●
4.7	Fysieke Beveiliging en Beveiliging van de omgeving	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
4.7	Beveiligde gebieden					

1	Systemen waarop zich een grote concentratie van ongerubriceerde of gemerkte <i>TBB</i> bevindt, zijn geplaatst in een ruimte die op <i>TBB</i> 4 niveau is beveiligd.	Bijlage 32				●
2	Systemen waarop zich een grote concentratie van <i>TBB</i> van Departementaal Vertrouwelijk bevindt, zijn geplaatst in een ruimte die op <i>TBB</i> 3 niveau is beveiligd.	Bijlage 32				●
3	Systemen waarop zich een grote concentratie van <i>TBB</i> van STG Confidentieel bevindt, zijn geplaatst in een ruimte die op <i>TBB</i> 2 niveau is beveiligd.	Bijlage 32			●	
4	Systemen waarop zich een grote concentratie van <i>TBB</i> van STG Geheim bevindt, zijn geplaatst in een ruimte die op <i>TBB</i> 1 niveau is beveiligd.	Bijlage 32		●		
4.7	Plaatsing en bescherming van apparatuur					
5	Apparatuur en bekabeling is zo geplaatst en beschermd dat risico's van schade en storing van buitenaf is geminimaliseerd.		●	●	●	●
6	Ter voorkoming van compromitterende emissies zijn <i>TEMPEST</i> maatregelen genomen. De maatregelen zijn vooraf afgestemd met <i>BIV</i> / <i>MIVD</i> .	Bijlage 36	●	●	●	
4.7	Onderhoud van apparatuur					
7	Apparatuur, software en gegevensdragers is geïnstalleerd, gebruikt en onderhouden volgens de voorschriften van de fabrikant voor zover dit past binnen het gebruik en onderhoudsplan van de organisatie.		●	●	●	●
8	Onderhoud vindt op locatie plaats en zijn uitsluitend toegestaan met toepassing van door <i>BIV</i> / <i>MIVD</i> goedgekeurde procedures.		●	●	●	●
4.7	Verwijdering van bedrijfsmiddelen					
9	Apparatuur, informatie en programmatuur van de organisatie is niet zonder toestemming vooraf van de locatie meegenomen. Bij <i>TBB</i> 1, <i>TBB</i> 2 en <i>TBB</i> 3 systemen geeft de <i>Cyber-BF</i> toestemming. Bij <i>TBB</i> 4 systemen de lijnmanager.		●	●	●	●
4.7	Veilig verwijderen of hergebruiken van apparatuur					
10	Hergebruik van <i>ICT-bedrijfsmiddelen</i> is toegestaan mits het dezelfde <i>TBB</i> betreft en is gewist door gebruik te maken van de door <i>BIV</i> / <i>MIVD</i> goedgekeurde middelen. Een procesverbaal van vernietiging (wissen) is opgesteld.	Bijlage 23.2.2	●	●	●	
4.7	Onbeheerde gebruikersapparatuur					
11	Bij het verlaten van de werkplek vergrendelt de gebruiker de werkplek (clear screen).		●	●	●	●
4.7	"Clear Desk"-beleid					

12	In het "clear-desk" beleid staat minimaal dat de gebruiker een <i>TBB</i> opbergt op de daartoe bestemde plaats indien men de Informatie niet gebruikt. Deze informatie is altijd opgeborgen in een afsluitbare opbergmogelijkheid van het juiste <i>TBB</i> niveau.		●	●	●	●
13	Bij het afdrucken van een <i>TBB</i> op een printer in een andere ruimte dan het werkstation is gebruik gemaakt van de functie "beveiligd afdrucken" (bijvoorbeeld pincode verificatie).		●	●	●	●
14	Een werkplek (sessie) is voor (<i>TBB1</i> en 2 na:5, <i>TBB3</i> na:10, <i>TBB4</i> na:15) minuten van inactiviteit automatisch geblokkeerd.		●	●	●	●
15	Toegangsbeveiligingslock is automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).		●	●	●	●
16	Voor het uitzetten/uitstellen van de schermbeveiliging op een bepaalde werkplek (sessie) gelden de volgende voorwaarden: - de schermbeveiliging is alleen uitgezet of uitgesteld als er een grote operationele noodzaak is; - voordat een schermbeveiliging wordt uitgezet of uitgesteld moet hiervoor toestemming verleend worden door de <i>Cyber-BF</i> ; - de <i>Cyber-BF</i> onderhoudt een registratie van werkplek (sessie) en de noodzaak waarom ontheffing is gegeven.		●	●	●	●
4.8	Beveiliging bedrijfsvoering	Verwijzing	<i>TBB 1 / ZG</i>	<i>TBB 2 / G</i>	<i>TBB 3 / C</i>	<i>TBB 4 / DV</i>
4.8	Gedocumenteerde bedieningsprocedures					
1	Bedieningsprocedures bevatten actuele en accurate informatie over opstarten, afsluiten, back-uppen en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures, speciale maatregelen voor <i>Beveiliging</i> en zijn beschikbaar gesteld aan alle gebruikers die deze nodig hebben.		●	●	●	●
2	Er zijn procedures voor de behandeling van gegevensdragers die ingaan op ontvangst, opslag, <i>Rubricering</i> , toegangsbeperkingen, verzending, hergebruik en vernietiging.		●	●	●	●
3	Systeemcomponenten - zoals <i>Firewall</i> , router, switches, servers - zijn in de basis ingericht volgens een standaard configuratie. Deze configuratie is vastgelegd en regelmatig gecheckt op actualiteit.		●	●	●	●
4	De verantwoordelijkheden en procedures voor het adequaat beheer en juist gebruik van de IT-voorzieningen waarin gerubriceerde informatie wordt verwerkt, zijn vastgesteld.		●	●	●	●
4.8	Wijzigingsbeheer					

5	Voor <i>TBB</i> systemen is een proces van wijzigingenbeheer ingesteld. Dit proces behelst minimaal: - het administreren van significante wijzigingen, activiteiten zijn tot de natuurlijke persoon te herleiden; - impactanalyse van mogelijke gevolgen van de wijzigingen; - goedkeuringsprocedure voor wijzigingen. De <i>Cyber-BF</i> is daarin opgenomen.		●	●	●	●
6	Instellingen van informatiebeveiligingsfuncties (b.v. securitysoftware) op het koppelveld tussen vertrouwde en onbetrouwbare netwerken, zijn automatisch op wijzigingen gecontroleerd.		●	●	●	●
4.8	Capaciteitsbeheer					
7	Op basis van een risicoanalyse is bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan zijn maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen, op te vangen. De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van <i>Beschikbaarheid</i> . Er zijn voorzieningen geïmplementeerd om de <i>Beschikbaarheid</i> van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik is actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.		●	●	●	●
8	Er zijn beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de <i>Beschikbaarheid</i> van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.		●	●	●	●
9	In koppelpunten met externe of onbetrouwbare segmenten zijn maatregelen getroffen om onder andere <i>DOS / DDOS</i> ((Distributed) Denial of Service attacks) aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is .		●	●	●	●
4.8	Scheiding van ontwikkel-, test- en productieomgevingen					
10	Er zijn gescheiden omgevingen voor Ontwikkeling, Test, Acceptatie en Productie (OTAP). De systemen en applicaties in deze omgevingen beïnvloeden systemen en applicaties in andere omgevingen niet.		●	●	●	●
11	Er is een fysieke scheiding aanwezig tussen de ontwikkel- en testomgeving (OT-omgeving) enerzijds en acceptatie- en de productieomgeving (AP-omgeving)		●	●	●	

	anderzijds.					
12	Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test, Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.		●	●	●	●
13	Indien er een experimenteer- of laboratorium omgeving is, is deze fysiek gescheiden van de andere omgevingen.		●	●	●	●
14	De scheiding tussen Ontwikkel-, Test-, Acceptatie- en Productiesystemen (OTAP-systemen) is ondersteund door formele overdrachtsprocedures.		●	●	●	●
15	Gegevens uit de productieomgeving zijn alleen in de Acceptatieomgeving in gebruik wanneer deze op dezelfde wijze beveiligd zijn als in de productieomgeving. Deze gegevens zijn niet in een Ontwikkel- of Testomgeving gebruikt.		●	●	●	●
4.8	Beheersmaatregelen tegen <i>Malware</i>					
16	Bij het openen van bestanden zijn deze geautomatiseerd gecontroleerd op <i>Malware</i> . De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, plaats.		●	●	●	●
17	Inkomende en uitgaande e-mails zijn gecontroleerd op <i>Malware</i> . De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, plaats.		●	●	●	●
18	Bestanden op een bestandssysteem, zowel server- als hostbased zijn automatisch gescand op <i>Malware</i> . Bij het aantreffen van <i>Malware</i> zijn deze in quarantaine geplaatst.		●	●	●	●
19	In verschillende schakels van een keten binnen de infrastructuur van een organisatie is anti- <i>Malware</i> programmatuur van verschillende leveranciers toegepast.		●	●	●	●
20	Er zijn maatregelen getroffen om verspreiding van <i>Malware</i> tegen te gaan en daarmee schade te beperken (bijv. quarantaine en <i>Compartimentering</i>).		●	●	●	●
21	Er zijn continuïteitsplannen voor herstel na aanvallen met <i>Malware</i> waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.		●	●	●	●
22	Gebruikers controleren alle van externen verkregen of door externen gebruikte digitale gegevensdragers met speciaal voor dit doel ingerichte <i>Scrubber</i> -functionaliteiten.		●	●	●	●
23	Afwijkingen van het normbeeld (anomalies) met betrekking tot sessies door perimeter devices zijn onderzocht op dreigingen zoals "covert channels". <i>Monitoring</i> op ongebruikelijke creaties, aanwezigheid en/of beëindiging van		●	●	●	●

	processen teneinde infiltratie te onderkennen, vindt continu plaats.					
4.8	Back-up van informatie					
24	Er zijn geteste procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.		●	●	●	●
25	Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.		●	●	●	●
26	Van back-upactiviteiten en de verblijfplaats van gegevensdragers is een registratie bijgehouden.		●	●	●	●
27	Back-ups zijn bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.		●	●	●	●
28	De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.		●	●	●	●
29	Back-ups zijn beveiligd conform de hoogste <i>Rubricering</i> van de gegevens.		●	●	●	●
30	Back-ups zijn minimaal één jaar en maximaal voor de duur van een project opgeslagen.		●	●	●	●
4.8	Gebeurtenissen registreren					
31	Per systeem zijn gebeurtenissen vastgelegd in de <i>Logging</i> . Zie bijlage voor de op te nemen gegevens. Op basis van risicoanalyse is vastgesteld welke aanvullende <i>Logging</i> noodzakelijk is. Deze <i>Logging</i> kan context-specifiek zijn. In het <i>Beveiligingsplan</i> zijn de resultaten van de analyse verwerkt/vastgelegd.	Bijlage 33	●	●	●	●
32	Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen zijn gegenereerd.	Bijlage 33	●	●	●	●
33	Controle op opslag van <i>Logging</i> : het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens is gelogd en leidt tot automatische alarmering van IT-beheer. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).		●	●	●	●
4.8	Beschermen van informatie in logbestanden					
34	Het (automatisch) overschrijven of verwijderen van logbestanden is gelogd in de nieuw aangelegde log.		●	●	●	●
35	Het raadplegen van logbestanden is voorbehouden aan IT-beheerders. Hierbij is de toegang beperkt tot leesrechten.		●	●	●	●

36	Logbestanden zijn zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.		●	●	●	●
37	De instellingen van logmechanismen zijn zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden is het vier-ogen principe toegepast.		●	●	●	●
38	De <i>Beschikbaarheid</i> van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden.		●	●	●	●
39	Loggegevens over een (vermoed) incident zijn gedurende vijf jaar bewaard.		●	●	●	●
40	Loggegevens dragen minimaal de <i>Rubricering</i> van de informatie waarop zij betrekking hebben.		●	●	●	●
4.8	Kloksynchronisatie					
41	Systeemklokken zijn zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.		●	●	●	●
4.8	Software installeren op operationele systemen					
42	Alleen geautoriseerd IT-beheer kan functies en software installeren of activeren.		●	●	●	●
43	Programmatuur is pas geïnstalleerd op een productieomgeving nadat een formele test en acceptatie procedure is doorlopen.		●	●	●	●
44	Er is alleen door de <i>Leverancier</i> onderhouden (versies van) software gebruikt.		●	●	●	●
45	Er is een rollbackstrategie.		●	●	●	●
46	Er is een integriteitcontrolemechanisme om ervoor te zorgen dat de <i>Integriteit</i> van programmatuur en systeembestanden behouden blijft.		●	●	●	●
47	Ongeautoriseerde programmatuur is gedetecteerd.		●	●	●	●
4.8	Beheer van technische kwetsbaarheden					
48	Er is een proces ingericht voor het onderkennen en <i>Mitigeren</i> van technische kwetsbaarheden; dit omvat minimaal penetratietests, risicoanalyses van kwetsbaarheden en patching.		●	●	●	●
49	Van softwarematige voorzieningen van de <i>Technische Infrastructuur</i> is gecontroleerd of de laatste updates (patches) zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken		●	●	●	●

	over zijn met de <i>Leverancier</i> .					
50	Kritische (security)updates en (security)patches zijn zo spoedig mogelijk doorgevoerd.		●	●	●	●
51	Het is niet toegestaan om een TOR (The Onion Router)/Darknet webbrowser te gebruiken		●	●	●	●
4.9	Communicatiebeveiliging	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV
4.9	Beheersmaatregelen voor netwerken					
1	Netwerken zijn voorzien van beheersmaatregelen voor routing gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.		●	●	●	●
2	Er zijn technische maatregelen getroffen om te voorkomen dat interne netwerkadressen naar buiten toe routeren.		●	●	●	●
3	Het gebruik van draadloze communicatie is niet toegestaan.		●	●	●	
4	Het gebruik van draadloze communicatie is toegestaan met toepassing van door BIV / MIVD goedgekeurde procedures en middelen.					●
5	In geval van een externe koppeling is een "Demilitarized Zone" (DMZ) toegepast. In de DMZ zijn <i>Monitoring systems</i> ingericht die tenminste <i>Packet Headers</i> informatie en bij voorkeur full packet header en payload van het data verkeer monitoren en loggen.					●
6	Alleen geïdentificeerde en geauthenticeerde apparatuur is aangesloten. De borging hiervan is beschreven in het <i>Beveiligingsplan</i> .		●	●	●	●
7	Blokkeer al het TOR (The Onion Router)/Darknet verkeer		●	●	●	●
8	Beperk op basis van een risicoanalyse het interne en externe dataverkeer tot de noodzakelijke protocollen en sessies.		●	●	●	●
9	Het netwerk is gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de <i>Betrouwbaarheid</i> van het netwerk niet onder het afgesproken minimum niveau komt.		●	●	●	●
10	Netwerken zijn gecontroleerd op ongeautoriseerde koppelingen.		●	●	●	●
11	Op aanwijzing van BIV / MIVD is medewerking verleend aan: - het plaatsen van monitoringboxen; - het monitoren van netwerkverkeer en hosts door gebruik van monitoringboxen.		●	●	●	●

4.9	Beveiliging van netwerkdiensten					
12	In geval van een externe koppeling is netwerkbased IDS of IPS <i>Monitoring</i> toegepast.					●
13	Een netwerkbased IDS of IPS is voorzien van actuele <i>Signatures</i> .					●
14	Er is een filter geïnstalleerd voor uitgaand dataverkeer.					●
15	Voor in- en uitgaand dataverkeer van en naar een onbeveiligde omgeving, zowel intern als extern, is in een <i>DMZ Proxy</i> -server en/of sandbox toegepast.	Bijlage 35				●
4.9	Scheiding in netwerken					
16	Een netwerk waarop <i>TBB</i> zijn opgeslagen, heeft geen verbinding met een ander netwerk, tenzij door <i>BIV / MIVD</i> goedgekeurde procedures en middelen zijn toegepast.		●	●	●	
17	De <i>Technische Infrastructuur</i> is ingedeeld in segmenten. Van systemen is bijgehouden in welk segment ze staan. Er is periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in het optimale segment zit of verplaatst moet worden.		●	●	●	●
18	Werkstations zijn zo ingericht dat routeren van verkeer tussen verschillende segmenten of netwerken niet mogelijk is.		●	●	●	●
19	Informatie die wordt overgedragen tussen netwerken en systemen kan <i>Malware</i> bevatten en is potentieel onveilig. Maatregelen zijn genomen om besmetting te voorkomen.		●	●	●	●
20	Elk segment heeft een gedefinieerd rubriceringsniveau. Bij overgang van segment vindt controle plaats op protocol, inhoud en richting van de communicatie.		●	●	●	●
21	Beheer en audit van segmenten vindt plaats vanuit een minimaal logisch gescheiden, separaat segment.		●	●	●	●
22	Segmentering is ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke.		●	●	●	●
23	Het netwerk is gesegmenteerd (<i>Compartimentering</i>) op basis van " <i>Need-to-be</i> ", " <i>Need-to-know</i> " en " <i>least privilege</i> " principes.		●	●	●	●
4.9	Beleid en procedures voor informatietransport					
24	Alle <i>TBB</i> die zich niet binnen het daarvoor bestemde fysieke compartiment bevindt is versleuteld. De toe te passen <i>Versleuteling</i> is goedgekeurd door <i>BIV /</i>		●	●	●	●

	<i>MIVD.</i>					
25	Een <i>TBB</i> is alleen verzonden over een onbeveiligde verbinding wanneer door BIV / <i>MIVD</i> goedgekeurde <i>Vercijfering</i> is toegepast.		●	●	●	●
26	Binnenkomende programmatuur (zowel op fysieke media als gedownload) is gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de <i>Leverancier</i> via een gescheiden kanaal geleverde checksum of certificaat.		●	●	●	●
27	Ontsluiting van <i>TBB</i> op een netwerk tussen verschillende bedrijfslocaties (<i>WAN</i>) is niet toegestaan.		●			
28	Ontsluiting van <i>TBB</i> op een netwerk tussen verschillende bedrijfslocaties (<i>WAN</i>) is alleen toegestaan indien de verbinding tussen de locaties van een door BIV / <i>MIVD</i> goedgekeurde <i>Vercijfering</i> is voorzien.			●	●	●
4.9	Cloudcomputing					
29	Het gebruik van een public Cloud-dienst (computing, opslag, transport) is niet toegestaan.		●	●	●	●
30	Het gebruik van een <i>Private Cloud-dienst</i> (computing, opslag, transport) is toegestaan.	Bijlage 8				○
31	<i>Private Cloud-dienst</i> (computing, opslag, transport) vindt plaats op Nederlands grondgebied, bij een Nederlandse rechtspersoon en met gebruik van personeel met de Nederlandse nationaliteit.					○
4.9	Virtualisatie					
32	Bij toepassing van <i>Virtualisatie</i> is een risicoanalyse uitgevoerd. De volgende voorwaarden zijn hierbij van toepassing: - securityfuncties draaien op fysiek gescheiden virtualisatieplatformen; - er zijn alleen systeemcomponenten gecombineerd die hetzelfde rubriceringsniveau hebben; - het ontwerp en implementatie is goedgekeurd door BIV / <i>MIVD</i> .	Bijlage 34	●	●	●	●
33	Het toepassen van VLAN's is alleen toegestaan in netwerken met een gelijk rubriceringsniveau. Het ontwerp en implementatie is goedgekeurd door BIV / <i>MIVD</i> .	Bijlage 34	●	●	●	●
4.10	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Verwijzing	<i>TBB 1 / ZG</i>	<i>TBB 2 / G</i>	<i>TBB 3 / C</i>	<i>TBB 4 / DV</i>
4.10	Analyse en specificatie van informatiebeveiligingseisen					
1	In projecten zijn beveiligingsrisicoanalyses en maatregelbepalingen opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen in het ontwerp zijn de beveiligingsconsequenties meegenomen. Deze zijn bij <i>Wijziging</i> en jaarlijks		●	●	●	●

	gecontroleerd op actualiteit.					
2	De samenhang tussen de <i>ICT-bedrijfsmiddelen</i> is in kaart gebracht in een netwerktekening.	Bijlage 27	●	●	●	●
4.10	Principes voor engineering van beveiligde systemen					
3	Er zijn controles uitgevoerd op de invoer van gegevens. Daarbij is minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen en inconsistentie van gegevens.		●	●	●	●
4	Het <i>Informatiesysteem</i> bevat functies waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.		●	●	●	●
5	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen.		●	●	●	●
4.10	Systeemacceptatietests					
6	Van acceptatietesten is een log bijgehouden.		●	●	●	●
7	Er zijn acceptatiecriteria vastgesteld voor het testen van de <i>Beveiliging</i> .		●	●	●	●
8	Voordat systemen en/of componenten in productie genomen zijn, zijn testgegevens en testaccounts verwijderd.		●	●	●	●
9	Acceptatie van systemen/software vindt plaats nadat vastgesteld is dat de <i>ABDO</i> beveiligingsmaatregelen daadwerkelijk zijn geïmplementeerd.		●	●	●	●
4.11	Leveranciersrelaties	Verwijzing	<i>TBB 1 / ZG</i>	<i>TBB 2 / G</i>	<i>TBB 3 / C</i>	<i>TBB 4 / DV</i>
4.11	Informatiebeveiligingsbeleid voor leveranciersrelaties					
1	Indien een externe partij betrokken is bij het beheer van een <i>TBB</i> omgeving, is voor deze partij door <i>BIV / MIVD</i> een <i>ABDO-Autorisatie</i> afgegeven.	Bijlage 8	●	●	●	●
2	Indien dataopslag van een <i>TBB</i> door een externe partij is gefaciliteerd, is voor deze partij door <i>BIV / MIVD</i> een <i>ABDO-Autorisatie</i> afgegeven.	Bijlage 8	●	●	●	●

5 Verklaring gebruikte afkortingen en begrippen

ABDO	Algemene Beveiligingseisen voor Defensieopdrachten. Voorschriften voor het adequaat Beveiligen van Te Beschermen Belangen, Bijzondere Informatie in het bijzonder, die aan een partij buiten de Rijksdienst zijn toevertrouwd.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst die namens de minister van Binnenlandse Zaken en Koninkrijksrelaties is belast met de zorg voor de staatsveiligheid.
APT	Advanced Persistent Threat. Een langdurige, complexe en doelgerichte digitale aanval met spionage als doel.
Authenticatie	Het proces waarbij wordt nagegaan of een persoon, een (andere) computer of applicatie daadwerkelijk is wie hij beweert te zijn.
Autorisatie	Het proces waarin aan een persoon, een (andere) computer of applicatie rechten worden toegekend tot het benaderen van een terrein, gebouw, systeem, gegevensbestand, etc.
Baseline	Een verzameling van technische beheersingsmaatregelen of instellingen voor de

	inrichting van een IT-middel, zonder rekening te houden met de eisen van een specifieke IT-dienst. Een baseline fungeert als uitgangspunt voor de beveiligingsstandaarden van specifieke IT-diensten.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beheer op afstand	Het extern uitvoeren van beheerwerkzaamheden op apparatuur intern de organisatie.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers of systemen op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Betrouwbaarheid	De mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening. (VIR 94)
Beveiligen	Het beschermen van een TBB, BI in het bijzonder, tegen toegang of kennisname door niet-gerechtigden.
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuity Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsfunctionaris	Beveiligingsfunctionaris (BF). De functionaris die is belast met de implementatie en uitvoering van de voorgeschreven beveiligingsmaatregelen.

Beveiligingsincident	Een beveiligingsincident is een (vermeende) gebeurtenis die kan leiden of heeft geleid tot een verstoring van de normale gang van zaken aangaande de integrale beveiliging, als gevolg waarvan de belangen van de Staat c.q. van een of meer ministeries, en/of van medewerkers, externen en bezoekers in gevaar gebracht zijn of kunnen worden
Beveiligingsplan	Opsomming van alle getroffen beveiligingsmaatregelen en/of de vindplaatsen daarvan welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht zijn.
Beveiligingsstandaard	Een verzameling van technische beheersingsmaatregelen of instellingen voor de inrichting van een IT-middel gericht op een specifieke IT-dienst
Beveiligingsverdrag	Een bilateraal verdrag dat de uitwisseling en wederzijdse bescherming van gerubriceerde informatie tussen twee landen faciliteert.
Bijzondere Informatie	Staatsgeheimen en overige bijzondere 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(BI) is informatie die voorzien is van een Rubricering en op grond daarvan moet worden beveiligd.
BO	Bijzondere Opdracht. Een opdracht vanuit de overheid als Opdrachtgever aan een civiele partij als Opdrachtnemer waarbij een TBB betrokken is.
Blacklist	Een zwarte lijst met bijvoorbeeld domeinen of IP adressen waarmee geen digitale communicatie mag plaatsvinden.

Broncode	Een computerprogramma in leesbare vorm zoals die door de programmeur in een programmeertaal is geschreven.
BIV / MIVD	Bureau Industrieveiligheid (BIV) van de MIVD dat namens Defensie toeziet op de beveiliging van TBB bij Opdrachtnemers en de onderaannemers hiervan.
BYOD / CYOD	Bring Your Own Device. De mogelijkheid voor een medewerker eigen apparatuur te gebruiken voor zakelijke toepassing
	Choose Your Own Device. De mogelijkheid voor een medewerker te kiezen uit een aantal door het bedrijf aangeboden apparaten.
CA / RA	Certificaat Autoriteit. De CA waarborgt de integriteit en authenticiteit van certificaten en garandeert de identiteit van de certificaatbezitter.
	Registratie Autoriteit. De RA stelt vast aan wie een certificaat kan worden verstrekt en controleert de uitgifte ervan
CCTV	Closed Circuit Television. Een gesloten systeem van camera's als hulpmiddel bij het voorkomen en verwerken van incidenten.
Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Cloudcomputing	Het via een netwerk, op aanvraag beschikbaar stellen van hardware, software en gegevens.
Code Security Review	Software die ondersteunt bij het vinden van fouten in de broncode van software.
Command & Control (C2)	Infrastructuur (servers en andere componenten), als

server	doelwit gebruikt om Malware aan te verspreiden en/of deze aan te sturen, in het bijzonder botnets of APT's.
Compartimentering	Het aanwijzen en Beveiligen van gewoonlijk afgescheiden fysieke dan wel digitale locaties waar een TBB mag worden verwerkt of opgeslagen, alsmede het aanwijzen van (groepen van) personen die toegang mogen hebben tot of kennis mogen nemen van een TBB.
Compromittatie	De ongeautoriseerde toegang tot of kennisname van een TBB, meestal BI.
Configuration Item (CI)	IT-middel dat van belang is voor een te leveren IT-dienst
Configuration management database (CMDB)	Een gestructureerde verzameling van gegevens (database) van relevante details van configuration items en gegevens over hun onderlinge relaties.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere “werkelijkheden of representaties daarvan” zodat objectieve oordeelsvorming mogelijk wordt.
COTS	Commercial off the Shelf. Een term om commerciële goederen en diensten aan te duiden die direct op de markt beschikbaar zijn.
Cryptofunctie	Een vertrouwensfunctie waarin behandeling van of kennisname van CRYPTO, CRYPTO-SECURITY of CRYPTO CONTROLLED ITEM (CCI)-gemarkt materiaal noodzakelijk is.
CUI	Controlled Unclassified Information / Item. Een categorie informatie of goederen die in het kader van de Amerikaanse ITAR, hoewel ongerubriceerd,

	een zekere mate van beveiliging vereist.
Cyber	Omvat naast de IT-infrastructuur ook het stelsel van activiteiten (o.a. bedrijfsvoering) wat met de infrastructuur mogelijk wordt gemaakt. Het zijn juist die activiteiten die beschermd moeten worden. Vaak als voorvoegsel gebruikt voor nadere specificering van begrippen (zoals: cybercrime, cybersecurity, cyberdreiging).
Darknet	Deel van het World Wide Web waarvan de inhoud alleen met behulp van specifieke software (browser) en/of configuraties toegankelijk is.
DBB	Het Defensie Beveiligingsbeleid zoals omschreven in aanwijzing SG/003.
Defensieopdracht	Een overeenkomst tussen (de Staat der Nederlanden ten behoeve van) het Ministerie van Defensie of een buitenlandse defensie instantie enerzijds en een natuurlijke of rechtspersoon anderzijds, waarbij overdracht of behandeling van Informatie, Materieel, Goederen of objecten plaatsvindt.
DMZ	Demilitarised zone. Een fysiek of logisch deel van het netwerk dat de extern, vanuit het Internet te benaderen services van een organisatie bevat, zonder dat de interne services en werkstations rechtstreeks te benaderen zijn (bijvoorbeeld mail- en webservers).
DV	Departementaal Vertrouwelijke Informatie is Bijzondere Informatie met de laagst mogelijke rubricering. DV wordt niet als Staatsgeheim aangemerkt maar behoeft wel een bepaald niveau van beveiliging.
Definitieve Autorisatie	De verklaring van BIV / MIVD aan de Opdrachtgever

	dat vanuit beveiligingsoogpunt geen bezwaar bestaat tegen gunning van een BO aan de geselecteerde Opdrachtnemer.
Dienstverlener (service provider)	Een bedrijf dat diensten aanbiedt. De term service provider wordt vaak geassocieerd met internet- en telefoniediensten.
Disclosure	De ontsluiting van een TBB waardoor dit ter beschikking of ter kennis wordt gesteld aan derden.
DoS / DDoS	Denial of Service. Het onbruikbaar maken van een computer, computernetwerk of dienst door overbelasting van de bandbreedte, geheugen- of verwerkingscapaciteit. Distributed Denial of Service. De DoS aanval wordt vanaf meerdere computers tegelijkertijd uitgevoerd.
Document(en)	Al datgene waarin gegevens ter raadpleging zijn vastgelegd (zoals een brief, aantekening, rapport, memorandum, bericht, telegram, tekening, foto, film, kaart, tabel, aantekenboek, stencil, magnetische en optische gegevensdrager enz.).
Elektronische Handtekening	Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van cryptografische technieken. De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie "ondertekent". De technieken worden toegepast met behulp van een PKI.
Encryptie	Zie Vercijfering.
Escrow Agent	Een betrouwbare derde partij waar sleutels of Broncode zijn opgeslagen.

ETS	Elektronisch Toegangsbeheer Systeem.
EU	Europese Unie.
Firewall	Het geheel van software- en eventueel ook hardware voorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de veiligheid in de laatstgenoemde te verhogen.
Facility Security Clearance	Facility Security Clearance (FSC) (Certificate FSCC).De verklaring van BIV / MIVD aan een (doorgaans buitenlandse) aanvrager dat een bedrijf vanuit beveiligingsoptiek in staat is een BO uit te voeren.
FTP	File Transfer Protocol. Een protocol dat uitwisseling van bestanden tussen computers faciliteert.
Gerubriceerde Opdracht	Een Defensieopdracht waarbij Bijzondere Informatie ter kennis van een externe organisatie moet worden gebracht of daarbij wordt gegenereerd.
Geheimhoudings-verklaring	De verklaring waarin men aangeeft bekend te zijn met voorschriften en verplichtingen aangaande het omgaan met een TBB, BI in het bijzonder.
Goederen	Alle materiële en immateriële zaken (producten en diensten) die kunnen worden gebruikt om in behoeften te voorzien.
Hardening	Het proces van systeembeveiliging door verkleining van de aanvalsmogelijkheden in een systeem. Dit wordt onder andere gerealiseerd door overbodige functies in besturingssystemen uit te schakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
Honeypot of Honeynet	Een computersysteem of -netwerk dat zich bewust

	kwetsbaar opstelt voor (worm)virussen en andere aanvallen, zodat de aanvaller en/of zijn eigenschappen zichtbaar worden.
Hypervisor	Een opstelling (software) die ertoe dient om meerdere besturingssystemen tegelijkertijd op een hostcomputer te laten draaien.
Identificatie	Het kenbaar maken van de identiteit van een subject (een gebruiker of een proces).
IDS(S)	Indringer Detectie en Signalering (Systeem).
Incident	Onder incident wordt verstaan elke gebeurtenis, die niet tot de standaardoperatie van een IT-service behoort en die een interruptie in of een vermindering van de kwaliteit van die service kan veroorzaken. Onder incident worden niet verstaan: elk verzoek van de gebruiker om ondersteuning, levering van informatie, advies of documentatie (ook wel aangeduid als "Service Request")
Informatie	Kennis die in welke vorm dan ook overdraagbaar is. Hieronder worden zowel Documenten verstaan als materieel waarin kennis opgeslagen kan worden c.q. waaruit kennis af te leiden valt.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het

	informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan.
Interventie	Interventie is de reactie op een alarmering (vermoeden van schending TBB) met als doel de alarmering te verifiëren en indien nodig de schending van het TBB te doen stoppen dan wel het TBB veilig te stellen. Het betreft daarom het geheel van maatregelen en/of activiteiten met als doel om aantasting van het beveiligingsniveau van een TBB te voorkomen of te herstellen.
Interventietijd	De tijd tussen detectie/verificatie van een poging tot inbraak en het ter plaatse ingrijpen door de bewaking, politie of defensiepersoneel.
Introspectieve Capaciteit	Het vermogen van een IDS om de interne activiteiten van een systeem (netwerk) op legitimiteit te beoordelen en zonodig actie te ondernemen.
IP-adres	Internet Protocol adres. Een numeriek label aangebracht op een apparaat (bv. computer, printer) dat deel uitmaakt van een netwerk dat het Internet Protocol gebruikt voor communicatie.
IRP	Incident Response Procedure. Een procedure waarin is opgenomen welke stappen in onderzoek en afhandeling moeten worden uitgevoerd als een Incident wordt gemeld.
ITAR	International Traffic of Arms Regulations.
ICT-Bedrijfsmiddelen	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.
Leverancier	Een bedrijf dat goederen of diensten levert in ruil

	voor geld.
Logging	Het vastleggen van gegevens die betrekking hebben op (pogingen tot) de toegang (zowel fysiek als digitaal) tot een TBB.
LvV	Lijst van Vertrouwensfuncties. Het overzicht van aantallen Vertrouwensfuncties ingedeeld naar functiecategorie en Veiligheidsmachtigingsniveau.
Malware	Software met ongewenste / kwaadaardige functies, zoals virussen en trojans.
WAN	Wide Area Network. Een term voor de koppeling van Local Area Networks (LAN) over een stedelijk of groter geografisch gebied.
Materieel	De Legerbehoefte zoals wapens, munitie, voertuigen, etc., onverschillig of zij tot gebruik of tot verbruik bestemd zijn.
Memorandum of Understanding	Zie Security MoU
Merking	Aanduiding op een TBB die een bepaalde wijze van behandeling en beperking van verspreiding inhoudt.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst die namens de minister van Defensie is belast met de zorg voor de staatsveiligheid.
MISWG	Multinational Industrial Security Working Group. Een informeel samenwerkingsverband op het gebied van Industrieveiligheid.
Mitigeren	Het minimaliseren van het effect van een (digitale) Compromittatie
Monitoring	Het meten van datastromen ('flows') en activiteiten in een netwerk via digitale poorten.
NAT	Netwerk Adres Translatie is een verzamelnaam voor technieken die gebruikt worden ter afscherming van private IP-adressen voor de buitenstaander voor wie

	dan alleen het enkele publiek bekende IP-adres zichtbaar is.
NAVO	Noord Atlantische Verdrags Organisatie.
NBV	Het Nationaal Bureau Verbindingsbeveiliging voorziet de Rijksoverheid van voornamelijk technische middelen (Cryptografie) voor de beveiliging van Bijzondere Informatie.
Need-to-Be	Een Vertrouwensfunctionaris heeft slechts fysieke toegang tot ruimten en locaties waar Vitale Informatie voorhanden is als dat nodig is om zijn werk te kunnen doen. Niet vertrouwensfunctionarissen hebben nooit toegang.
Need-to-Know	Een Vertrouwensfunctionaris mag slechts van Bijzondere Informatie kennisnemen als dat nodig is om zijn werk te kunnen doen. Bovendien mag hij deze kennis niet met collega's delen voor wie deze kennis niet noodzakelijk is en/of geen vertrouwensfunctionaris zijn.
Netwerk Perimeter Devices	Apparaten die op het grensvlak van het vertrouwde netwerk zorgdragen voor beveiliging, toegang, verzending of ontvangst van data.
Netwerksegmentatie	Het opsplitsen van een netwerk in kleine coherente delen teneinde Compromittatie van grotere delen van een netwerk in één actie te bemoeilijken.
Object(en)	Door de mens geproduceerd of gerealiseerd voorwerp, constructie of kunstwerk.
Onderhoud op afstand	Het extern uitvoeren van onderhoudswerkzaamheden op apparatuur intern de organisatie.
Opdrachtgever	(De Staat der Nederlanden ten behoeve van) de Rijksoverheid dan wel een natuurlijke of

	rechtspersoon of een buitenlandse instantie die een Bijzondere Opdracht (BO) verstrekt.
Opdrachtnemer	Een natuurlijke persoon of een juridische entiteit (een rechtspersoon als bedoeld in boek 2 van het Burgerlijk Wetboek dan wel een maatschap als bedoeld in boek 7A van het Burgerlijk Wetboek, of een vennootschap onder firma of een commanditaire vennootschap als bedoeld in boek 1, derde titel van het Wetboek van Koophandel) die bij een Defensieopdracht wordt betrokken dan wel een Defensieopdracht heeft ontvangen en aanvaard, alsmede derden nadat zij bij de uitvoering van een dergelijke opdracht zijn betrokken.
OPG	Opgave Persoonlijke Gegevens op basis waarvan een Veiligheidsonderzoek wordt uitgevoerd.
Packet Headers	Data die aan het begin van een digitaal blok is geplaatst, benodigd voor interpretatie van de te transporteren data.
Partner	Onder partner wordt verstaan: - echtgenoot, echtgenote of geregistreerd partner van betrokkene; - degene waarmee betrokkene een gezamenlijke huishouding voert, tenzij het betreft een bloedverwant in de eerste of tweede graad; - degene ten aanzien van wie uit het veiligheidsonderzoek blijkt dat deze een affectieve relatie met betrokkene onderhoudt, tenzij het betreft een bloedverwant in de eerste of tweede graad.
Patch	Onderdeel van software dat de leverancier van

	software uitgeeft om fouten aan door hem vervaardigde software te repareren
Penetratietest	Een toets op kwetsbaarheden van een of meerdere computersystemen met als doel de systemen beter te beveiligen.
Phishing	Het trachten informatie te ontfutselen aan mensen door hen te lokken naar een valse website, die een kopie is van een bekende, bestaande website. De aanvaller doet zich hierbij voor als een vertrouwde instantie of persoon, veelal via een e-mail met besmette files.
Private Cloud-dienst	Een vorm van Cloud-computing waarbij, op specifiek toegewezen (geïsoleerde) hard- en software, gegevens beschikbaar worden gesteld aan de opdrachtnemer.
Privileged Accounts	Een gebruikersaccount dat over aanvullende rechten beschikt zoals bijvoorbeeld; - Beheerder accounts - Service accounts - Calamiteiten accounts - Change accounts - Groepsaccounts
Proxy	Een computersysteem dat of applicatie die als een intermediair functioneert tussen verzoeken van werkstations en resources van servers.
PKI	PKI (Public Key Infrastructure) ondersteunt uitgifte en beheer van digitale certificaten. PKI geeft gebruikers extra garanties over via netwerken uitgewisselde informatie. De garanties die een PKI verstrekt, zijn een grotere zekerheid betreffende verzender en ontvanger van de uitgewisselde informatie.

PSC(C)	Personnel Security Clearance (Certificate). De verklaring dat een persoon is geautoriseerd tot toegang of kennisname van een TBB, BI in het bijzonder.
PSI	Project Security Instruction. Een Document waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van een buitenlandse opdracht.
Rijksdienst	De ministeries met hun directoraten-generaal, centrale en stafdirecties, buitendiensten en intern verzelfstandigde dienstonderdelen.
Rijksoverheid	De Rijksoverheid, als onderdeel van de Nederlandse overheid, is de bestuurslaag op landelijk niveau en wordt gevormd door alle ministeries en de uitvoeringsorganisaties die onder de verantwoordelijkheid van een minister vallen.
Rubricering	Het vaststellen en aangeven dat een TBB Bijzondere Informatie is of bevat, alsmede het bepalen en aangeven van de mate van beveiliging daarvan.
RAL	Rubriceringsaanduidingslijst. Een lijst die in het kader van een BO per onderwerp de rubricering van het daarop betrekking hebbende TBB aangeeft.
RfV	RequestforVisit. Het verzoek aan de betrokken veiligheidsautoriteiten om toestemming voor een bezoek aan een defensielocatie of een bedrijf in het buitenland.
SAL	Security Aspect Letter. Een Document waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van kleinere buitenlandse projecten.
Screening	Zie Veiligheidsonderzoek.
Scrubber	Een standalone systeem dat informatiedragers controleert op de aanwezigheid van Malware en

	deze zonodig onschadelijk maakt.
Security MoU	Memorandum of Understanding. Een bilaterale overeenkomst tussen partijen waarin wederzijdse beveiligingsafspraken zijn vastgelegd.
SG	De Secretaris-generaal van het betrokken ministerie.
Signatures	Eigenschappen van Malware op basis waarvan herkenning kan plaatsvinden.
Social Engineering	Het onder valse voorwendselen verzamelen van informatie uit communicatie waarbij wordt gebruikgemaakt van de intrinsieke motivatie van een ander behulpzaam te zijn, met het oogmerk toegang tot een TBB, BI in het bijzonder, te verkrijgen.
Staatsgeheim	Bijzondere Informatie waarvan de geheimhouding vanwege het belang van de Staat of zijn bondgenoten is geboden.
Staat Van Inlichtingen (SVI)	Staat van Inlichtingen op basis waarvan een Veiligheidsonderzoek wordt uitgevoerd.
Subcontractor	Een bedrijf waaraan de Opdrachtnemer bepaalde werkzaamheden aan een TBB uitbesteed.
TBB	Te Beschermen Belang. Alle Informatie, Materieel, Goederen en objecten die een zekere mate van bescherming behoeven zijn door Defensie ingedeeld in een viertal categorieën Te Beschermen Belang (TBB 1 tot en met TBB 4, waarbij TBB 1 de zwaarst te Beveiligen categorie is).
Technische Infrastructuur	Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database

	management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
<i>Toeleverancier</i>	Een bedrijf dat goederen levert aan een ander bedrijf dat die Goederen op zijn beurt verwerkt in een door de eindgebruiker gewenst product.
<i>TEMPEST</i>	Het tegengaan van mogelijk compromitterende emissie van elektronische systemen die kan leiden tot het onbevoegd opvangen, verwerken en reproduceren van data.
<i>Two-factor authenticatie</i>	Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: 1. iets dat de gebruiker weet (b.v. password, PIN); 2. iets dat de gebruiker heeft (b.v. toegangspas, sleutel); en 3. iets dat de gebruiker is (b.v. biometrische eigenschap zoals een vingerafdruk).
<i>Spanpoort</i>	Een fysieke poort op een actieve component (router of switch) die het mogelijk maakt diagnose op een apparaat of netwerkverkeer te verrichten
<i>Uitsteltijd</i>	De tijd tussen detectie/verificatie van een inbraak en Compromittatie van een TBB.
<i>unPrivileged accounts</i>	Een gebruikersaccount dat over beperkt rechten beschikt zoals bijvoorbeeld; - Gebruiker accounts
<i>Veiligheidsonderzoek</i>	Het proces dat leidt tot afgifte, weigering, verlenging of intrekking van een VGB.
<i>Vercijfering</i>	Het door middel van een algoritme zodanig wijzigen van informatie dat deze onleesbaar en onbegrijpelijk is voor niet-gerechtigden.
<i>Vertrouwd(e)</i>	In overeenstemming met een door een bevoegde

	autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken.
<i>Vertrouwelijke Informatie</i>	Informatie die niet algemeen bekend mag worden (bron: van Dale) In het kader van de BIR:2012 worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met departementaal vertrouwelijk (volgens definitie uit VIRBI) en persoonsvertrouwelijke informatie van risicoklassen 1 en 2 zoals gedefinieerd de toelichting op de WBP: AV23
<i>Vertrouwelijkheid</i>	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
<i>Verwijderbare Gegevensdragers</i>	Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CRDROMs, USB sticks, verwijderbare schijven, tapes of gedrukte media.
<i>Vertrouwensfunctie</i>	Een functie die in beginsel de mogelijkheid biedt de veiligheid of andere gewichtige belangen van de Staat te schaden.
<i>Vertrouwensfunctionaris</i>	Een persoon die op een vertrouwensfunctie geplaatst is.
<i>Veiligheidsbriefing</i>	Een voorlichting met als doel het beveiligingsbewustzijn te vergroten.
<i>VGB</i>	Verklaring van Geen Bezwaar. De verklaring dat uit het oogpunt van de nationale veiligheid geen bezwaar bestaat tegen vervulling van een bepaalde Vertrouwensfunctie door een bepaald persoon.
<i>VMN</i>	Veiligheidsmachtigingsniveau. Het voor de Vertrouwensfunctie vereiste niveau waarop het

	Veiligheidsonderzoek moet worden uitgevoerd (A, B dan wel C).
Virtualisatie	Het op een virtuele wijze creëren van een computersysteem in plaats van een combinatie van hard- en software. Hierbij werken computers, operating systemen, dataopslag systemen en andere actieve componenten virtueel samen.
Vitaal	De term waarmee een opdracht wordt aangemerkt als deze betrekking heeft op TBB waarvan aantasting een nadelige invloed heeft op de bedrijfsvoering van de Staat, Defensie of zijn bondgenoten. Aan een Vitale Opdracht kan een Rubricering worden toegekend.
VOG	Verklaring Omtrent Gedrag. Een verklaring van de Dienst Justis van het Ministerie van V&J benodigd voor toegang tot of kennisname van informatie op DV-niveau.
Voorlopige autorisatie	De verklaring van BIV / MIVD aan de Opdrachtgever dat er vanuit beveiligingsoogpunt geen bezwaar bestaat tegen een bedrijf als kandidaat Opdrachtnemer.
VPN	Virtual Private Network. Een gecijferde verbinding tussen twee systemen, waarbij de integriteit en de vertrouwelijkheid van de data gewaarborgd blijft.
Wateringholes	Een strategie waarbij een aanvaller een website infecteert met Malware na te hebben vastgesteld dat een bepaalde groep gebruikers die website regelmatig bezoekt.
Wet op de inlichtingen- en veiligheidsdiensten	De Wet op de inlichtingen- en veiligheidsdiensten zoals gepubliceerd 2002 (zie stb. 2002, 148) of de

(Wiv)	rechtsopvolger.
Wet veiligheidsonderzoeken (Wvo)	De Wet veiligheidsonderzoeken zoals gepubliceerd 1996 (zie stb. 1996, 525) en gewijzigd in 2015 (zie stb. 2015, 208).
Wetboek van strafrecht (Wvs)	Het wetboek van strafrecht waarin ondergebracht de Nederlandse strafwet die toepasselijk is op een ieder die zich in Nederland aan enig strafbaar feit schuldig maakt.
Wijziging	Elke toevoeging, verandering of verwijdering in een IT-dienst of IT-middel.
Zeggenschap	Onder “Zeggenschap” wordt verstaan de mogelijkheid op grond van feitelijke of juridische omstandigheden een 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.
Zero-day	Een (onbedoelde) kwetsbaarheid in software die nog onbekend is bij de softwareontwikkelaar en anderen. Een Zero-day-exploit is software die misbruik maakt van een dergelijke kwetsbaarheid in de software.
Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen

6 Inhoudsopgave bijlagen

1	Tabel meest voorkomende <i>Merkingen</i> gekoppeld aan <i>TBB</i> -categorie
2	Tabel Buitenlandse <i>Rubriceringen</i>
3	Inrichten beveiligingsorganisatie
4	<i>Beveiligingsfunctionaris</i>
5	Bedrijfsstructuur, eigendom en <i>Zeggenschap</i>
6	Beveiligingsbewustzijn
7	Rubriceringsaanduidingslijst
8	Logistieke keten
9	Incident Handling procedure
10	<i>Vertrouwensfuncties</i>
11	<i>Veiligheidsonderzoek</i>
12	Verklaring van bekendheid met de geheimhoudingsplicht voor <i>Vertrouwensfunctionarissen</i>
13	Toestemming tot plaatsing van een persoon die niet beschikt over de Nederlandse nationaliteit op een <i>Vertrouwensfunctie</i>
14	Wijziging persoonlijke omstandigheden
15	Ontheffing uit een <i>Vertrouwensfunctie</i>
16	Reizen naar het buitenland
17	Beveiligingsmaatregelen en schillenstructuur
18	Organisatorische maatregelen
19	Bouwkundige maatregelen
20	Elektronische maatregelen
21	Reactieve maatregelen

22	Transport en verzenden van een <i>TBB</i>
23	Fysieke opslag, verwerking, ontwikkeling en vernietiging
24	Cyber <i>Beveiligingsfunctionaris</i>
25	Goedkeuring middelen
26	Cybersecurity Awareness training
27	Registratie van ICT-bedrijfsmiddelen
28	Mobiele apparatuur en <i>BYOD</i>
29	Systeemdokumentatie
30	Labelen van gegevensdragers
31	Gebruikers, IT-beheerders en accounts
32	Grote concentratie <i>TBB</i>
33	Logging en monitoring
34	<i>Virtualisatie</i>
35	<i>DMZ</i>
36	TEMPEST
37	Zelfinspectierichtlijnen
38	Identificatie van werkstations
39	Daderprofiel (GERUBRICEERD)
40	Cryptofunctionaris

	Procedure ABDO	
--	-----------------------	--

Inschakeling van bedrijven in het kader van een defensiecontract waarbij ABDO van toepassing is.

BIV / MIVD neem contact op met een potentiële *Opdrachtnemer* op verzoek van de volgende aanvragers:

1. de inkoper of projectleider van Defensie (bij voorkeur via de Beveiligingscoördinator) of;
2. een buitenlandse Defensieorganisatie (bilateraal, NAVO, EU) of;
3. een reeds gecontracteerde *Opdrachtnemer* die werkzaamheden of leveranties in het kader van een *BO* wil uitbesteden aan een *Subcontractor*. In deze situatie vervult de *Opdrachtnemer* de rol van *Opdrachtgever* en de *Subcontractor* de rol van *Opdrachtnemer*.

NB: *BIV / MIVD* neemt geen contact op met een potentiële *Opdrachtnemer* wanneer dit op verzoek van een bedrijf is dat een *ABDO*-autorisatie wil verkrijgen om zo voor een *BO* in aanmerking te komen. NAVO- of EU-inschrijvingsprocedures (tenders) waarin vooraf een *Facility Security Clearance (FSC)* wordt verlangd, vormen hierop een mogelijke uitzondering.

Een *Opdrachtnemer* waaraan een *BO* wordt gegund dient te voldoen aan de *ABDO 2017*. Deze *ABDO 2017* is in het contract tussen Defensie en *Opdrachtnemer* als contractvoorwaarde bedongen. De verklaring dat een *Opdrachtnemer* aan de *ABDO 2017* voldoet, wordt afgegeven aan de aanvrager en de *Opdrachtnemer* in de vorm van een *ABDO*-autorisatie per *BO*. Deze autorisatie is bij de *Opdrachtnemer* pas na gunning van de *BO* afgegeven.

Voordat een *TBB* in enige vorm wordt verstrekt aan een *Opdrachtnemer*, heeft de aanvrager deze autorisatie van *BIV / MIVD* ontvangen. De autorisatie wordt verstrekt per opdracht en heeft geen betrekking op het zaken doen met een bepaald bedrijf in zijn algemeenheid. Slechts bij uitzondering, wanneer sprake is van een doorlopende stroom van *BO*, wordt een algemene autorisatie afgegeven, steeds voor de duur van maximaal vijf jaar;

In het proces dat leidt tot gunning van *BO* door Defensie aan bedrijven, waarbij aan die bedrijven *TBB* worden toevertrouwd en/of bij die bedrijven in opdracht worden gegenereerd, worden drie fasen onderscheiden: de oriëntatiefase, de onderhandelingsfase/offertefase en de gunningsfase.

Oriëntatiefase

In de oriëntatiefase dient zo vroeg mogelijk het bijzondere karakter van een opdracht te worden vastgesteld. Hiertoe wordt overleg gevoerd tussen de behoeftesteller, de inkoper (*Opdrachtgever*), de projectleider, de Beveiligingscoördinator (BC) en zo nodig de Beveiligingsautoriteit (BA). Daarbij wordt bepaald welke merking, *TBB*-categorie en/of rubriceringsniveau van toepassing is en daarmee welk beveiligingsniveau uit de *ABDO 2017* moet worden opgenomen in het contract.

Vervolgens wordt een *Rubriceringsaanduidingslijst* (RAL, **bijlage 7**) opgesteld waarmee de aanvrager informatie over de aard van de te verstrekken opdracht verschaft en, waar van toepassing, per onderwerp de merking, de *TBB*-categorie en/of de hoogte van de rubricering vastlegt.

De aanvrager meldt, voordat contact wordt opgenomen met potentiële *Opdrachtnemers*, zijn voornemen tot oriëntatie bij zijn BC en geeft aan welke bedrijven mogelijk in aanmerking komen voor een oriënterende benadering door *Opdrachtgever*.

De BC kan deze lijst van bedrijven aanbieden aan BIV / MIVD voor een administratieve controle. BIV / MIVD heeft de mogelijkheid te adviseren om een bedrijf uit te sluiten van het verdere proces.

Onderhandelingsfase (offertefase)

Na de oriëntatiefase is het aantal bedrijven dat uitgenodigd wordt voor verdere onderhandeling of om een offerte uit te brengen, beperkt. Wanneer een aanvrager een potentiële *Opdrachtnemer* geselecteerd heeft om offerte uit te brengen voor een *BO* en deze dient tijdens de offerte fase al over *Bijzondere Informatie* (BI) te beschikken en / of in te zien, dan meldt deze aanvrager dit vooraf met het formulier 'aanvraag voor autorisatie van natuurlijke of rechtspersonen voor gerubriceerde defensieopdrachten' bij BIV / MIVD. Deze bedrijven worden door BIV / MIVD bezocht om de stand van zaken m.b.t. de beveiliging te inspecteren. Met het bedrijf wordt aan de hand van de *ABDO 2017* overlegd welke (aanvullende) beveiligingsmaatregelen op welk niveau noodzakelijk zijn om voor een mogelijke uiteindelijke gunning in aanmerking te komen.

Het kan noodzakelijk zijn dat een potentiële *Opdrachtnemer* in de onderhandelingsfase reeds dient te beschikken over een *TBB*. Voordat een *TBB* in de onderhandelingsfase aan potentiële *Opdrachtnemers* wordt verstrekt, dient BIV / MIVD hiervoor een voorlopige autorisatie te hebben afgegeven aan de aanvrager en aan de potentiële *Opdrachtnemer*. Wanneer een *TBB* in deze fase alleen op een defensielocatie wordt ingezien en er geen *TBB* op de bedrijfslocatie aanwezig is, wordt de voorlopige autorisatie aan de aanvrager afgegeven nadat:

- BIV / MIVD een onderzoek heeft uitgevoerd aangaande de geselecteerde bedrijven;
- bij een *TBB* op het niveau van Departementaal Vertrouwelijk de desbetreffende medewerkers een *Verklaring Omtrent Gedrag (VOG)* hebben overlegd en een geheimhoudingsverklaring hebben ondertekend;
- bij een *TBB* op het niveau van Stg. CONFIDENTIEEL en hoger, BIV / MIVD een voorlopige *Lijst van Vertrouwensfuncties (LvV, zie hoofdstuk 5 Personeel)* heeft vastgesteld en de desbetreffende medewerkers van het bedrijf een *Verklaring van Geen Bezwaar (VGB)* hebben ontvangen en een geheimhoudingsverklaring hebben ondertekend.

Aanvullend wordt, indien in deze fase een *TBB* op bedrijfslocatie benodigd is, door BIV / MIVD de locatie van het bedrijf nader onderzocht op:

- beveiligingsorganisatie en procedures;
- fysieke beveiliging;
- digitale beveiliging.

Indien het *ABDO*-onderzoek met positief resultaat is afgerond geeft *BIV / MIVD* een voorlopige autorisatie af aan de aanvrager, hetgeen toestemming inhoudt om met de desbetreffende potentiële *Opdrachtnemers* een *TBB* te delen. Indien uit het onderzoek blijkt dat het bedrijf niet bereid of in staat is te voldoen aan de *ABDO* 2017, wordt de aanvrager geadviseerd het bedrijf niet langer te betrekken in het gunningsproces. Een weigering van de aangevraagde autorisatie volgt.

Indien de offerte niet tot een opdracht leidt, zal de aanvrager er zorg voor dragen dat er geen *TBB* op de locatie van het bedrijf achterblijft. De eventuele verstrekte *LvV* en *VGB* vervallen.

Gunningsfase en uitvoering van de opdracht

Wanneer Defensie een *BO* aan een potentiële *Opdrachtnemer* wil verstrekken en deze dient pas na gunning over *BI* te beschikken en / of in te zien, dan meldt de aanvrager dit vooraf met het formulier 'aanvraag voor autorisatie van natuurlijke of rechtspersonen voor gerubriceerde defensieopdrachten' bij *BIV / MIVD*. De geselecteerde *Opdrachtnemer* wordt door *BIV / MIVD* onderworpen aan een integrale beveiligingsinspectie op de betrokken bedrijfslocatie en er wordt een definitieve *LvV* opgemaakt. Aan het bij de opdracht betrokken personeel wordt, na positieve afronding van het *Veiligheidsonderzoek*, een *VGB* verstrekt. Vervolgens wordt de definitieve autorisatie aan de aanvrager en aan de potentiële *Opdrachtnemer* afgegeven, waarmee *BIV / MIVD* verklaart dat er vanuit beveiligingsoogpunt geen bezwaar bestaat tegen gunning van de *BO* aan de geselecteerde *Opdrachtnemer*. Bij gunning dient de *ABDO* 2017 bedongen te zijn in het contract waarbij het vereiste beveiligingsniveau is aangegeven. Deze autorisatie zal:

- de Staat niet verplichten tot een (volgend) contract;
- niet aan derden worden verstrekt zonder schriftelijke toestemming van *BIV / MIVD*;
- niet worden gebruikt voor promotiedoeleinden of advertenties zonder schriftelijke toestemming van *BIV / MIVD*.

BIV / MIVD onderhoudt ten aanzien van beveiligingsaspecten contact met de *Opdrachtnemer* gedurende de uitvoering van de opdracht en zo lang als nodig daarna.

Beëindiging van het contract

Bij beëindiging van het contract vervallen alle bijbehorende autorisaties, de *LvV* en de *VGB*. Indien de *Opdrachtnemer* daarnaast nog andere *BO* uitvoert vindt aanpassing van de *LvV* plaats en blijven de daarop van toepassing zijnde *VGB* gehandhaafd. De overige *VGB* komen hiermee te vervallen.

Hieraan voorafgaand dient de *Opdrachtnemer* de door *Opdrachtgever* verstrekte *TBB* te retourneren tenzij *Opdrachtgever*, eventueel in overleg met *BIV / MIVD*, schriftelijk toestemming heeft verleend de *TBB* te vernietigen of te behouden. Zo nodig kan op aangeven van de *Opdrachtgever*, *BIV / MIVD* controleren of alle betrokken *TBB* zijn geretourneerd, vernietigd dan wel met toestemming van de *Opdrachtgever* zijn achtergebleven bij de *Opdrachtnemer*. De *Opdrachtnemer* verstrekt hiervan een opgave aan *BIV / MIVD*. Door *Opdrachtnemer* gegenereerde *TBB*, die mede betrekking hebben op mogelijke andere nationale of internationale *BO* kunnen met toestemming van de *Opdrachtgever* achterblijven, mits aan de juiste beveiligingseisen voldaan kan blijven worden.

Tot slot vindt er door de *Beveiligingsfunctionaris (BF)* van de *Opdrachtnemer* een debriefing plaats van de betrokken medewerkers. Hierin wordt gewezen op het voortduren van de geheimhoudingsplicht en andere mogelijk nog relevante beveiligingsaspecten.

Inschakeling buitenlands bedrijf

Voor de inschakeling van een buitenlandse *Opdrachtnemer* is toestemming van *BIV / MIVD* vereist. Wanneer het voornemen bestaat om een buitenlands bedrijf in te schakelen voor een *BO*, of als *Subcontractor* van een reeds bestaand *ABDO* bedrijf, dient een autorisatieverzoek bij *BIV / MIVD* te worden ingediend. Indien het nationale belang zich hiertegen niet verzet neemt *BIV / MIVD* contact op met de bevoegde autoriteit op het gebied van Industrieveiligheid in het desbetreffende land. Deze autoriteit verstrekt op verzoek van *BIV / MIVD* een “*Facility Security Clearance*” (*FSC*) van het betreffende bedrijf op basis van het in dat land vigerende stelsel van beveiligingseisen. Op basis van deze *FSC* verstrekt *BIV / MIVD* de autorisatie aan de aanvrager. In het contract met een buitenlandse *Opdrachtnemer* is het in beginsel niet mogelijk om bij een *BO* kortweg te verwijzen naar de *ABDO 2017* in verband met nationale wetgeving. Wel kunnen alle noodzakelijke beveiligingseisen integraal in het te sluiten contract worden opgenomen. Ook kan in het contract worden verwezen naar het in het betrokken land vigerende, met de *ABDO 2017* overeenkomende, nationale stelsel van beveiligingseisen. Hieronder begrepen de screening van de medewerkers van het buitenlandse bedrijf. Zonodig kunnen in het contract nog aanvullende beveiligingseisen worden opgenomen, bijvoorbeeld m.b.t. cybersecurity of buitenlandse invloed. *BIV / MIVD* treedt dan in overleg met de bevoegde autoriteit teneinde te bewerkstelligen dat op implementatie van de aanvullende eisen wordt gecontroleerd.

Inschakeling Nederlands bedrijf op verzoek van het buitenland

Als het buitenland een Nederlands bedrijf wil inschakelen voor een *BO* ontvangt *BIV / MIVD* een verzoek om ten aanzien van dat bedrijf een *FSC* te verstrekken. In dat geval gaat *BIV / MIVD* tot verstrekking over als het bedrijf voldoet aan de in de *ABDO 2017* gestelde beveiligingseisen, waarbij de hierboven beschreven procedure wordt doorlopen.

Bilaterale beveiligingsafspraken

Voorwaarde voor de wederzijdse internationale inschakeling van bedrijven in het kader van een *BO*, is dat er tussen Nederland en het betreffende buitenland een beveiligingsverdrag, - overeenkomst of - MoU bestaat, waarin uitwisseling van *TBB* wordt gefaciliteerd en wederzijds de beveiliging van die uitgewisselde *TBB* is gegarandeerd. *BIV / MIVD* heeft met een groot aantal landen in multilateraal verband en met een beperkt aantal landen op bilaterale basis afspraken om de wederzijdse inschakeling op efficiënte wijze te faciliteren.

Bijlage 1 Tabel meest voorkomende <i>Merkingen</i> gekoppeld aan <i>TBB</i>-categorie		
---	--	--

<u>NEDERLANDSE MERKINGEN</u>	<u>Toe te passen TBB categorie</u>	<u>Betekenis</u>
NLD ONGERUBRICEERD	-	Ongerubriceerde <i>Informatie</i> is niet zonder meer bedoeld voor brede kennisname (" <i>Need-to-Know</i> ").
PERSONEELS- VERTROUWELIJK	TBB 4	Aangebracht op <i>Informatie</i> met persoonsgegevens. Kennisname door niet-gerechtigden kan de belangen van een persoon schaden.
COMMERCEEL VERTROUWELIJK	TBB 4	Aangebracht op <i>Informatie</i> met bedrijfs- en fabricagegegevens. Kennisname door niet-gerechtigden kunnen de belangen van het bedrijf of de Staat schaden.
MEDISCH GEHEIM	TBB 4	Aangebracht op <i>Informatie</i> over de lichamelijke of geestelijke gesteldheid van een persoon. Kennisname door niet-gerechtigden kan de belangen van een persoon schaden.
NLD-EYES-ONLY	Afhankelijk van het rubriceringsniveau	Meestal in combinatie met een <i>Rubricering</i> aangebracht ter <i>Identificatie</i> van nationaal gevoelige <i>Informatie</i> . Kennisname door niet-Nederlanders kan de belangen van Defensie schaden.
RELEASABLE TO (land, missie, organisatie)	Afhankelijk van het rubriceringsniveau	Meestal in combinatie met een <i>Rubricering</i> aangebracht. Kennisname door personen die niet behoren tot de aangegeven categorie kan de belangen van de Staat, een bondgenoot, een missie of een organisatie schaden.
CRYPTO	Afhankelijk van het rubriceringsniveau	Aangebracht op gerubriceerde <i>Informatie</i> die betrekking heeft op gerubriceerde sleutelmiddelen. Deze <i>Informatie</i> mag alleen worden behandeld door personen die als cryptodeelnemer zijn geregistreerd.
CRYPTO-SECURITY	Afhankelijk van het rubriceringsniveau	Aangebracht op documenten die crypto- <i>Informatie</i> bevatten. Kennisname door niet-gerechtigden kan bijdragen aan het ontcijferen van <i>Vercijferde Informatie</i> door niet-gerechtigden.
COMSEC	Afhankelijk van het rubriceringsniveau	Aangebracht ter <i>Identificatie</i> van middelen t.b.v. verbindingsbeveiliging, die niet als CRYPTO of CRYPTOSECURITY zijn gemerkt, maar waarvoor speciale regels gelden voor de behandeling.
EXPORT CONTROLLED	Afhankelijk van het rubriceringsniveau	Aangebracht op <i>Informatie</i> die op grond van exportregelgeving op een bepaalde wijze moet worden behandeld.

Bijlage 2

Tabel buitenlandse Rubriceringen

Nederland	<i>Stg.</i> ZEER GEHEIM	<i>Stg.</i> GEHEIM	<i>Stg.</i> CONFIDENTIEEL	<i>Departementaal</i> VERTROUWELIJK
Optioneel voor int. gebruik: <i>Rubricering</i> aanvullen met	NLD TOP SECRET	NLD SECRET	NLD CONFIDENTIAL	NLD RESTRICTED
<i>EU-Rubricering</i>	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
<i>NAVO- Rubricering</i>	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
	COSMIC TRÈS SECRET	OTAN SECRET	OTAN CONFIDENTIEL	OTAN DIFFUSION RESTREINTE
<i>VN-Rubricering</i>		UN STRICTLY CONFIDENTIAL	UN CONFIDENTIAL	
<i>Albanië</i>	TEPËR SEKRET	SECKRET	KONFIDENCIAL	I KUFIZUAR
<i>België</i>	TRÈS SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERKTE VERSPREIDING
<i>Bulgarije</i>	СТОГО СЕКРЕТНО	СЕКРЕТНО	ПОВЕИТЕЛНО	ЗА СПУЖЕБНО ПОЛЗВЕНЕ
<i>Canada¹</i>	TOP SECRET	SECRET	CONFIDENTIAL	
	TRÈS SECRET	SECRET	CONFIDENTIEL	
<i>Cyprus</i>	ἈΚΡΩΣ ΑΠΌΡΡΗΤΟ	ΑΠΌΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΟ	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ
<i>Denemarken</i>	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG

¹ Canada gebruikt geen equivalente *Rubricering*. Canada behandelt en beveiligt deze *Informatie* conform de C-M(2002)49, *supporting directives* en het *supporting document* voor de beveiliging van NATO RESTRICTED *Informatie*.

Algemene Beveiligingseisen Defensie Opdrachten 2017

Duitsland	STRENG GEHEIM	GEHEIM	VS - VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
Estland	TÄIESTI SALAJANE	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITETTU
	YTTERST HEMLIG	HEMLIG	KONFIDENTIELL	BEGRÄNSAD TILLGÅNG
Frankrijk²	TRÈS SECRET DÉFENSE	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	
Griekenland	ἈΚΡΩΣ ΑΠΟΡΡΗΤΟ	ΑΠΟΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΟ	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ
Hongarije	SZIGORÚAN TITKOS!	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTTÉÜ!
Ierland	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
IJsland	ALGERT LEYNDARMAL	LEYNDARMAL	TRUNADARMAL	THJONUSTJSKJAL
Italië	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Kroatië	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Letland	SEVIŠĶI SLEPENI	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADŽĪBĀM
Litouwen	VISIŠKAI SLAPTAI	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDJIMO
Luxemburg	TRÈS SECRET LUX	SECRET LUX	CONFIDENTIEL LUX	DIFFUSION RESTREINTE LUX
Malta	L-OGHLA SEGRETEZZA	SIGRIET	KUNFIDENZJALI	RISTRETT
Nieuw Zeeland	TOP SECRET	SECRET	CONFIDENTIAL	
Noorwegen	STRENGT HEMMELIG	HEMMELIG	KONFIDENTSIELT	BEGRENSSET
Oostenrijk	STRENG GEHEIM	GEHEIM	VERTRAULICH	EINGSCHRÄNK
Polen	ŚCIŚLE TAJNE	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	MUITO SEGRETO	SEGRETO	CONFIDENCIAL	RESERVADO

² Frankrijk gebruikt geen equivalente *Rubricering* voor Departementaal Vertrouwelijk. Frankrijk behandelt en beveiligd deze informatie conform de C-M(2002)49, *supporting directives* en het *supporting document* voor de beveiliging van NATO RESTRICTED Informatie.

Algemene Beveiligingseisen Defensie Opdrachten 2017

Roemenië	STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	STRICT SECRET	SECRET	SECRET DE SERVICIU
Spanje	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Slowakije	PRÍSNE TAJNÉ	TAJNÉ	DŮVERNÉ	VYHRADENÉ
Slovenië	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Tsjechië	(TOP SECRET) PŘISNĚ TAJNÉ	(SECRET) TAJNÉ	(CONFIDENTIAL) DŮVĚRNÉ	VYHRAZENÉ
Turkije	ÇOK GİZLİ	GİZLİ	ÖZEL	HİZMETE ÖZEL
Verenigd Koninkrijk³	TOP SECRET	SECRET	NO EQUIVALENT TO CONFIDENTIAL	OFFICIAL-SENSITIVE
Verenigde Staten⁴	TOP SECRET	SECRET	CONFIDENTIAL	
Zweden	KVALIFICERAT HEMLIG	HEMLIG	HEMLIG	HEMLIG
Zwitserland - Franstalig - Duitstalig - Italiaans- Riservato talig	TRÈS SECRET DÉFENSE STRENG GEHEIM SEGRETISSIMO	SECRET DÉFENSE GEHEIM SEGRETO	CONFIDENTIEL DÉFENSE VS - VERTRAULICH RISERVATISSIMO	DIFFUSION RESTREINTE VS-NUR FÜR DEN DIENSTGEBRAUCH

³ Het Verenigd Koninkrijk hanteert per 02 april 2014 alleen nog de rubriceringsniveaus TOP SECRET, SECRET en OFFICIAL. De Rubricering UK CONFIDENTIAL is vervallen en wordt behandeld conform UK SECRET. *Informatie* die voorheen als RESTRICTED werd aangeduid wordt voortaan aangemerkt als OFFICIAL - SENSITIVE.

⁴ De VS gebruikt geen equivalente Rubricering. De VS behandelt en beveiligt deze *Informatie* conform de C-M(2002)49, *supporting directives* en het *supporting document* voor de beveiliging van NATO RESTRICTED *Informatie*.

Bijlage 3

Inrichten beveiligingsorganisatie

Elk bedrijf dat beschikt over gevoelige bedrijfseigen *Informatie* zou moeten beschikken over een adequaat **beveiligingsbeleid** en **beveiligingsplan** als noodzakelijke instrumenten om deze informatie tegen ongewenste toegang te beschermen. De beveiliging van informatie blijkt voor veel bedrijven echter nog een sluitpost. Helaas worden risico's vaak onderschat, vooral de risico's die sociale media, mobiliteit en de "Cloud" met zich meebrengen; voorzieningen waarmee vertrouwelijke bedrijfsgegevens buiten de veilige grenzen van de werkplek beschikbaar zijn en daarmee ook gemakkelijker toegankelijk voor derden. De verantwoordelijkheid voor beveiligingsbeleid, -plan en (de implementatie van) -maatregelen moet derhalve op het hoogste bestuurlijke niveau zijn belegd. Voor toezicht op de beveiliging wordt, met voorafgaande instemming van *BIV / MIVD*, een *BF* benoemd die over voldoende autonomie, bevoegdheden, slagkracht en senioriteit beschikt en rechtstreeks toegang heeft tot het hoogste bestuurlijke niveau.

Om de vertrouwelijkheid van de *TBB* te borgen dient de Opdrachtnemer het beheer van de aan hem verstrekte of door hem gegenereerde *TBB* zodanig in te richten dat te allen tijde inzichtelijk is waar en bij wie deze zich bevinden en in behandeling zijn, en wie er op welke momenten kennis van heeft genomen. Zorgvuldige registratie hiervan, inclusief (de pogingen tot) ongeautoriseerde kennisname en behandeling is derhalve essentieel. Dit vergt structuur in de organisatie alsmede duidelijke, eenduidige, in het beveiligingsplan vastgelegde procedures en werkwijzen voor de toegang tot en behandeling van *TBB*. Hierbij moet worden gedacht aan gestandaardiseerde procedures voor het registreren, overdragen, modificeren, kopiëren, distribueren, opslaan, communiceren en vernietigen van *TBB*, zowel in fysieke als in digitale vorm. Hieronder valt dus ook het systematisch beheer van (toegang tot) het informatiesysteem en de daarop aanwezige *Informatie*. Met zorgvuldig beheer kan ongeautoriseerde kennisname en behandeling, en daarmee *Compromittatie* van *TBB* mogelijk worden voorkomen.

Beveiligingsplan

De *Opdrachtnemer* dient over een beveiligingsplan te beschikken. In het beveiligingsplan staat kort en eenduidig beschreven op welke wijze de beveiliging van *TBB* wordt uitgevoerd. Het ontwikkelen van een beveiligingsplan start met een (dreigings-)analyse van de bestaande situatie, een inventarisatie van de reeds bestaande beveiligingsvoorzieningen en het vaststellen van noodzakelijke aanvullende maatregelen. Op basis van de beveiligingseisen als genoemd in hoofdstuk 1, 2, 3 en 4 wordt het beveiligingsplan nader uitgewerkt. Vervolgens worden de noodzakelijke aanvullende maatregelen en procedures doorgevoerd waarna het beveiligingsplan definitief, met goedkeuring van *BIV / MIVD*, wordt vastgesteld en geïmplementeerd. Periodiek, doch minimaal eenmaal per jaar, dient een evaluatie plaats te vinden waaruit moet blijken of het beveiligingsplan nog voldoet dan wel moet worden bijgesteld.

Naast een planmatige controle of de maatregelen nog afdoende zijn, kan ook een incident of een veranderd dreigingsbeeld een reden zijn om het (kring)proces weer te doorlopen. Met deze systematiek wordt bewerkstelligd dat *TBB* worden beveiligd op basis van een actueel dreigingsbeeld met toepassing van adequate beveiligingsmaatregelen. Dit is van toepassing voor zowel de fysieke beveiliging van *TBB* als voor de digitale beveiliging van *Bijzondere Informatie* die wordt verwerkt in IT-systemen en -netwerken.

Bijlage 3.1

Leidraad beveiligingsplan

--	--	--

Beveiligingsplan ABDO

Beschrijving op welke wijze de beveiliging van TBB wordt uitgevoerd.

Beveiligingsplan bevat In ieder geval de volgende punten:

- korte beschrijving van de lopende *Bijzondere Opdrachten* en/of projecten inclusief hoogte van de *Rubricering*;
- bedrijf (adres, organogram, uittreksel Kamer van Koophandel, introductie bedrijf);
- contactgegevens *Beveiligingsfunctionaris* en zijn positie binnen het bedrijf;
- belegging verantwoordelijkheden directie aangaande *Bijzondere Opdrachten*;
- eenduidige beschrijving van het *TBB* op de bedrijfslocatie.

De volgende onderwerpen zijn, indien van toepassing, in dit beveiligingsplan uitgeschreven tot duidelijk en hanteerbare maatregelen en procedures conform de eisen in de *ABDO 2017*.

Bestuur en Organisatie
Inrichten beveiligingsorganisatie
De <i>Beveiligingsfunctionaris</i>
Structuur, eigendom en zeggenschap van de <i>Opdrachtnemer</i>
Beveiligingsbewustzijn
Rubriceringaanduidingslijst
<i>Subcontracting</i>
Pers, internet, sociale media, publicatie, fotografische opnamen, etc.
<i>Incident Handling</i>

Personeel
Beheer van aantal en de invulling van <i>Vertrouwensfuncties</i> en het juiste <i>Veiligheidsmachtigingsniveau</i> conform de <i>Bijzondere Opdracht(en)</i>
Aanvragen <i>Veiligheidsonderzoek(en)</i>
Actueel overzicht van geldige <i>VGB('n)</i> en <i>VOG('n)</i> in relatie tot de <i>Bijzondere Opdrachten</i>
<i>Geheimhoudingsverklaring</i>
Niet-Nederlander op een <i>Vertrouwensfunctie</i>
Verplichtingen van de <i>Vertrouwensfunctionaris</i>
Reizen naar het buitenland van een <i>Vertrouwensfunctionaris</i>

Fysiek
Schillenstructuur en de bijbehorende beveiligingsmaatregelen op het gebied van:
Organisatorische maatregelen: - toegangscontrole; - <i>Autorisaties</i>; - <i>Logging</i>.
Bouwkundige maatregelen: - <i>Uitsteltijd</i>; - <i>Compartimentering</i>; - bouwkundige schillen; - terrein en parkeervoorziening; - visueel en akoestisch beperkende maatregelen.
Elektronische maatregelen: - <i>IDSS</i>; - <i>ETS</i>; - <i>CCTV</i>.

Algemene Beveiligingseisen Defensie Opdrachten 2017

Reactieve maatregelen: - proces alarmopvolging; - alarmverificatie.
Transport en verzenden
Safety
Fysieke opslag, verwerking en ontwikkeling

Cyber
Informatiebeveiligingsbeleid - <i>Beleidsregels voor informatiebeveiliging</i>
Organiseren van informatiebeveiliging - <i>Interne organisatie</i> - <i>Scheiding van taken</i> - <i>Mobiele apparatuur en telewerken</i> - <i>Telewerken</i>
Veilig personeel - <i>Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging</i> - <i>Beëindiging of wijziging van verantwoordelijkheden van het dienstverband</i>
Beheer van bedrijfsmiddelen - <i>Inventariseren van ICT-bedrijfsmiddelen</i> - <i>Eigendom van ICT-bedrijfsmiddelen</i> - <i>Aanvaardbaar gebruik van ICT-bedrijfsmiddelen</i> - <i>Classificatie van informatie</i> - <i>Informatie labelen</i> - <i>Behandelen van ICT-bedrijfsmiddelen</i> - <i>Beheer van verwijderbare gegevensdragers</i>
Toegangsbeveiliging - <i>Bedrijfseisen voor toegangsbeveiliging</i> - <i>Beleid voor toegangsbeveiliging</i> - <i>Toegang tot netwerken en netwerkdiensten</i> - <i>Registratie en afmelden van gebruikers</i> - <i>Beheren van speciale toegangsrechten</i> - <i>Beheer van geheime authenticatie-informatie van gebruikers</i> - <i>Beoordeling van toegangsrechten van gebruikers</i> - <i>Geheime authenticatie-informatie gebruiken</i> - <i>Beperking toegang tot informatie</i> - <i>Beveiligde inlogprocedures</i> - <i>Systeem voor wachtwoordbeheer</i> - <i>Speciale systeemhulpmiddelen gebruiken</i> - <i>Toegangsbeveiliging op programmabroncode</i>
Cryptografie - <i>Beleid inzake het gebruik van cryptografische beheersmaatregelen</i> - <i>Sleutelbeheer</i>
Fysieke beveiliging en beveiliging van de omgeving - <i>Beveiligde gebieden</i> - <i>Plaatsing en bescherming van apparatuur</i> - <i>Beveiliging van bekabeling</i> - <i>Onderhoud van apparatuur</i> - <i>Verwijdering van bedrijfsmiddelen</i> - <i>Veilig verwijderen of hergebruiken van apparatuur</i> - <i>Onbeheerde gebruikersapparatuur</i> - <i>'Clear desk'- en 'clear screen'-beleid</i>
Beveiliging bedrijfsvoering - <i>Gedocumenteerde bedieningsprocedures</i> - <i>Wijzigingsbeheer</i> - <i>Capaciteitsbeheer</i> - <i>Scheiding van ontwikkel-, test- en productieomgevingen</i> - <i>Beheersmaatregelen tegen malware</i> - <i>Back-up van informatie</i>

Algemene Beveiligingseisen Defensie Opdrachten 2017

- <i>Gebeurtenissen registreren</i> - <i>Beschermen van informatie in logbestanden</i> - <i>Kloksynchronisatie</i> - <i>Software installeren op operationele systemen</i> - <i>Beheer van technische kwetsbaarheden</i>
<i>Communicatiebeveiliging</i> - <i>Beheersmaatregelen voor netwerken</i> - <i>Beveiliging van netwerkdiensten</i> - <i>Scheiding in netwerken</i> - <i>Beleid en procedures voor informatietransport</i> - <i>Cloudcomputing</i> - <i>Virtualisatie</i>
<i>Acquisitie, ontwikkeling en onderhoud van informatiesystemen</i> - <i>Analyse en specificatie van informatiebeveiligingseisen</i> - <i>Principes voor engineering van beveiligde systemen</i> - <i>Systeemacceptatietests</i>
<i>Leveranciersrelaties</i> - <i>Informatiebeveiligingsbeleid voor leveranciersrelaties</i>

	Bijlage 4 <i>Beveiligingsfunctionaris</i>	
--	--	--

Beveiligingsfunctionaris en sub-Beveiligingsfunctionaris

De *Beveiligingsfunctionaris* (BF) is belast met de dagelijkse zorg voor de beveiliging en kan bij deze werkzaamheden terzijde worden gestaan door één of meer aangewezen sub-*Beveiligingsfunctionarissen*, bijvoorbeeld, als vervanger bij afwezigheid van de BF of één voor elke bedrijfslocatie. Ook kan een sub-BF worden aangewezen op grond van een specialisatie, zoals cyberdeskundigheid. Voor meer informatie over de rol van de cyber BF wordt verwezen naar **bijlage 24**. De directie draagt aan MIVD de kandidaat (sub-) BF voor die voldoet aan de eisen, taken en verantwoordelijkheden zoals gesteld in de ABDO 2017 (**voor aanmelding BF en sub-BF zie formulieren in deze bijlage**).

Minimale eisen voor de aanwijzing van een (sub-) *Beveiligingsfunctionaris*

Als minimum eis dient een (sub-) *Beveiligingsfunctionaris*:

- een Nederlandse nationaliteit te hebben en in dienst te zijn van het desbetreffende bedrijf;
- over voldoende autonomie, bevoegdheden, slagkracht en senioriteit te beschikken;
- gescreend te zijn op het hoogst geldende niveau van de *Bijzondere Opdrachten* die het bedrijf uitvoert;
- rechtstreekse en onafhankelijke toegang te hebben tot de CEO, directie of Raad van Bestuur.

Taken en verantwoordelijkheden

In relatie tot een *ABDO Autorisatie* is de (sub-) BF verantwoordelijk voor:

- het vaste aanspreekpunt vanuit de *Opdrachtnemer* te zijn voor de MIVD en de AIVD en vertegenwoordigt hierbij de *Opdrachtnemer* voor wat betreft alle beveiligingsaspecten en is bevoegd tot het nemen van de vereiste maatregelen en beslissingen;
- de dagelijkse zorg voor de beveiliging;
- toezicht houden op de deugdelijkheid van de beveiliging van de TBB conform de beveiligingseisen zoals beschreven in de ABDO 2017. Wanneer nodig maatregelen treffen ter verbetering van het beveiligingsbeleid;
- het vastleggen van gegevens t.a.v. toegang tot en inzicht in een TBB en worden gedurende de aangegeven periode bewaard om achteraf onderzoek naar vermoede incidenten mogelijk te maken;
- het opstellen van een beveiligingsplan in relatie tot de *Bijzondere Opdrachten* en TBB conform de eisen van de ABDO 2017;
- implementatie van noodzakelijke wijzigingen n.a.v. een verhoogd dreigingsbeeld of een incident, in het beveiligingsplan binnen de gestelde termijn;
- het zorgdragen voor volledige medewerking bij controles, audits en onderzoeken bij *Opdrachtnemer* door BIV / MIVD;
- op basis van de voortgang van *Bijzondere Opdrachten* en het op locatie hebben van een TBB regelmatig actualiseren van het (door BIV / MIVD ingestemde) beveiligingsplan;
- periodiek toetsen van dit beveiligingsplan aan de praktijk en dit schriftelijk rapporteren aan de directie en BIV / MIVD. Voor een totaalbeoordeling van de beveiliging stelt de BF minstens eenmaal per jaar een rapport zelfinspectie op en stuurt dit aan het bestuur;
- het geven van volledige medewerking bij controles, audits en onderzoeken door BIV / MIVD;
- het melden, onderzoeken en treffen van maatregelen aangaande incidenten. Dit gebeurt volgens het Incident Handling proces (zie bijlage 9);
- het bijhouden van een actueel overzicht van alle *Bijzondere Opdrachten*, TBB en medewerkers waaraan een VGB of VOG en bijbehorende geheimhoudingsverklaringen zijn verstrekt;

Algemene Beveiligingseisen Defensie Opdrachten 2017

- het beheren van het aantal en de invulling van *Vertrouwensfuncties* en draagt zorg voor een juist en geldig *Veiligheidsmachtigingsniveau*;
- het tijdig aanvragen van (hernieuwde) *Veiligheidsonderzoeken* voor medewerkers die geplaatst zijn op *Vertrouwensfuncties*;
- het beheer van de toegang tot een *TBB* en heeft hiervoor de *Autorisaties* vastgesteld;
- het inzichtelijk hebben waar en bij wie *TBB* zich bevinden en wie er op welk moment kennis van heeft;
- de *BF* coördineert en controleert de ontvangst en de verzending van *Bijzondere Informatie* en waar nodig, het gebruik van koerierspassen;
- de *BF* adviseert inzake de *Merking* en *Rubricering* van nieuwe *Informatie*;
- periodiek, doch minimaal eenmaal per jaar, het controleren op de aanwezigheid en compleetheid van geregistreerde *TBB* (en kopieën);
- waar nodig het rechtstreeks en onafhankelijk adviseren van de directie over beveiligingszaken;
- voorlichting, in het kader van Security Awareness, aan vertrouwensfunctionarissen bij de start van een nieuwe *Bijzondere Opdracht*, periodiek gedurende *Bijzondere Opdrachten* aangaande *ABDO* procedures en de bijbehorende verantwoordelijkheden;
- zo nodig individueel advies en begeleiding geven aan medewerkers, die werken aan *Bijzondere Opdrachten*, buitenlandse contacten hebben of op reis gaan naar zogenoemde risicolanden.
- bemiddelt in internationale bezoekaankondigingen in het kader van de 'International Visits'
- het aanvragen van een *Subcontractor* bij *BIV / MIVD* bij voorgenomen uitbesteding van werkzaamheden in het kader van een *Bijzondere Opdracht* (zie bijlage 8). De *ABDO* 2017 is bedongen in het contract met de *Subcontractor*;
- de *BF* houdt zich op de hoogte van de acquisitie van het bedrijf en informeert de *MIVD* dienaangaande bij voorgenomen export naar risicolanden. Hierbij in acht genomen dat de voorgenomen export direct of indirect gerelateerd is aan defensietechnologie of dat de ontwikkeling initieel betaald is door defensie;
- op regelmatige wijze de sub-*BF* op de hoogte te stellen van procedures en incidenten zodat deze de taken kan uitvoeren bij afwezigheid van de *BF*.

Bijlage 4.1 Benoeming <i>Beveiligingsfunctionaris</i>
--

Benoeming *Beveiligingsfunctionaris* en toekennen van verantwoordelijkheden

Naar:
Bureau Industrie Veiligheid
Afdeling Contra-Inlichtingen en Veiligheid
Militaire Inlichtingen-en Veiligheidsdienst
Postbus 90701
2597 LS Den Haag

Benoeming *Beveiligingsfunctionaris*

Ik, _____ van _____
(hoogst bestuursorgaan, directie en / of eigenaar) (Bedrijf / Organisatie)

benoem, na instemming van *BIV / MIVD*, de hierna genoemde medewerker, als *Beveiligingsfunctionaris (BF)* conform de in de *ABDO 2017* gestelde eisen.

_____ (volledige naam van *BF*)

Datum _____

Handtekening _____
(Handtekening van hoogste bestuursorgaan, directie en / of eigenaar)

Ik, _____
(volledige naam van aangewezen *BF*)

Werknemer van _____

Functie _____

begrijp en accepteer hierbij de taken en verantwoordelijkheden van de *BF*, zoals beschreven in bijlage 4 van de *ABDO 2017* en zal mij hieraan houden.

_____ (handtekening van de *BF*)

Alleen in te vullen door *BIV / MIVD*

Goedgekeurd door _____ Afgekeurd door _____

Datum _____ Datum _____

Reden _____

Bijlage 4.2

Benoeming sub - *Beveiligingsfunctionaris*

Benoeming sub - *Beveiligingsfunctionaris* en toekennen van verantwoordelijkheden

Naar:

Bureau Industrie Veiligheid

Afdeling Contra-Inlichtingen en Veiligheid

Militaire Inlichtingen-en Veiligheidsdienst

Postbus 90701

2597 LS Den Haag

Benoeming sub - *Beveiligingsfunctionaris*

Ik, _____ van _____
(hoogst bestuursorgaan, directie en / of eigenaar) (Bedrijf / Organisatie)

benoem, na instemming van *BIV / MIVD*, de hierna genoemde medewerker, als sub - *Beveiligingsfunctionaris* conform de in de *ABDO 2017* gestelde eisen.

(volledige naam van *BF*)

Datum _____

Handtekening

(Handtekening van hoogste bestuursorgaan, directie en / of eigenaar)

Ik, _____
(volledige naam van aangewezen *BF*)

Werknemer van _____

Functie _____

begrijp en accepteer hierbij de taken en verantwoordelijkheden van de *BF*, zoals beschreven in bijlage 4 van de *ABDO 2017* en zal mij hieraan houden.

.

(handtekening van de *BF*)

Alleen in te vullen door *BIV / MIVD*

Goedgekeurd door _____ Afgekeurd door _____

Datum _____ Datum _____

Reden _____

	Bijlage 5 <i>Zeggenschap en bedrijfsstructuur</i>	
--	---	--

1. Initiële informatieverstrekking m.b.t. *Zeggenschap*, bedrijfsstructuur etc.

In beginsel heeft het bestuur van een *Opdrachtnemer* de dagelijkse leiding van een onderneming. Soms echter kunnen anderen dan het bestuur zodanige invloed uitoefenen op besluiten dat de bescherming van *TBB* in het geding kan komen. Het is derhalve noodzakelijk om altijd inzicht te hebben in wie of wat *Zeggenschap* heeft, of die *Zeggenschap* berust bij buitenlandse partijen, of er andere (buitenlandse) relaties, waaronder samenwerkingsverbanden, zijn, of er werkzaamheden worden verricht op buitenlandse locaties e.d.

Om de veiligheid van de Staat en zijn bondgenoten te beschermen dient de invloed te worden gecontroleerd van derden die belangen kunnen hebben die daarmee tegenstrijdig zijn. Teneinde te beoordelen of er sprake is van ongewenste (buitenlandse) invloed dient het bedrijf als onderdeel van de te volgen autorisatieprocedure alle gegevens aan *BIV / MIVD* te overleggen die volgens *BIV / MIVD* noodzakelijk zijn om dit te kunnen beoordelen, waaronder in elk geval wordt begrepen:

- Verklaring van eigendom, informatie over *Zeggenschap*, aandeelhouders en bedrijfsstructuur;
- informatie over de bedrijfsactiviteiten, locaties en samenwerkingsverbanden;
- naam, geboortedatum en -plaats, adres en nationaliteit van de bestuurder(s), toezichthouders (bv. commissarissen), management en andere personen die een doorslaggevende invloed kunnen hebben op het beleid van de onderneming;
- een exemplaar van de statuten en het meest recente jaarverslag.

Opdrachtnemer is gehouden op eerste verzoek van *BIV / MIVD* aanvullende informatie te verstrekken.

2. Veranderingen in *Zeggenschap* etc. zoals opgegeven

Veranderingen in de hierboven genoemde informatie dienen te worden beoordeeld op mogelijk ongewenste invloed.

Derhalve dienen voorgenomen wijzigingen in de onder paragraaf 1 vermelde gegevens en informatie, alsmede voorgenomen bedrijfsbeëindiging, fusies, sourcing, splitsing, surseance van betaling of aanstaand faillissement onverwijld te worden gemeld aan *BIV / MIVD*.

De Directeur *MIVD* zal de *Opdrachtnemer* in voorkomend geval(een en ander ter beoordeling van *BIV / MIVD*) binnen vier weken schriftelijk mededelen of uit beveiligingsoverwegingen bezwaren bestaan tegen de voorgenomen wijziging in *Zeggenschap*, eigendom of aandeelhouderschap, voorgenomen fusie, samenwerking of aanstaand faillissement en wat daarvan de mogelijke consequenties zijn.. Afhankelijk van de mogelijke veiligheidsrisico's kan de Directeur *MIVD* besluiten de verleende *ABDO*-autorisatie op te schorten of in te trekken.

3. Bedrijfslocaties

Een bedrijf kan gevestigd zijn op één of meerdere locaties (in binnen - en buitenland). De *Opdrachtnemer* dient te allen tijde inzicht te verschaffen in de locaties en aan te geven waar de *TBB* worden opgeslagen, bewerkt of gegenereerd. Daarbij dient eveneens te worden vermeld hoe de bedrijfsstructuur van de in het contract betrokken locaties is geregeld en wie verantwoordelijk is voor de beveiliging. Wijzigingen in bedrijfslocaties alsmede verantwoordelijkheden dienen te worden gemeld aan *BIV / MIVD*.

Indien een *Opdrachtnemer* werkzaamheden aan een *TBB* over zijn locaties verdeelt dient dit in een opdrachtspecifiek beveiligingsplan te worden verwerkt. Er dient te worden beschreven welke locatie wordt belast

Algemene Beveiligingseisen Defensie Opdrachten 2017

met werkzaamheden aan een *TBB*. Per locatie dient te worden voldaan aan de in de *ABDO* 2017 gestelde eisen rekening houdend met de voor die locatie van toepassing zijnde *TBB*-categorie.

4. Wijze van verstrekken informatie

Op de volgende pagina is het formulier: “Verklaring van eigendom, *Zeggenschap* en bedrijfsstructuur *Opdrachtnemer*” te vinden. Deze dient zowel bij een reguliere verklaring als bij een wijziging hieromtrent ingevuld en ondertekend verstuurd te worden naar *BIV / MIVD*.

	Bijlage 5 Formulier: Verklaring (wijziging) van eigendom, Zeggenschap en bedrijfsstructuur	
--	--	--

Naam <i>Opdrachtnemer</i>	
Correspondentieadres en postcode	
Primair vestigingsadres en postcode	
Telefoonnummer	
Faxnummer	
E-mailadres	

Bedrijfsactiviteiten	
Eventuele andere vestigingsadressen en postcodes	
Locaties	

Aandeelhouderschap ^{a b}	
Structuur binnen bedrijf	
Zeggenschap binnen bedrijf ^c	
Aanstelling en ontslagbeleid ^d	

Volledige personalia (achternaam, voornamen, geboortedatum en -plaats, woonadres, huidige en eventuele vroegere nationaliteiten)	1. <u>De eigenaar(s) / aandeelhouders</u>
	2. <u>De vennoten</u>
	3. <u>Bestuurder(s) / directeur(en)</u>
	4. <u>Commissaris(sen)</u>

Bestaat er enige vorm van samenwerking met een buitenlandse of onder buitenlandse invloed staande Nederlandse organisatie onder zodanige voorwaarden dat die organisatie invloed heeft verkregen op het bedrijfsbeleid of verstrekking van bedrijfsgegevens c.q. het verlenen van inzage daarvan aan vertegenwoordigers of gemachtigden kan verlangen?

(Indien deze vraag bevestigend wordt beantwoord dienen bijzonderheden vermeld te worden in een afzonderlijke bijlage)

Is de organisatie enige financiële verplichting aangegaan onder zodanige voorwaarden dat een vreemdeling, groep van vreemdelingen of een buitenlandse c.q. onder buitenlandse invloed staande Nederlandse organisatie, invloed heeft verkregen op het bedrijfsbeleid of verstrekking van bedrijfsgegevens c.q. het verlenen van inzage daarvan aan vertegenwoordigers of gemachtigden kan verlangen?

Algemene Beveiligingseisen Defensie Opdrachten 2017

(Indien deze vraag bevestigend wordt beantwoord dienen bijzonderheden te worden vermeld in een afzonderlijke bijlage)

Voeg het meest recente jaarverslag van uw bedrijf toe aan deze verklaring.

De ondergetekende, _____

(functie van ondertekenaar)

verklaart dat de vorenstaande gegevens overeenkomstig de waarheid zijn verstrekt *)

_____, te _____
(datum) (plaats)

(handtekening)

*) Het verstrekken van gegevens in strijd met de waarheid of het opzettelijk verzwijgen van gegevens waarop de vorenstaande vragen betrekking hebben, kan leiden tot weigering, opschorting of intrekking van de ABDO-autorisatie.

- a. Beschrijving van de grootte van het aandelenkapitaal c.q. lidmaatschapsrechten, de samenstelling in soorten aandelen c.q. lidmaatschapsrecht en de verdeling over de aandeelhouders c.q. leden (met opgave van contractuele of statutaire rechten verbonden aan die aandelen c.q. lidmaatschapsrechten) van 1. De *Opdrachtnemer*; 2. Ieder die direct of indirect aandelen c.q. lidmaatschapsrecht in de opdrachtnemer houdt en 3. Ieder van de rechtspersonen en vennootschappen die tot het concern behoren, voor zover die leden van het concern aandelen (rechtstreeks of onmiddellijk) in de *Opdrachtnemer* houden.
- b. Schematisch overzicht van degenen die direct of indirect aandelen of lidmaatschapsrechten in de opdrachthouder houden alsmede van het concern waarvan de *Opdrachtnemer* deel uitmaakt, met opgave van iedere rechtspersoon en vennootschap behorende tot het concern, ieder lid van het bestuur en eventueel ieder van de leden van het op dat bestuur toezichthoudend orgaan van die rechtspersoon c.q. vennootschap, met hun nummer van inschrijving in het handelsregister of daar mee vergelijkbaar register.
- c. Voor zover van toepassing, beschrijving van (potentiële) directe of middellijke zeggenschap over aandelen of lidmaatschapsrechten in de *Opdrachtnemer*. En indien van toepassing beschrijving van *Zeggenschap* door een ander dan de houders van die aandelen c.q. lidmaatschapsrechten (bijvoorbeeld als gevolg van volmachten, pandrechten, vruchtgebruik, beheerovereenkomsten of stemafspraken).
- d. Voor zover van toepassing, beschrijving hoe de benoeming en het ontslag plaatsvindt van de leden van het bestuur en/of het toezichthoudend orgaan daarop.

	Bijlage 6 Beveiligingsbewustzijn	
--	--	--

Hoe verstrekkend de genomen beveiligingsmaatregelen ook zijn, uiteindelijk is de mens de belangrijkste schakel. De kwetsbaarheid en kans op *Compromittatie* van een *TBB* worden vergroot wanneer een *Opdrachtnemer* en zijn medewerkers zich niet bewust zijn van de waarde van deze belangen en het risico dat deze in verkeerde handen kunnen vallen. Medewerkers dienen zich bij voortduring te realiseren hoe en waar deze *TBB* te verwerken en op te slaan, en met wie zij deze mogen uitwisselen. Medewerkers die op de hoogte zijn van gevoelige *Informatie* of beschikken over sleutels of wachtwoorden die toegang geven tot bijzondere (digitale) bestanden, dienen zich te realiseren dat zij beschikken over of toegang hebben tot interessante *Informatie*, daardoor zelf interessant zijn en mogelijk een risico vormen.

De ervaring leert dat een werknemer en/of de *Opdrachtnemer* zich lang niet altijd realiseert dat hij over gevoelige, voor derden interessante *Informatie* beschikt. Dit hoeft niet alleen een *TBB* te zijn, ook de eigen bedrijfsgevoelige informatie valt hieronder. Buitenlandse inlichtingendiensten, maar ook concurrerende bedrijven kunnen grote interesse hebben in deze *Informatie*.

Medewerkers kunnen onbewust belangrijke *Informatie* prijsgeven wanneer zij geen juiste inschatting kunnen maken van de waarde ervan. Pas als de waarde van *Informatie*, in de gehele organisatie van de *Opdrachtnemer*, van hoog tot laag is doordrongen, kan een bedrijfscultuur ontstaan waarin de *TBB* ook daadwerkelijk als zodanig worden behandeld door alle medewerkers.

Het is van belang dat het beveiligingsbewustzijn nadrukkelijk wordt uitgedragen door bestuurders op het hoogste niveau. De *Opdrachtnemer* is derhalve verplicht alle medewerkers te onderwerpen aan voorlichting ter verhoging van het beveiligingsbewustzijn. In deze voorlichting worden relevante delen van de *ABDO 2017* behandeld en wordt aandacht besteed aan ontwikkelingen op het gebied van dreiging en beveiligingsmaatregelen. Vorm en inhoud kunnen zo nodig met *BIV / MIVD* worden afgestemd.

Een dergelijke voorlichting bewerkstelligt dat iedere medewerker in de organisatie het belang en de mate van beveiliging begrijpt, zijn eigen individuele verantwoordelijkheid in dezen inziet en daar ook naar handelt. Naast structurele groepsvoorlichting kan er aanleiding zijn voor individuele gesprekken, zoals bij reizen naar het buitenland of het ontvangen van (buitenlands) bezoek.

Tot slot dient een medewerker voorafgaand aan diens plaatsing binnen een *BO* een degelijke veiligheidsbriefing te ontvangen waarin gewezen wordt op het belang van beveiliging van de toevertrouwde *TBB* bij transport en opslag. Daarbij dient nut en vooral noodzaak van een veiligheidsregime uitvoerig te worden toegelicht. Ook dienen de verplichtingen die voortvloeien uit het bekleden van een (*Vertrouwens*)functie binnen een *BO* te worden uitgelegd (**bijlage 10**). Eenmaal geplaatst op een (*Vertrouwens*)functie binnen een *BO* wordt de betrokken medewerker met enige regelmaat onderworpen aan beveiligingsbegeleiding. Met regelmaat dienen door de zorg van de *BF* beveiligingsinstructies of trainingen te worden gegeven (zie ook de eisen in hoofdstuk 1).

	Bijlage 6.1. Beveiligingsbewustzijn: verschillende vormen van spionage	
--	--	--

Spionage kan op verschillende manieren tot uiting komen. Onderstaande links laten toelichtingen zien van de verschillende vormen van benadering van spionage:

- www.aivd.nl - Tabblad Onderwerpen (o.a. cyberdreiging & economische spionage).
- www.ncsc.nl - Securitybeeld Nederland. Koppeling Whitepapers.
- www.alertonline.nl beveiligingsbewustzijn, ransomware, beveiliging persoonsgegevens.
- www.veiliginternetten.nl - phishing en cybercrime.
- www.fraudehelpdesk.nl – phishing en actiepatronen.
- www.csacademy.nl - informatie, ontwikkelingen. Begrippenlijst (rechter kolom)
- www.veiligbankieren.nl - Fraude (o.a. Phishing en Social Engineering).

Brochures:

Spionage in Nederland

<https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/documenten/brochures/2014/01/31/spionage-in-nederland>

Spionage bij reizen naar het buitenland

<https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/documenten/brochures/2014/01/31/spionage-bij-reizen-naar-het-buitenland>

Digitale spionage

<https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/documenten/brochures/2014/01/31/digitale-spionage>

	Bijlage 7 <i>Rubriceringsaanduidingslijst</i>	
--	---	--

In een zo vroeg mogelijk stadium moet de bijzondere aard van de opdracht door de *Opdrachtgever* worden vastgelegd. De *Opdrachtgever* verstrekt aan de hand van een *Rubriceringsaanduidingslijst (RAL)* Informatie over de aard van de te verstrekken opdracht, het *TBB* die aan het bedrijf wordt overgedragen of aldaar wordt gegenereerd en de hoogte van het beveiligingsniveau hiervan. Aan de hand van deze *RAL* kan de *Opdrachtnemer* beveiligingsmaatregelen gaan toepassen om het *TBB* op de juiste manier te beschermen.

Een *RAL* die de *Opdrachtgever* heeft opgesteld geeft de *Opdrachtnemer* inzicht in welke deelgebieden van toepassing zijn voor de specifieke *Bijzondere Opdracht*.

Buitenlands equivalent *RAL*

Bedrijven kunnen ook in aanmerking komen voor een defensie gerelateerde *Bijzondere Opdracht* van *NAVO*, *EU* of een buitenlandse Defensieorganisatie. Naast nationale *TBB* kan derhalve sprake zijn van *NAVO*- of *EU*- of buitenlandse *TBB*. *BIV / MIVD* treedt naar het betrokken bedrijf op als de aangewezen beveiligingsautoriteit namens die organisaties en landen. Vaak is daarbij de voorwaarde dat daarover afspraken zijn vastgelegd in een veiligheidsverdrag of een zogenaamd *Memorandum of Understanding (MoU)*. *BIV / MIVD* vervult dan de rol van Designated Security Authority (DSA).

NAVO- en *EU*-regelgeving en vaak ook internationale verdragen schrijven voor dat in de contracten met *NAVO*, *EU* en buitenlandse organisaties 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 de *ABDO* 2017. Zo kent de *PSI* een "Security Classification Guide", en de *SAL* een "Security Classification Checklist", het equivalent van de *RAL* uit de *ABDO* 2017. Bedrijven die dergelijke opdrachten krijgen, worden gecontroleerd op basis van de *ABDO* 2017 omdat de daarin opgenomen beveiligingseisen van tenminste hetzelfde niveau zijn als de eisen die *NAVO* en *EU* voor soortgelijke gevallen stellen.

Bijlage 7.1 Formulier Rubriceringsaanduidingslijst	
--	--

ALGEMEEN

	OMSCHRIJVING	ZG / TBB 1	G / TBB 2	C / TBB 3	DV / TBB 4	Geen	OPMERKINGEN
1	Contract						
2	Stafeisen						
3	Omschrijving van de hoofdsamenstelling						
4	Hoofdsamenstelling						
5	Sub samenstelling						
6	Projectbeschrijving						
7	Eindproduct (compleet)						
8	Uiterlijke vorm / aanzicht						
9	Correspondentie betreffende de opdracht						
10	TMT eisen						
11	Tekeningen, calques, eisenbladen, modellen, foto's enz. Berekeningen en rapporten betreffende de constructie						
12	Ontwikkelingsplanning						
13	Productieplanning						
14	Technische specificaties						
15	Analyse						
16	Operationele en technische resultaten						
17	Test- en meetgegevens						
18	Prijscalculaties						
19	Onderdelen						
20	Prototypen						
21	Behoefte						
22	Aantallen te leveren / geleverd						
23	Lijst van reservedelen						
24	Verpakking en verzendinstructies						
25	Gebruiksaanwijzing / handboeken						
26	Documentatie (algemeen)						
27	Keurings- / afleveringsdocumentatie						
28	Fabrieksdocumentatie						
29	Software						
30	ECM / ECCM						
31	Crypto apparatuur en handboeken						
32							
33							
34							
35							
36							

Algemene Beveiligingseisen Defensie Opdrachten 2017

37							
38							
39							
40							

GETEKEND DOOR:	
ONDERDEEL:	
DATUM:	

Bijlage 7.2 Formulier Rubriceringsaanduidingslijst	
--	--

INFRASTRUCTUUR / GEBOUWEN

	OMSCHRIJVING	ZG / TBB 1	G / TBB 2	C / TBB 3	DV / TBB 4	Geen	OPMERKINGEN
1	Correspondentie						
2	Schetsontwerp						
3	Definitief ontwerp						
4	Tekeningen, calques, modellen, foto's e.d.						
5	Project beschrijving						
6	Prijscalculaties						
7	Bestemming / functie van het gebouw						
8	Bestemming / functie ruimten (specificatie)						
9	Indeling van het gebouw						
10	Inrichting van de ruimten (applicatie)						
11	Constructie van het gebouw						
12	Constructie elementen van ruimten						
13	Electrische installatie (c.q. delen daarvan)						
14	Noodstroomvoorziening						
15	Verlichtingsinstallatie (c.q. delen daarvan)						
16	Verwarmingsinstallatie						
17	Luchtbehandeling, gas afsluitende/gasdichte voorzieningen Watervoorzieningsinstallatie						
18	Noodwatervoorziening						
19	Telefoon-intercominstallatie						
20	Telex-crypto installatie						
21	Elektrische / elektronische alarmeringsinstallatie						
22	EMP-beveiliging						
23	NBC-beveiliging						
24	Computerruimte						
25	Test- en meetgegevens						
26	Bedieningsinstructies						
27	Onderhoudsinstructies (specificaties)						
28	Bijzondere technische voorzieningen						
29							
30							

Algemene Beveiligingseisen Defensie Opdrachten 2017

TERREINEN / WERKEN

	OMSCHRIJVING	ZG / TBB 1	G / TBB 2	C / TBB 3	DV / TBB 4	Geen	OPMERKINGEN
1	Bestemming						
2	Waterhuishouding - riolering - drainage - watergangen						
3	Inrichting						
4	Opstellen (specificatie)						
5	Elektriciteitsvoorziening - hoogspanningsinstallatie - laagspanningsinstallatie						
6	Gasdistributiesysteem						
7	Watervoorzieningssysteem - koelwater - drinkwater - bluswater						
8	Rioolwater afvoersysteem - riolering - waterzuiveringsinstallatie(s)						
9	Afrastering						
10	Elektrische / elektronische						
11	alarmeringsinstallatie(s)						
12	EMP-beveiliging						
13							
14							
15							
16							

GETEKEND DOOR:	
ONDERDEEL:	
DATUM:	

	Bijlage 8 Logistieke keten	
--	--	--

De *Opdrachtnemer* zal doorgaans niet geheel onafhankelijk van derden de *Bijzondere Opdracht* uitvoeren, maar een logistieke keten van bedrijven vertegenwoordigen naar de *Opdrachtgever*. Vanuit beveiligingsoogpunt is het noodzakelijk inzicht te hebben in de keten en zonodig eisen te stellen aan de schakels in die keten.

Op hoofdlijnen bestaat de logistieke keten naast de *Opdrachtnemer* uit meerdere *Subcontractors* en (*Toe-)**leveranciers*. Dit zijn andere bedrijven (d.w.z. andere rechtspersonen dan de *Opdrachtnemer*) waaraan de *Opdrachtnemer* bepaalde werkzaamheden aan een *TBB* uitbesteed.

De *ABDO 2017* dient derhalve naast van toepassing op de *Opdrachtnemer* zelf ook van toepassing te zijn op alle *Subcontractors* (en eventuele sub-*Subcontractors*) en (*Toe-)**leveranciers* die in aanraking kunnen komen met of toegang hebben tot een *TBB* of dit produceren. De *ABDO 2017* dient ook van toepassing te zijn op *Subcontractors* en (*Toe-)**leveranciers* van systeemonderdelen die op grond van hun kritische / *Vitale* functie een zekere mate van bescherming verdienen. Op basis van het door *Opdrachtnemer* verschaft inzicht wordt in overleg met *BIV / MIVD* bepaald op welke betrokken *Subcontractors* en/of (*Toe-)**leveranciers* de *ABDO 2017* van toepassing is. Zodoende kunnen alle betrokken partijen in de keten voor wat betreft beveiliging onder toezicht worden geplaatst. Mocht de beoogde *Subcontractor* en/of (*Toe-)**leverancier* zich in het buitenland bevinden, dan dient in plaats van de *ABDO 2017* te worden verwezen naar de in het betreffende land vigerende regelgeving m.b.t. industrieveiligheid. *BIV / MIVD* vraagt in dergelijke gevallen bij de buitenlandse partner een zogenoemde Facility Security Clearance op.

Subcontractors en (Toe-)leveranciers

Wanneer een *Opdrachtnemer* werkzaamheden aan een *TBB* uitbesteedt of *Vitale* systeemonderdelen van derden betreft worden de *Subcontractors* en/of (*Toe-)**leveranciers* voorafgaand aan het contract door de *Opdrachtnemer* schriftelijk aangemeld bij *BIV / MIVD*, zie hiervoor bijgevoegd formulier. *Opdrachtnemer* wordt conform de procedure zoals beschreven in **Leidraad procedure ABDO** van de *ABDO 2017* door *BIV / MIVD* al dan niet geautoriseerd om hen in te schakelen. In het contract met hen dient door de *Opdrachtnemer* de *ABDO 2017* bedongen te worden. De reguliere *ABDO 2017* procedure wordt derhalve gevolgd om de *ABDO 2017* eisen aan hen op te leggen, alvorens zij kunnen starten met hun werkzaamheden en/of het leveren van *Vitale* systeemonderdelen. Mochten zij zich in het buitenland bevinden, dan dient in plaats van de *ABDO 2017* te worden verwezen naar de in het betreffende land vigerende regelgeving m.b.t. industrieveiligheid. *BIV / MIVD* vraagt in dergelijke gevallen bij de buitenlandse partner een zogenoemde Facility Security Clearance op.

ZZP'er

De zelfstandige zonder personeel (hierna ZZP'er) is een bijzondere bedrijfsvorm. Bij een ZZP'er zijn alle taken en functies die in een bedrijf normaliter zijn belegd bij verschillende personen of bedrijfsonderdelen, verenigd in een persoon. Vanwege de flexibiliteit van deze bedrijfsvorm maken Defensie en *Opdrachtnemers* veelvuldig gebruik van ZZP'ers. Vanuit beveiligingsoogpunt wordt een ZZP'er in beginsel op dezelfde wijze beoordeeld als een *Opdrachtnemer* of *Subcontractor*. Dat wil zeggen dat een ZZP'er die werkt aan een *TBB* waarop de *ABDO 2017* van toepassing is, aan de beveiligingseisen zoals vermeld in de *ABDO 2017* dient te voldoen. De bijzondere omstandigheid van de ZZP'er, die de werkzaamheden vaak niet uitvoert in een bedrijfspand maar in een daartoe ingerichte ruimte in zijn privé-omgeving, heeft echter tot gevolg dat mogelijk niet aan alle eisen van de *ABDO 2017* kan worden voldaan. Maatwerk dient hierbij uitkomst te bieden.

Algemene Beveiligingseisen Defensie Opdrachten 2017

In een aantal gevallen is het niet noodzakelijk om de ZZP'er vanuit beveiligingsoogpunt als bedrijf te behandelen, bijvoorbeeld als deze de (gerubriceerde) werkzaamheden uitvoert op locatie van *Opdrachtnemer* of op Defensielocatie, gebruikmakend van de geacordeerde IT-infrastructuur van *Opdrachtnemer* of van Defensie. Als een ZZP'er als een bedrijf wordt beschouwd in de zin van de *ABDO 2017*, functioneert de ZZP'er als zijn eigen *BF* en dient derhalve zijn eigen aanvraag *Veiligheidsonderzoek* in.

Als het een buitenlandse *Opdrachtgever* betreft wordt de ZZP'er altijd als een bedrijf beschouwd.

Dienstverleners (Serviceproviders)

Een *Dienstverlener* levert bepaalde hulp / ondersteuning aan de *Opdrachtnemer* of aan *Subcontractors* en/of *(Toe)leveranciers* hetgeen kan variëren van facilitair (schoonmaak, bewaking, catering) tot IT-diensten. Vaak wordt de term *Serviceprovider* uitsluitend geassocieerd met internet- en telefoniediensten. De *ABDO 2017* is van toepassing op *Dienstverleners* die in aanraking kunnen komen met of toegang hebben tot een *TBB* of dit produceren, ofwel een product leveren dat op zichzelf geen *TBB* is maar van invloed is op de integriteit van het uiteindelijke systeem.

Een eventuele interne dienstverlener valt onder de *Opdrachtnemer*, d.w.z. de *ABDO 2017* is daarop automatisch van toepassing.

	Bijlage 8.1 Formulier aanvraag <i>Subcontractors</i> en/of <i>(Toe)leveranciers</i>	
--	---	--

Aanvraag voor toestemming voor het inschakelen van een *Subcontractor*

Indien ten behoeve van de uitvoering van een *Bijzondere Opdracht* een *Subcontractor* moet worden ingeschakeld, dient hiervoor vooraf door middel van dit formulier toestemming te worden gevraagd aan *BIV / MIVD*.

Onder '*Subcontractor*' wordt verstaan: (interne) *Subcontractors*, (*Toe*-) *Leveranciers* en (interne) *Serviceproviders*, ZZP-ers.

Naar:

Bureau Industrie Veiligheid

Algemene Beveiligingseisen Defensie Opdrachten 2017

Indussec@mindef.nl

070- 4419463

Behoeftesteller / Opdrachtgever
Naam
Adres
Postcode / Plaats
Contactpersoon
Telefoonnummer
Email

Subcontractor / Opdrachtnemer
Naam
Adres
Postcode / Plaats
Contactpersoon
Telefoonnummer
Email

Het betreft
Naam opdracht
Omschrijving opdracht
Aanvang en looptijd van opdracht
Rubricering
Locatie van werkzaamheden
Wordt een <i>TBB</i> op locatie van <i>Subcontractor</i> verwerkt, opgeslagen en/of gegenereerd? - Zo ja, op welke manier? Fysiek ☐ Digitaal ☐
Is de <i>ABDO</i> bedongen in het contract? - Zo ja, wanneer? - Zo nee, dan dient alsnog in het af te sluiten contract alsnog te geschieden.
Een ingevulde <i>RAL</i> dient bijgevoegd te worden bij deze aanvraag.

Ondertekening
Naam <i>Beveiligingsfunctionaris</i>
Datum

Algemene Beveiligingseisen Defensie Opdrachten 2017

Handtekening

Alleen in te vullen door BIV / MIVD

Goedgekeurd door

Afgekeurd door

Datum

Rubriceringsniveau

TBB op locatie Subcontractor

Fysiek

☐

Opmerkingen:

Digitaal

☐

Zie volgende pagina voor formulier *RAL*.

Algemene Beveiligingseisen Defensie Opdrachten 2017

	OMSCHRIJVING	ZG / TBB 1	G / TBB 2	C / TBB 3	DV / TBB 4	Geen	OPMERKINGEN
1	Contract						
2	Stafeisen						
3	Omschrijving van de hoofdsamenstelling						
4	Hoofdsamenstelling						
5	Sub-samenstelling						
6	Projectbeschrijving						
7	Eindproduct (compleet)						
8	Uiterlijke vorm / aanzicht						
9	Correspondentie betreffende de opdracht						
10	TMT eisen						
11	Tekeningen, calques, eisenbladen, modellen, foto's enz. Berekeningen en rapporten betreffende de constructie						
12	Ontwikkelingsplanning						
13	Productieplanning						
14	Technische specificaties						
15	Analyse						
16	Operationele en technische resultaten						
17	Test- en meetgegevens						
18	Prijscalculaties						
19	Onderdelen						
20	Prototypen						
21	Behoefte						
22	Aantallen te leveren / geleverd						
23	Lijst van reservedelen						
24	Verpakking en verzendinstructies						
25	Gebruiksaanwijzing / handboeken						
26	Documentatie (algemeen)						
27	Keurings- / afleveringsdocumentatie						
28	Fabrieksdocumentatie						
29	Software						
30	ECM / ECCM						
31	Crypto apparatuur en handboeken						
32							
33							
34							
35							
36							
37							
38							
39							
40							

	Bijlage 9 Incident Handling procedure	
--	---	--

Wanneer *compromittatie* van een *TBB* of een poging daartoe heeft plaatsgevonden of wordt vermoed, is er sprake van een *Beveiligingsincident*. Als gesignaleerd wordt dat dit zich voordoet of heeft voorgedaan is een adequate afhandeling vereist conform de Incident Responce Procedure (IRP). Het hoofddoel daarbij is zo snel mogelijk de schade te beperken en maatregelen te treffen ter voorkoming van herhaling. Dit wordt bewerkstelligd door:

- het vastleggen van alle *Informatie* over het incident;
- voorlopige analyse en validatie ter vaststelling van de mogelijke schade;
- het informeren van de belanghebbenden;
- het treffen van maatregelen ter beperking van de schade;
- het aanpassen van het gebruik van of de werkzaamheden aan het *TBB*;
- het aanpassen van de beveiligingsmaatregelen teneinde herhaling te voorkomen.

In deze **bijlage** is een stappenplan (**bijlage 9.1**) opgenomen volgens welk een gestructureerde afhandeling van een *Beveiligingsincident* dient plaats te vinden. Deze is gebaseerd op de internationale "Incident Handling"-methodiek. Naast het stappenplan kent deze methodiek een classificatie - indeling (**bijlage 9.2**) die de mate van urgentie van handelen aangeeft. In **bijlage 9.3** is een 'eerste incident rapport' toegevoegd om een eerste schriftelijke melding te maken van het (mogelijke) incident. Alleen door vlotte en voortvarende opvolging wordt de schade door (mogelijke) *Compromittatie* in de kortst mogelijke tijd tot een minimum gereduceerd zodat de operationele en financiële schade voor Defensie en *Opdrachtnemer* beperkt kan blijven.

Bijlage 9.1 Incident Handling stappenplan		
---	--	--

Bij digitale incidenten dienen er in het Incident Handling proces extra stappen te worden genomen. Dit is in dit stappenplan in rood aangegeven en voorzien van een *.

Stap ^s	Doel	Uitvoering
1. Identificatie	Valideren, identificeren en rapporteren.	1. Verzamel de audit logs en analyseer. 2. Rapporteer direct na constatering van het incident via een initiele melding naar <i>BIV / MIVD</i> en eigen management (telefonisch via accountmanager én via Incident Handling formulier, te vinden in bijlage 9.3). 3. Stel het onderzoeksteam samen. 4. Bepaal de initiele impact van het incident en classificeer.
2. Incident vastlegging	Leg de details van het voorval vast.	1. Leg datum en tijdstip vast. 2. Wie is de melder? 3. Details van het incident.
3. Eerste response	Verzamel voldoende informatie om de juiste respons vast te stellen.	1. Onderzoek het incident (echtheid of 'valse positive'). 2. Leg details vast. 3. Pas eventueel de teamsamenstelling aan. 4. Communiceer naar medewerkers binnen het defensieproject.
4. Communicatie	Communicatie en afstemming met belanghebbenden.	1. Ingeval van een niet-Cyber incident: Bespreek het incident met teamleden van het incident response team en de accountmanager van <i>BIV / MIVD</i>. 2. Ingeval van een Cyber incident: Bespreek het incident in een sessie met teamleden van het incident response team en met de Cyber auditor <i>BIV / MIVD</i>. * 3. Bepaal de maatregelen en verdere coordinatie om de impact te reduceren.
5. Containment	Beperk de scope en impact van het incident.	1. Mogelijkheden. 2. Uitzetten systeem. 3. Stoppen van de service. 4. Ontkoppelen accounts. 5. Maak een volledige Backup van het geïnfecteerde systeem. 6. Restoratie van het geïnfecteerde systeem.
6. Response strategie	Bepaal respons. Situationeel afhankelijk.	Onderzoek de meest passende respons. Neem daarbij de politieke, technische en juridische factoren in overweging.
7. Classificatie	Bepaal de classificatie van het incident met behulp van tabel "classificatie".	1. Substap. 2. Categoriseer. 3. Prioriteer. 4. Alloceer resources. Noot: Neem hierbij tevens in overweging: 1. Kritiekheid van het systeem. 2. Verschijning van het incident. (ramp of vorm van digitale aanval). * 3. Reikwijdte van het incident. 4. Juridisch werkkader.

Algemene Beveiligingseisen Defensie Opdrachten 2017

8. Incident onderzoek	Verzamelen van bewijsmateriaal in relatie tot het incident.	1. Identificeer. 2. Incident beschrijving. 3. Datum, tijdstip van het incident. 4. Oorsprong van het incident (actor). 5. Mitigatie stappen om herhaling te voorkomen.
9. Data Collection	Verzamelen van feiten en bewijsmiddelen op hosts, netwerk apparatuur, en andere media, nodig voor forensisch onderzoek.	1. Hosts: Verzamel logs, system backups, data in vluchtige geheugen zoals: datum tijd stamps, application logs, open ports, luisterende applicaties en status van netwerk interfaces. * 2. Netwerk apparatuur: IDS/IPS logs, router logs, wire taps, authentication servers. * 3. Overige: verzamel informatie van andere bronnen via interviews en sociale media.
10. Forensische analyse	Analyse en reviewing van verzamelde data.	Stappen: a. Fotografeer te onderzoeken materiaal. b. Software analyse, keyword zoekslag, datum / tijd chronologie. * c. Onderzoek data die systematisch van het systeem verwijderd is. * d. Documenteer forensics op processen en activiteiten.
11. Bescherming van bewijsmateriaal	Nodig om de informatie voor juridische stappen te kunnen gebruiken.	1. Maak een volledige backup op een nog nooit gebruikte gegevensdrager. * 2. Bescherm tegen fysieke en logische schade. 3. Documenteer de chain-of-custody (beheer keten?).
12. Neutralisatie	Lost de oorzaak van het incident op.	1. Kwetsbaarheid wegnemen. 2. Voorkom door implementatie van de maatregel dat de kwetsbaarheid opnieuw wordt uitgenut.
13. System recovery	Breng het systeem terug naar normale operationele omstandigheden. Systemen en netwerken worden gemonitord en zijn gevalideerd.	1. Bepaal de werkwijze tot volledige recovery. * 2. Monitor het systeem op netwerk loggers, system files en mogelijke backdoors. * a. Bouw het Operating System op. * b. Restore de data vanuit de backup. * c. Onderzoek mogelijk bescherming en detectie maatregelen. * d. Installeer security patches en log functionaliteit. *
14. Incident documentatie	Documenteer de stappen en conclusies direct na voltooiing van het forensisch onderzoek.	1. Beschrijf : a. Het <i>Beveiligingsincident</i>. b. De oorzaak. c. Genomen maatregelen i. Wie ii. Welke iii. Wanneer Voor de verzending naar BIV / MIVD wordt gebruik gemaakt van het format Incident Handling en meldingen rapport, te vinden in bijlage 9.3.
15. Incident schade assessment	Bepaal het effect van het security incident.	Bepaal in samenspraak met de accountmanager en / of <i>Cyber</i> auditer BIV/MIVD het effect van het incident op de BO van het Ministerie van Defensie.
16. Review & update response procedure	Lessons learned.	1. Bepaal hoe het beveiligingsplan aangepast moet worden aan de hand van het incident. 2. Update het beveiligingsplan.

Algemene Beveiligingseisen Defensie Opdrachten 2017

17. Rapportage	Afdoening.	Schrijf een rapport met daarin de uitwerking van alle bovenstaande stappen en biedt deze aan aan de <i>MIVD</i> .
----------------	------------	---

Bijlage 9.2 Incident Handling classificatie		
---	--	--

Categorie	Name	Omschrijving <u>Digitaal</u>	Omschrijving <u>Fysiek</u>	Time frame
<u>Cat 0</u>	Oefening en (netwerk) test Na vooraf gemeld te hebben: EXERCISE EXERCISE EXERCISE	Deze categorie wordt gebruikt gedurende netwerk testen en oefen situaties. Deze categorie wordt bij communicatie mondeling dan wel schriftelijk voorafgegaan door driemaal EXERCISE te vermelden teneinde verwarring met een echt incident te vermijden.	Deze categorie wordt gebruikt gedurende testen en oefen situaties.	Niet van toepassing.
<u>Cat 1</u>	Ongeautoriseerde toegang	Een individu heeft bewust ongeautoriseerde logische of fysieke toegang tot bijzondere informatie op een netwerk, systeem, applicatie of data.	Een individu heeft bewust ongeautoriseerde toegang tot bijzondere informatie gekregen of heeft niet geautoriseerde toegang gekregen tot een beveiligde ruimte.	Binnen <u>1 uur</u> na detectie.
<u>Cat 2</u>	<i>Denial of Service (DoS)</i>	Een aanval die succesvol voorkomt dat geautoriseerde medewerkers toegang krijgen of hebben tot <i>Bijzondere Informatie</i> . Deze situatie omvat ook het zijn van een slachtoffer in een <i>DoS</i> aanval.	Activiteiten die er toe leiden dat geautoriseerde personen geen toegang kunnen krijgen tot <i>Bijzondere Informatie</i> of beveiligde ruimtes.	Binnen <u>2 uur</u> na detectie indien de aanval plaatsvindt of heeft plaatsgevonden
<u>Cat 3</u>	Malicious software	Succesvolle besmetting van malicious software (worm, virus, Trojan Horse of andere vormen van <i>Malware</i>) die <i>Operating Systems</i> of applicaties besmette software. Uitzondering op deze meldplicht is een succesvol gemitigeerde besmetting op een niet geclassificeerd netwerk of host.	Geconstateerd is dat een maatregel uit een van de categoriën O,B, E en R buiten werking is gesteld.	Binnen 1 dag. Note: Wanneer de besmetting een <i>Stg.</i> gerubriceerd netwerk betreft, binnen 1 uur. Wanneer van toepassing direct op een beveiligde ruimte, binnen 1 uur.
<u>Cat 4</u>	Ongeoorloofd gebruik	Een individu overtreedt de <i>ABDO</i> regels	Een individu overtreedt de <i>ABDO</i> regels.	Binnen 1 week.
<u>Cat 5</u>	Scans / Probes / Pogingen tot toegang.	Deze categorie bevat alle min of meer gerichte activiteiten die er toe dienen een netwerk, host, open port, protocols, service of een combinatie voor latere exploitatie te gebruiken. Ongerichte scan behoren niet tot deze meldplicht.	Deze categorie bevat alle min of meer gerichte activiteiten die er toe dienen zich later toegang te verschaffen tot de <i>Bijzondere</i>	Binnen 1 maand. Indien het een gerubriceerd netwerk betreft of een beveiligde ruimte, binnen 1 uur.

Algemene Beveiligingseisen Defensie Opdrachten 2017

			<i>Informatie of beveiligde ruimtes (o.a. verkenningen, inclusief periferie).</i> Ongerichte aandacht behoort <u>niet</u> tot deze meldplicht.	
--	--	--	--	--

	Bijlage 9.3 Incident Eerste Rapport	
--	--	--

ABDO 2017 INCIDENT Eerste Rapport
--

Incidentnummer	
Datum	
Naam	
Email	
Telefoon	

Datum en tijd waarop het incident is opgemerkt			
Status van het incident	☐ Actief	☐ Inactief	
Soort incident	☐ Cat 1 ☐ Cat 3 ☐ Cat 5 ☐ Cat 2 ☐ Cat 4		
Korte omschrijving van het incident			
Vertrouwelijkheid van de betrokken data	☐ TBB 1 / Stg. Zeer Geheim ☐ TBB 3 / Stg. Confidentieel ☐ TBB 2 / Stg. Geheim ☐ TBB 4 / Departementaal Vertrouwelijk		
Hoe is het incident ontdekt en door wie?			

Eerste analyse	
----------------	--

Handtekening	
--------------	--

Print deze pagina uit en stuur het ingevuld op naar uw accountmanager of indussec@mindef.nl

	Bijlage 10 <i>Vertrouwensfuncties</i>	
--	---	--

Een *Vertrouwensfunctie* is een functie zoals bedoeld in de Ambtenarenwet 1929 en in de *Wet veiligheidsonderzoeken (Wvo)*. De minister van Defensie mag slechts een functie als *Vertrouwensfunctie* aanwijzen indien de taken van die functie de mogelijkheid bieden de nationale veiligheid te schaden. Hiervan is sprake indien:

- het een functie betreft waarbij kennis wordt/kan worden genomen van *Staatsgeheimen*. Functies waarbij kennis wordt genomen van *Crypto* -informatie of -materiaal vormen in dezen een bijzondere categorie;
 - de functie van *Vitaal* belang is voor de instandhouding van het maatschappelijk leven;
 - het een functie betreft waarbij toegang tot militaire installaties noodzakelijk is.
- Werkzaamheden waarbij kennis moet of kan worden genomen van een *TBB*, in het bijzonder *Bijzondere Informatie (BI)*, alsmede werkzaamheden die in andere zin van belang zijn in verband met de beveiliging van *Staatsgeheimen*, mogen uitsluitend worden opgedragen aan werknemers die een *Vertrouwensfunctie* vervullen.

Verplichtingen van de *Vertrouwensfunctionaris*

Belangrijke verplichtingen van de *Vertrouwensfunctionaris* zijn onder andere:

- het nauwkeurig naleven van de beveiligingsregels van de *Opdrachtnemer*;
- sociale controle (elkaar scherp houden en wijzen op verantwoordelijkheden);
- melden van nalatigheden;
- verantwoord gedrag op sociale media;
- melden van incidenten;
- melden van wijzigingen in persoonlijke omstandigheden;
- uitsluitend gebruik van door Defensie goedgekeurde (mobiele) apparatuur en datadragers zoals telefoons, laptops, notebooks, usb-sticks, etc. bij een *Bijzondere Opdracht (BO)*.

Lijst van Vertrouwensfuncties

De *Lijst van Vertrouwensfuncties (LvV)*, zie hiervoor het formulier in deze bijlage, is een overzicht van de maximum aantallen *Vertrouwensfuncties*, verdeeld over 13 functiecategorieën die bij de *Opdrachtnemer* noodzakelijk zijn om een of meerdere *BO* uit te voeren. Per functiecategorie wordt het aantal *Vertrouwensfuncties* opgesplitst naar het vereiste *Veiligheidsmachtigingsniveau* (A, B of C). In de kolom *NAVO* (en *EU*) wordt het aantal *Vertrouwensfunctionarissen* aangegeven dat uit hoofde van hun functie extern (bijvoorbeeld bij bezoek aan het NAVO-Hoofdkwartier) aan moeten kunnen tonen te beschikken over de vereiste security clearance. Aan hen wordt een zogenaamde *NATO Personnel Security Clearance Certificate (PSCC)* verstrekt.

Algemene Beveiligingseisen Defensie Opdrachten 2017

De *LvV* wordt opgesteld door de *BF* van de *Opdrachtnemer* in overleg met *BIV / MIVD*.

Besluit aanwijzing *Vertrouwensfuncties*

De *LvV* wordt door de *MIVD* namens de minister van Defensie, eventueel in overeenstemming met de *Algemene Inlichtingen- en Veiligheidsdienst (AIVD)* namens de minister van Binnenlandse Zaken en Koninkrijksrelaties⁶, formeel vastgesteld door middel van het “Besluit aanwijzing *Vertrouwensfuncties*”. Op grond van dit besluit kunnen *Veiligheidsonderzoeken* worden aangevraagd. De in de *LvV* genoemde maximum aantallen mogen niet zonder voorafgaande toestemming van *BIV / MIVD* worden overschreden. Bij wijziging van de opdracht of van het aantal opdrachten dient herziening van de *LvV* plaats te vinden. De gewijzigde *LvV* wordt door middel van een wijzigingsbesluit wederom formeel vastgesteld. Als een *Opdrachtnemer* doorlopend één of meerdere gerubriceerde opdrachten uitvoert voor het ministerie van Defensie kan een integrale, permanente *LvV* worden opgesteld.

Indien een bedrijf in de offertefase reeds in aanraking komt met een *TBB* wordt een tijdelijke *LvV* opgesteld. Deze wordt ingetrokken als geen gunning plaatsvindt en uitgebreid tot de definitieve *LvV* als wel gunning plaatsvindt. Na beëindiging van de opdracht(en) wordt de *LvV* ingetrokken nadat, indien van toepassing, het *TBB* conform het contract is geretourneerd aan Defensie of is vernietigd en kennisname van of toegang tot het *TBB* door de *Opdrachtnemer* niet meer mogelijk is. Het bedrijf wordt schriftelijk in kennis gesteld van verwijdering uit het actieve *ABDO*-bestand van *BIV / MIVD*. De *LvV* en *Verklaringen van Geen Bezwaar (VGB)* dienen te worden vernietigd.

⁶ Overeenstemming met de *AIVD* is noodzakelijk indien de *AIVD* zorgdraagt voor de verstrekking van de *VGB* aan medewerkers van de *Opdrachtnemer*.

Bijlage 10.1		
Model <i>Lijst van Vertrouwensfuncties</i>		

DATUM:		CATEGORIE:				
NAAM ORGANISATIE:		WERKGEVERSCODE:				
VESTIGINGSPLAATS:						
WERKVELD/VERTROUWENSFUNCTIE	MACHTIGINGSNIVEAU			DEELNEMER		
	(A) 011 (ZEER GEHEIM)	(B) 012 (GEHEIM)	(C) 013 (CONFIDEN- TIEEL)	NAVO	EU	
E	BELEID EN MANAGEMENT DIRECTEUR / CEO					
E	BELEID EN MANAGEMENT MEDEWERKER BELEID EN MANAGEMENT					
F	AUTOMATISERING MEDEWERKER AUTOMATISERING					
G	ADMINISTRATIE/ONDERSTEUNING MEDEWERKER ADMINISTRATIE/ONDERSTEUNING					
H	VERWERVING/AANBESTEDING MEDEWERKER VERWERVING/AANBESTEDING					
K	BEWAKING/BEVEILIGING MEDEWERKER BEWAKING/BEVEILIGING					
L	PERSONEELSVORZIENING MEDEWERKER PERSONEELSVORZIENING					

Algemene Beveiligingseisen Defensie Opdrachten 2017

M	FINANCIËN MEDEWERKER FINANCIËN					
N	ONDERZOEK MEDEWERKER ONDERZOEK					
P	PRODUCTIE MEDEWERKER PRODUCTIE					
R	COMMERCEEL MEDEWERKER COMMERCEEL					
S	TECHNIEK/INSTALLATIE MEDEWERKER TECHNIEK/INSTALLATIE					
T	OVERIG MEDEWERKER					
U	(SUB) BEVEILIGINGSFUNCTIONARIS MEDEWERKER BEVEILIGINGSFUNCTIONARIS					
<u>TOTAAL AANTAL:</u>						

A	Bijlage 11 <i>Veiligheidsonderzoek , VGB en VOG</i>
---	---

Het *Veiligheidsonderzoek* en de *Verklaring van Geen Bezwaar*

Medewerkers die door de *Opdrachtnemer* geplaatst worden op een *Vertrouwensfunctie* dienen te beschikken over een geldige *VGB*. Pas dan mogen betrokkenen op de *Vertrouwensfunctie* worden geplaatst. Ter verkrijging van een *VGB* dienen zij een *Veiligheidsonderzoek* te ondergaan. Daarvoor dienen zij door middel van het invullen en ondertekenen van een (elektronische) *Opgave Persoonlijke Gegevens (OPG)*, indien het *Veiligheidsonderzoek* wordt uitgevoerd door de *AIVD*) of *Staat van Inlichtingen (SVI)*, indien het *Veiligheidsonderzoek* wordt uitgevoerd door de *MIVD*) toestemming te geven die tevens toestemming inhoudt voor hernieuwde onderzoeken zolang de *Vertrouwensfunctie* wordt uitgevoerd. Het proces dat leidt tot afgifte, verlenging, intrekking of weigering van een *VGB* wordt *Veiligheidsonderzoek* genoemd. Aan de aanvraag van een *VGB* zijn kosten verbonden die bij de aanvrager in rekening worden gebracht. De tarieven zijn afhankelijk van het gevraagde *Veiligheidsmachtigingsniveau*.

Veiligheidsonderzoeken worden aangevraagd door de *BF* van de *Opdrachtnemer* door aan de ingevulde *OPG* of *SVI* een ingevuld aanvraagformulier toe te voegen en het geheel vervolgens te zenden naar *BIV / MIVD* respectievelijk *MIVD* ter attentie van Bureau Veiligheidsonderzoeken Defensie. Indien uit het *Veiligheidsonderzoek* blijkt dat er voldoende waarborgen aanwezig zijn dat betrokkene de uit de *Vertrouwensfunctie* voortvloeiende plichten onder alle omstandigheden getrouwelijk zal volbrengen, wordt de *VGB* afgegeven danwel verlengd. Is dat niet het geval dan wordt de *VGB* niet afgegeven danwel ingetrokken en kan betrokken medewerker niet op een *Vertrouwensfunctie* worden geplaatst danwel gehandhaafd. Het is mogelijk om tegen een (voornemen tot) weigering of intrekking van een *VGB* bezwaar aan te tekenen.

Afhankelijk van het aan de functie toegekende *Veiligheidsmachtigingsniveau* (hierna *VMN*) vindt het *Veiligheidsonderzoek* plaats op:

- A-niveau, indien werkzaamheden worden verricht met betrekking tot *Stg. ZEER GEHEIM* en lager *gerubriceerde Staatsgeheimen*;
- B-niveau, indien werkzaamheden worden verricht met betrekking tot *Stg. GEHEIM* en lager *gerubriceerde Staatsgeheimen*;
- C-niveau, indien werkzaamheden worden verricht met betrekking tot *Stg. CONFIDENTIEEL* en lager *gerubriceerde Informatie*.

Indien sprake is van werkzaamheden met betrekking tot *Vitale* (niet *gerubriceerde*) of grote hoeveelheden laag gerubriceerde en/of gemerkte *Informatie* kan eveneens een *VMN A, B of C* aan een functie worden toegekend en is een *Veiligheidsonderzoek* noodzakelijk . Een en ander ter beoordeling van *BIV / MIVD* op basis van het *DBB* en zonodig in overleg met de Beveiligingsautoriteit

van Defensie. Zo wordt bijvoorbeeld aan systeembeheerders met ‘full administrative privileges’ die toegang hebben tot grote hoeveelheden op zich ongerubriceerde gegevens het VMN B toegekend.

Conform de *Wvo* wordt een *Veiligheidsonderzoek* in beginsel uitgevoerd door de *AIVD*. Indien het een functie betreft die als *Vertrouwensfunctie* moet worden aangemerkt op grond van de noodzaak om toegang te hebben tot militaire installaties, wordt het *Veiligheidsonderzoek* uitgevoerd door de *MIVD*.

Aanstelling voor korte duur

In verband met ongewenste verspreiding van *Staatsgeheimen* en onder afweging van de kosten en baten van het *Veiligheidsonderzoek*, zowel in geld als in tijd, dient uiterste terughoudendheid te worden betracht met het plaatsen van tijdelijke medewerkers (bijvoorbeeld uitzendkrachten en stagiairs) op *Vertrouwensfuncties*.

Hernieuwd *Veiligheidsonderzoek*

Een *Veiligheidsonderzoek* jegens een betrokken *Vertrouwensfunctionaris* vindt elke vijf jaren plaats. Tenminste drie maanden voor het verstrijken van de periode van vijf jaar na afgifte *VGB* dient door de *BF* een nieuw veiligheidsonderzoek te worden aangevraagd, waarbij tevens een opnieuw ingevulde *OPG* of *SVI* dient te worden toegevoegd.

Verklaring Omtrent het Gedrag

Indien sprake is van werkzaamheden met betrekking tot maximaal *Departementaal Vertrouwelijk* (*TBB 4*) gerubriceerde *Informatie* vindt in beginsel geen *Veiligheidsonderzoek* plaats. Wel is in zulke gevallen een zogenoemde *Verklaring Omtrent het Gedrag* (*VOG*) vereist die betrekking heeft op bepaalde categorieën justitiële antecedenten. Een *VOG* wordt afgegeven door Dienst Justis van het ministerie van Veiligheid en Justitie (V&J) en is aan te vragen via de gemeente van inschrijving. V&J hanteert bij de beoordeling een aantal verschillende profielen. Op het aanvraagformulier dienen bij het algemeen screeningsprofiel de functieaspecten te worden aangekruist die corresponderen met de opgedragen functie.

Bijlage 11.1

Aanvragen van een *Veiligheidsonderzoek* en/of *Verklaring Omtrent het Gedrag*

Veiligheidsonderzoek

- <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/documenten/brochures/2013/10/22/beleidsregele-veiligheidsonderzoeken>
- <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/documenten/brochures/2015/02/05/leidraad-gedrag-bij-veiligheidsonderzoek>
- <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/documenten/richtlijnen/2013/10/21/beleidsregel-veiligheidsonderzoeken-defensie>

- <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/inhoud/veiligheidsonderzoek>

- <https://www.aivd.nl/onderwerpen/veiligheidsonderzoeken/inhoud/digitale-formulieren-veiligheidsonderzoek>

VOG

- <https://www.justis.nl/producten/vog/>

- <https://www.justis.nl/producten/vog/vog-aanvragen/>

Bijlage 12

Verklaring van bekendheid met de geheimhoudingsplicht voor (*Vertrouwens*)functionarissen

Medewerkers van de *Opdrachtnemer* die kennis moeten nemen dan wel toegang hebben tot een *TBB* dienen een *Geheimhoudingsverklaring* te ondertekenen waarin wordt verklaard dat zij op de hoogte zijn gesteld van de bepalingen omtrent de geheimhoudingsplicht en de strafmaatregelen op basis van het *Wetboek van strafrecht (Wvs)* bij het verzaken van die plicht (zie formulier 1 in deze bijlage). Medewerkers die bovendien kennis moeten nemen van *Crypto*, *Crypto-security* of *CCI-gemerkte* informatie of materieel dienen een *Geheimhoudingsverklaring* in het kader van een *Crypto*-functie te ondertekenen (zie formulier 2 in deze bijlage).

Vanaf *TBB* 3 en hoger dient de *Geheimhoudingsverklaring* elke 5 jaar te worden vernieuwd.

Bijlage 12.1

Verklaring van bekendheid met de geheimhoudingsplicht voor (*Vertrouwens*)functionarissen

Ondergetekende,

Naam : _____

Geboortedatum : _____

Geboorteplaats : _____

Verklaart hierbij dat hij/zij:

- op de hoogte is gesteld van de verplichting tot geheimhouding van de gerubriceerde *Informatie* die hem/haar ter kennis komen;
- de voorschriften welke zijn of zullen worden gegeven inzake de beveiliging van die *Informatie* getrouwelijk te zullen nakomen;
- die *Informatie* niet aan niet gerechtigden zal onthullen;
- kennis heeft genomen van de bepalingen in het *Wetboek van Strafrecht* inzake geheimhouding, te weten de artikelen 2, 3, 4, 5, 23, 98, 98a, 98b, 98c, 272 en 273 en dat hij / zij de betekenis en het belang van die bepalingen heeft begrepen.

Plaats : _____

Datum : _____

Handtekening : _____

Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst
Bureau Industrieveiligheid

Bijlage 12.1

Verklaring van bekendheid met de geheimhoudingsplicht voor (Vertrouwens)functionarissen

WETSARTIKELEN

Art. 2, 3, 4, 5, 23, 98, 98a, 98b, 98c, 272, 273 Wvs.

Art. 2. De Nederlandse Strafwet is toepasselijk op ieder die zich in Nederland aan enig strafbaar feit schuldig maakt.

Art. 3. De Nederlandse Strafwet is toepasselijk op ieder die zich buiten Nederland aan boord van een Nederlands vaartuig of luchtvaartuig aan enig strafbaar feit schuldig maakt.

Art. 4. De Nederlandse Strafwet is toepasselijk op ieder die zich buiten Nederland schuldig maakt:

1. Aan een der misdrijven omschreven in artikel 92-96, 97a, 98-98c, 105 en 108-110.

Art. 5. -1. De Nederlandse Strafwet is toepasselijk op de Nederlander die zich buiten Nederland schuldig maakt:

1. aan een der misdrijven omschreven in de Titels I en II van het Tweede boek, en in de artikelen 206, 237, 272, 273, 388 en 389.

2. aan een feit hetwelk door de Nederlandse strafwet als misdrijf wordt beschouwd en waarop door de wet van het land waar het begaan is, straf is gesteld.

-2. De vervolging kan ook plaatshebben, indien de verdachte eerst na het begaan van het feit Nederlander wordt.

Art. 23. -1 Hij die tot een geldboete is veroordeeld is verplicht tot betaling van het bij de rechterlijke uitspraak vastgestelde bedrag aan de staat binnen de termijn door het openbaar ministerie dat met de tenuitvoerlegging van het vonnis of arrest is belast, te stellen.

-2. Het bedrag van de geldboete is ten minste twee euro vijftig.

-3. De geldboete die voor een strafbaar feit ten hoogste kan worden opgelegd, is gelijk aan het bedrag van die categorie die voor dat feit is bepaald.

-4. Er zijn zes categorieën: de eerste categorie, € tweehonderdvijftientig;

de tweede categorie, € tweeduizendtweehonderdvijftig;

de derde categorie, € vierduizendvijfhonderd;

de vierde categorie, € elfduizendtweehonderdvijftig;

de vijfde categorie, € vijfenveertigduizend;

de zesde categorie, € vierhonderdvijftigduizend.

-5. Voor een overtreding, onderscheidenlijk een misdrijf, waarop geen geldboete is gesteld, kan de rechter een geldboete opleggen tot ten hoogste het bedrag van de eerste, onderscheidenlijk de derde categorie.

Art. 98. -1. Hij die een inlichting waarvan de geheimhouding door het belang van de staat of van zijn bondgenoten wordt geboden, een voorwerp waaraan een zodanige inlichting kan worden ontleend, of zodanig gegevens opzettelijk verstrekt aan of ter beschikking stelt van een tot kennisneming daarvan niet gerechtigd persoon of lichaam, wordt, indien hij weet of redelijkerwijs moet vermoeden dat het een zodanige inlichting, een zodanig voorwerp of zodanige gegevens betreft, gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.

-2. Met dezelfde straf wordt gestraft hij die een inlichting die van een verboden plaats afkomstig is en tot de veiligheid van de staat of van zijn bondgenoten in betrekking staat, een voorwerp waaraan een zodanige inlichting kan worden ontleend, of zodanige gegevens opzettelijk verstrekt aan of ter beschikking stelt van een tot kennisneming daarvan niet gerechtigd persoon of lichaam, indien hij weet of redelijkerwijs moet vermoeden dat het een zodanige inlichting, een zodanig voorwerp of zodanige gegevens betreft.

Art. 98a. -1 Hij die een inlichting, een voorwerp of gegevens als bedoeld in artikel 98, hetzij opzettelijk openbaar maakt, hetzij zonder daartoe gerechtigd te zijn opzettelijk aan of ter beschikking stelt van een buitenlandse mogendheid, een in het buitenland gevestigd persoon of lichaam, dan wel een zodanig persoon of lichaam dat gevaar ontstaat dat de inlichting of de gegevens aan een buitenlandse mogendheid of aan een in het buitenland gevestigd persoon of lichaam bekend wordt, indien hij weet of redelijkerwijs moet vermoeden dat

het een zodanige inlichting of zodanige gegevens betreft, wordt gestraft met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie.

-2. Indien de schuldige heeft gehandeld in tijd van oorlog dan wel in dienst of in opdracht van een buitenlandse mogendheid of van een in het buitenland gevestigd persoon of lichaam, kan levenslange gevangenisstraf of tijdelijke van ten hoogste twintig jaren of geldboete van de vijfde categorie worden opgelegd.

-3. Handelingen gepleegd ter voorbereiding van een misdrijf als omschreven in de voorgaande leden worden gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.

Art. 98b. Hij aan wiens schuld te wijten is dat een inlichting, een voorwerp of gegevens bedoeld in artikel 98, openbaar worden gemaakt of ter beschikking komt van een tot kennisneming daarvan niet gerechtigd persoon of lichaam, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

Art. 98c.-1. Met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie wordt gestraft:

1. hij die opzettelijk een inlichting, een voorwerp of gegevens als bedoeld in artikel 98, zonder daartoe gerechtigd te zijn, onder zich neemt of houdt;
2. hij die enige handeling verricht, ondernomen met het oogmerk om, zonder daartoe gerechtigd te zijn, de beschikking te krijgen over een inlichting, een voorwerp als bedoeld in artikel 98;
3. hij die tersluiks, onder een vals voorgeven, door middel van een vermomming of langs een andere dan de gewone toegang op of in een verboden plaats komt of tracht te komen, aldaar in dier voege aanwezig is, of zich op een van die wijzen of door een van die middelen vandaar verwijderd of tracht te verwijderen.

-2. De bepaling onder 3 is niet toepasselijk, indien de rechter blijkt dat de dader niet heeft gehandeld met het oogmerk bedoeld onder 2.

Art. 272.-1. Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

-2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

Art. 273.-1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die opzettelijk

1. aangaande een onderneming van handel, nijverheid of dienstverlening bij welke hij werkzaam is of is geweest, bijzonderheden waarvan hem geheimhouding is opgelegd, bekend maakt of
2. gegevens die door misdrijf zijn verkregen uit een geautomatiseerd werk van een onderneming van handel, nijverheid of dienstverlening en die betrekking hebben op deze onderneming, bekend maakt of uit winstbejag gebruikt, indien deze gegevens ten tijde van de bekendmaking of het gebruik niet algemeen bekend waren en daaruit enig nadeel kan ontstaan.

-2. Niet strafbaar is hij die te goeder trouw heeft kunnen aannemen dat het algemeen belang de bekendmaking vereiste.

-3. Geen vervolg heeft plaats dan op klacht van het bestuur van de onderneming.

Bijlage 13

**Toestemming tot plaatsing van een persoon die
niet beschikt over de Nederlandse nationaliteit op een *Vertrouwensfunctie***

Het is slechts na toestemming van de *MIVD* toegestaan om personen die niet beschikken over de Nederlandse nationaliteit te plaatsen op een *Vertrouwensfunctie*. Een verzoek hiertoe dient door de *Opdrachtnemer* bij *BIV / MIVD* te worden ingediend. Zie deze bijlage voor het aanmeldformulier.

Het verzoek dient te zijn voorzien van de reden waarom vervulling van de *Vertrouwensfunctie* dient te geschieden door een niet-Nederlander en van het bijzondere project en/of opdracht waarop betrokkene wordt ingezet.

BIV / MIVD beoordeelt in overleg met de *Opdrachtgever*/projectleider bij Defensie of het voornemen vanuit de veiligheidsoptiek mogelijk is en voorts niet strijdig is met verplichtingen die door of namens de Nederlandse overheid, dan wel de minister van Defensie zijn aangegaan, hetzij nationaal, bilateraal of bondgenootschappelijk. In voorkomend geval dient, door tussenkomst van *BIV / MIVD*, tevens toestemming te worden gevraagd aan een eventuele medebelanghebbende partij, bijvoorbeeld een derde land waarmee wordt samengewerkt in het onderhavige project.

De verkregen toestemming geldt uitsluitend voor inzet op het *Bijzondere Opdracht* en/of project dat in de aanvraag is vermeld. Indien betrokkene eveneens op andere projecten en/of opdrachten moet worden ingezet, dient hiervoor per project en/of opdracht toestemming te worden gevraagd. Na verkregen toestemming dient het *Veiligheidsonderzoek* te worden aangevraagd waarbij vaak *Informatie* noodzakelijk is uit het land van herkomst van betrokkene. Dit kan het *Veiligheidsonderzoek* bemoeilijken en in de regel ook vertragen. In sommige gevallen is het onderzoek zelfs onmogelijk en kan geen *VGB* worden verstrekt, waardoor betrokkene niet op een *Vertrouwensfunctie* kan worden geplaatst.

	Bijlage 13.1 PERSONEELSVERTROUWELIJK <i>(Indien ingevuld)</i> Verzoek toestemming tot plaatsing van een persoon die niet beschikt over de Nederlandse nationaliteit op een <i>Vertrouwensfunctie</i>	
--	--	--

Persoonsgegevens
1. Opdrachtnemer: _____ verzoekt toestemming om onderstaande persoon, die niet beschikt over de Nederlandse nationaliteit te plaatsen op een <i>Vertrouwensfunctie</i>.
2. Achternaam kandidaat: _____ Voornamen: _____ M / V
3. Huidig adres: _____ Woonplaats: _____ Land: _____
4. Geboortedatum: _____ Geboorteplaats: _____ Geboorteland: _____ BSN: _____
5. Nationaliteit(en): _____ Woonachtig in Nederland sinds: _____
6. Werkzaam bij: _____ Sinds wanneer: _____

Opdracht gegevens
1. Omschrijving van de opdracht waaraan de kandidaat tewerk moet worden gesteld: _____ _____ _____ _____
4. Opdrachtgever bij Defensie:

Algemene Beveiligingseisen Defensie Opdrachten 2017

5. Aard van de werkzaamheden:		
6. Motivatie voor tewerkstelling:		
Een duidelijk omschreven motivatie, waarin de noodzaak om betrokkene bij de werkzaamheden in te zetten wordt toegelicht.		
7. Rubricering van de opdracht:		
Buitenlandse Rubricering:		
8. "Eyes Only" merkingen?	ja	neen

Onderstaande niet in te vullen door de aanvrager!

Beslissing <i>Opdrachtgever</i>	akkoord	niet akkoord
Naam		
Datum		
Handtekening		

Beslissing <i>MIVD</i>	akkoord	niet akkoord
Correspondentie nummer		
Handtekening	Directeur Militaire Inlichtingen- en Veiligheidsdienst voor deze <i>Hoofd Bureau Industrieveiligheid</i>	

Algemene Beveiligingseisen Defensie Opdrachten 2017

Datum	
Opmerkingen	

	Bijlage 14 Wijziging persoonlijke omstandigheden	
--	--	--

Wijziging persoonlijke omstandigheden

Binnen de periode van vijf jaar kan er aanleiding zijn een nieuw *Veiligheidsonderzoek* uit te voeren, in het bijzonder door wijziging in persoonlijke omstandigheden⁷. Indien zulke wijzigingen zich voordoen is de betrokken medewerker verplicht zich te melden bij de *BF*. Deze informeert *BIV / MIVD*, gebruikmakend van het in deze bijlage toegevoegde mutatieformulier, waarna mogelijk een nieuw *Veiligheidsonderzoek* wordt opgestart. Denk bij wijzigingen aan:

- scheiding, een nieuwe relatie of partner;
- problematische financiële situatie;
- aanraking met justitie of politie;
- lidmaatschap van organisaties of verenigingen die mogelijk strijdig zijn met de belangen van Defensie;
- drugsgebruik;
- langdurig verblijf in het buitenland (zakelijk dan wel privé);
- functiewijziging;
- wijziging van het vereiste *VMN*.

⁷ Zie: Leidraad Persoonlijke gedragingen en omstandigheden
<https://www.defensie.nl/binaries/defensie/documenten/brochures/2015/02/05/leidraad-gedrag-bij-veiligheidsonderzoek/DEF+Leidraad+pers+gedragingen+WEB.pdf>.

Bijlage 14.1 PERSONEELSVERTROUWELIJK <i>(Indien ingevuld)</i> Mutatieformulier wijziging persoonlijke omstandigheden	
--	--

Onderwerp			
Bedrijf			
Hierbij deel ik u mee dat : _____ , _____ (achternaam) (voorletters) _____ , _____ (Geboortedatum) (BSN nummer) niet langer een <i>Vertrouwensfunctie</i> vervult. de in bijlage genoemde personen niet langer een <i>Vertrouwensfunctie</i> vervullen. het <i>Veiligheidsonderzoek</i> naar betrokken persoon kan worden stopgezet. sinds ____.-____.-____ is gehuwd* / verloofd* / samenwoont* met: <i>Naam, voornaam:</i> _____ <i>Geboortedatum, geboorteplaats:</i> _____ <i>Nationaliteit:</i> _____ Overige mededelingen : _____ _____ _____			
Beveiligings- functionaris			
Handtekening		Datum	

Niet invullen door aanvrager

In MIVD d.d. _____	Naar AIVD d.d. _____	Naar BVD d.d. _____
Gemuteerd d.d. _____	Gemuteerd d.d. _____	Gemuteerd d.d. : _____
Door : _____	Door _____	Door: _____

	Bijlage 15 Ontheffing uit een <i>Vertrouwensfunctie</i>	
--	---	--

De medewerker wordt uit de *Vertrouwensfunctie* ontheven en de VGB van rechtswege vervalt:

- bij onvoldoende waarborgen dat de betrokken medewerker de uit de *Vertrouwensfunctie* voortvloeiende plichten onder alle omstandigheden getrouwelijk zal vervullen;
- als de betrokken medewerker geen *Vertrouwensfunctie* meer vervult en herplaatsing ook binnen drie maanden niet wordt voorzien;
- wanneer de *Vertrouwensfunctionaris* het bedrijf verlaat. Als betrokkene een *Vertrouwensfunctie* bij een andere *Opdrachtnemer* aanvaardt, dient opnieuw een *Veiligheidsonderzoek* te worden uitgevoerd.

Indien de *Vertrouwensfunctionaris* de beveiligingsregels van de *Opdrachtnemer* bewust of onbewust negeert of overtreedt dient de *BF* van de *Opdrachtnemer* passende maatregelen te nemen en *BIV* / *MIVD* hierover te informeren. Grove nalatigheid of bewuste *Compromittatie* van *Staatsgeheime* of *Vitale Informatie* of *Materieel* kan aanleiding zijn tot strafrechtelijke vervolging.

Medewerkers van de *Opdrachtnemer* die om één van bovengenoemde redenen worden ontheven uit de *Vertrouwensfunctie* respectievelijk *Crypto-functie* dienen een ontheffingsverklaring te ondertekenen (**bijlage 15.1 en bijlage 15.2**). De *BF* stelt zeker dat een toelichting wordt gegeven op de ontheffingsverklaring, zo mogelijk de (kopie) *VGB* wordt ingenomen en dat de medewerker geen *TBB*, in het bijzonder *BI* respectievelijk *Crypto*, meer in bezit heeft.

	Bijlage 15.1 PERSONEELSVERTROUWELIJK <i>(Indien ingevuld)</i> Verklaring bij ontheffing uit een <i>Vertrouwensfunctie</i>	
--	--	--

Ontheffingsverklaring

Ondergetekende (Naam, voorletters)	
Geboren op	
BSN nummer	
Werkzaam bij bedrijf	
Ontheven van de functie van	
Verklaart dat hij / zij: - de gerubriceerde <i>Informatie</i> die in de uitoefening van zijn / haar functie tot zijn of haar kennis is gekomen, niet zal onthullen aan niet-gerechtigden; - beseft dat hij / zij na beëindiging van het dienstverband dan wel de arbeidsovereenkomst blijft onderworpen aan de wettelijke en andere voorschriften inzake de geheimhouding van <i>Informatie</i> en aan de in die voorschriften gestelde sancties op schending van de geheimhoudingsplicht; - geen gerubriceerde <i>Informatie</i> die hem / haar in zijn / haar functie ter beschikking zijn gesteld, meer onder zijn / haar berusting heeft.	
_____ Handtekening	_____ Plaats, datum

Bijlage 15.2 PERSONEELSVERTROUWELIJK <i>(Indien ingevuld)</i> Verklaring bij ontheffing uit een <i>Cryptofunctie</i>
--

Ontheffingsverklaring *Crypto* functie

Ondergetekende (Naam, voorletters)	
Geboren op	
BSN nummer	
Werzaam bij bedrijf	
Ontheven van de functie van	
Verklaart dat hij / zij: - dat de gerubriceerde en/of <i>CRYPTO</i>, <i>CRYPTO-SECURITY</i> of <i>CCI-gemerkte</i> Informatie, die in de uitoefening van zijn / haar functie tot zijn of haar kennis zijn gekomen, niet zal onthullen aan niet-gerechtigden; - beseft dat hij / zij na beëindiging van het dienstverband dan wel de arbeidsovereenkomst onderworpen blijft aan de wettelijke en andere voorschriften inzake de geheimhouding van <i>Informatie</i> en aan de in die voorschriften gestelde sancties op schending van de geheimhoudingsplicht; - geen gerubriceerde en/of <i>CRYPTO</i>, <i>CRYPTO-SECURITY</i> of <i>CCI-gemerkte</i> documenten of materieel die hem / haar in zijn / haar functie ter beschikking zijn gesteld, meer onder zijn / haar berusting heeft.	
_____ Handtekening	_____ Plaats, datum

Bijlage 16

Reizen naar het buitenland

Reizen naar het buitenland

Zakelijke reis

Een zakelijke reis naar het buitenland die in het kader van een *BO* wordt ondernomen dient voorafgaand te worden gemeld bij de *BF*. Via de *BF* dient een zogenoemd (elektronisch) *Request for Visit* (*e-RfV*, het formulier is op te vragen via uw Accountmanager bij *BIV / MIVD*) te worden ingediend bij *BIV / MIVD* (Sectie *RfV*). Een *RfV* is doorgaans eveneens noodzakelijk indien in het buitenland een militaire locatie moet worden betreden. Alvorens de *e-RfV* door te sturen dient de *BF* deze te controleren op volledigheid, juistheid en tijdigheid. Een *e-RfV* dient tijdig te worden ingediend vanwege de lange doorlooptijd die dit proces kent.

Reizen naar landen met een veiligheidsrisico

Als gevolg van mondiale politieke ontwikkelingen zijn de veiligheidsrisico's die verbonden zijn aan reizen naar bepaalde landen aan veranderingen onderhevig. Defensie heeft criteria opgesteld m.b.t. het reizen naar het buitenland. Een veiligheidsrisico kan bijvoorbeeld gebaseerd zijn op spionagedreiging of betrokkenheid in een gewapend conflict. Defensie geeft aan voor welke landen een verhoogd of beperkt veiligheidsrisico van toepassing is en stelt criteria op voor het reizen naar deze landen. Voor verdere informatie hierover kan contact opgenomen worden met *BIV / MIVD*. Voor *Vertrouwensfunctionarissen* bij defensieorderbedrijven geldt, zowel in persoonlijk belang als in bedrijfsbelang, een meldingsplicht aan de BF m.b.t. voorgenomen reizen naar deze landen. De BF meldt aan BIV / MIVD zakelijk reizen en/of privéverblijf van een Vertrouwensfunctionaris naar of resp. in een risicoland door middel van het formulier in **bijlage 16.1**.

Zonodig vindt voorafgaand aan de reis een veiligheidsbriefing door de *BF* plaats, toegespitst op het land van bestemming. Na terugkeer vindt debriefing plaats. In de briefing wordt ingegaan op het meenemen van IT-middelen en op de handelwijze van mogelijke actoren die het gemunt hebben op relevante *Informatie*. Ook persoonlijke gedragingen (do's and don'ts) in het land van bestemming kunnen onderwerp van de briefing en debriefing zijn.

Privéreizen naar het buitenland

Vertrouwensfunctionarissen dienen ook privéreizen naar landen met een veiligheidsrisico te melden aan de *BF*. Hiervoor kunnen briefing en debriefing wenselijk of noodzakelijk zijn. Het Ministerie van Buitenlandse Zaken (BZ) geeft op internet: www.rijksoverheid.nl/onderwerp/reisadviezen, adviezen uit voor reizen naar het buitenland, onder andere over landen waarnaar het reizen sterk wordt afgeraden in verband met risico's voor de persoonlijke veiligheid. Personeel wordt aangeraden bij reizen of verblijf in het buitenland een negatief reisadvies van BZ op te volgen.

Langdurig verblijf in het buitenland

Zakelijk of privéverblijf in het buitenland langer dan drie aaneengesloten maanden kan gevolgen hebben voor de *VGB*. Dit betreft zowel de betrokken medewerker als diens partner. Indien in het land van verblijf onvoldoende mogelijkheden zijn tot het doen van naslag omtrent het verblijf aldaar wordt de *VGB* in beginsel ingetrokken.

Bijlage 16.1 Formulier melding bezoek risicoland ABDO	
---	--

Melding bezoek risicoland ABDO

Voor het melden van een aanstaande reis van een medewerker geplaatst op een *Vertrouwensfunctie* dienen de volgende gegevens te worden aangeleverd.

Bedrijfsgegevens:

Naam bedrijf:

--

Naam BF/melder:

--

Reisgegevens:

Datum aanvang reis:

--

Datum einde reis:

--

Land van bestemming:

--

Plaats van bestemming:

--

Naam bedrijf/organisatie bestemming:

--

Reden van bezoek/onderwerp:

--

Prive/zakelijke reis:

--

Reiziger gegevens:

Achternaam reiziger:

--

Tussenvoegsels:

--

Voornamen reiziger:

--

BSN:

--

Functie reiziger:

--

Expertiseveld reiziger:

--

	Bijlage 17 Beveiligingsmaatregelen en schillenstructuur	
--	--	--

Beveiligingsmaatregelen en schillenstructuur

Om te voorkomen dat een niet-geautoriseerd persoon, met name een kwaadwillend persoon, toegang krijgt tot een compartiment worden beveiligingsmaatregelen genomen. Fysieke beveiligingsmaatregelen zijn bijvoorbeeld een dikke stalen deur en braakwerend glas. Optimale beveiliging maakt gebruik van meerdere maatregelen die elkaar qua reikwijdte overlappen en die meerdere barrières vormen. Deze barrières kunnen als schillen worden voorgesteld om het *TBB* heen. Zo vormen bijvoorbeeld een kluis, het compartiment, het gebouw en het hekwerk vier verschillende beveiligingsschillen. Voor de schillenstructuur geldt dat als het niet mogelijk is om een voorgeschreven maatregel uit de *ABDO* 2017 eisen in een bepaalde schil uit te voeren, de eerstvolgende schil sterker moet worden gemaakt.

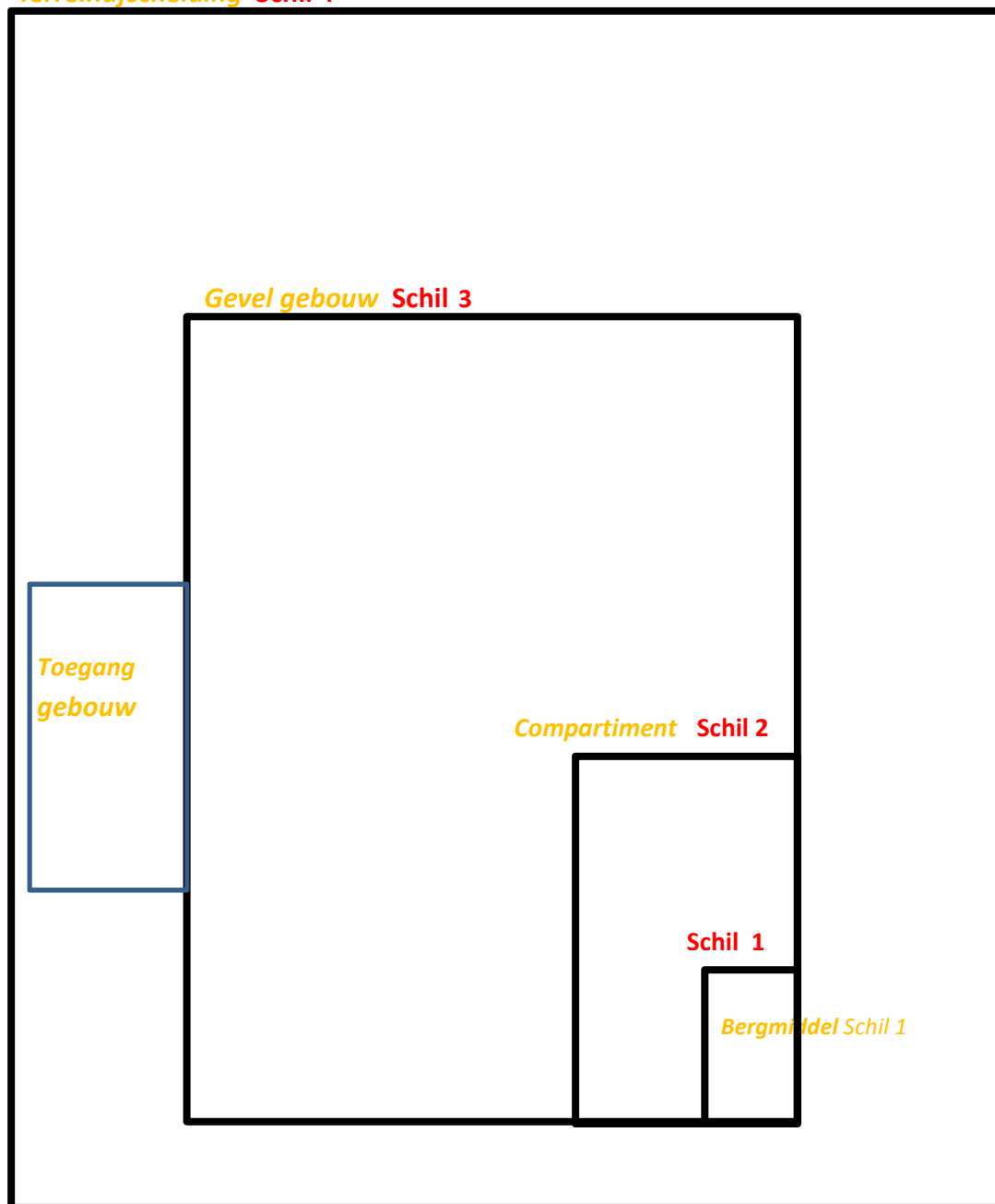
In de *ABDO* 2017 eisen zijn de minimaal vereiste beveiligingsmaatregelen opgenomen.

Voorbeelden van schillenstructuren per *TBB* categorie (bijlage 17.2 tm 17.5) zijn gerubriceerd en daarom alleen op te vragen bij uw accountmanager van BIV / MIVD.

Bijlage 17.1

Algemene situatie beveiligingsmaatregelen en schillenstructuur

Terreinafscheiding Schil 4



	Bijlage 18 Organisatorische maatregelen	
--	---	--

Toegangscontrole

Toegangscontrole, wordt tegenwoordig vaak aangeduid met de Engelse term “Access control”. Het is het alomvattend begrip voor *Identificatie*, *Authenticatie*, *Autorisatie*, goedkeuring dan wel weigering van toegang en alle vormen van registratie daarbij. Toegangscontrole is de functionaliteit die op basis van *Autorisatie* daadwerkelijk toegang tot een beoogd compartiment verleent dan wel weigert aan de persoon die daarom verzoekt. Een adequaat toegangscontrolesysteem, als onderdeel van de integrale beveiliging, garandeert dat alleen geautoriseerde personen toegang krijgen tot een compartiment van een *TBB*. Door middel van *Authenticatie* wordt gecontroleerd of de persoon die verzoekt om toegang tot een compartiment daartoe is geautoriseerd. *Authenticatie* vindt plaats door mensen (bewakers) of door een geautomatiseerd systeem en geschiedt op basis van ID-bewijzen, wachtwoorden, tokens, biometrische gegevens, elektronische sleutels, fysieke sleutels en dergelijke. Het verlies van authenticatiemiddelen zoals een (elektronische) sleutel is een beveiligingsincident.

Autorisatie

De *Autorisaties* worden toegekend aan personen op basis van “Need-to-be” en “Need-to-Know”. Deze geven aan tot welke *TBB* die personen gerechtigd zijn zich toegang te verschaffen. *Autorisaties* worden door toedoen van de *Beveiligingsfunctionaris (BF)* in het toegangscontrolesysteem ingesteld. Er is onderscheid tussen geautoriseerde en niet-geautoriseerde personen. Of een persoon geautoriseerd kan worden hangt af van een aantal voorwaarden die zijn opgenomen in Hoofdstuk 2. Voor het juist en adequaat beheer van de *Autorisaties* dienen procedures en instructies te worden opgesteld. Elke onduidelijkheid over wie wel of niet geautoriseerd is, dient te worden vermeden.

De toegang van niet-geautoriseerde personen tot een *TBB* dient tot een minimum te worden beperkt. Het is daarom wenselijk dat taken zoals bedrijfshulpverleners (BHV) zoveel mogelijk als neventaak worden uitgevoerd door geautoriseerde personen. Bij niet-geautoriseerde personen kan worden gedacht aan schoonmakers, facilitair medewerkers, onderhoudsmonteurs, leveranciers of extern betrokkenen bij een *Bijzondere Opdracht*. Indien een niet-geautoriseerde persoon vanwege werkzaamheden toch toegang moet krijgen tot een compartiment, wordt deze persoon in alle gevallen door geautoriseerd personeel begeleid en is de niet geautoriseerde persoon binnen het compartiment herkenbaar door middel van een zichtbaar gedragen pas met daarop duidelijk vermeld “BEZOEKER”. Zij dienen te allen tijde te worden begeleid door geautoriseerd personeel dat verantwoordelijk is voor het afschermen van het *TBB*. Daarnaast zijn bezoekers die niet beschikken over de Nederlandse nationaliteit vijf werkdagen voor het bezoek aangemeld bij *BIV / MIVD*. Dit aanmeldformulier is in deze bijlage toegevoegd.

Alleen elektronische apparatuur die essentieel is voor het uitvoeren van de opdracht is toegestaan binnen de ruimten van het *TBB*. Een lijst van deze apparatuur is opgenomen in het beveiligingsplan.

Vanaf *TBB 3* is bij het verlaten van een compartiment met een *TBB* is een sluitronde gemaakt, waarbij de deur van het opbergmiddel, het compartiment en zo mogelijk het gebouw is afgesloten. Ramen en deuren zijn afgesloten en het *Indringer Detectie- en Signaleringssysteem (IDSS)* is geactiveerd. Tevens is een controle op insluiping en de verzegeling van nooddeuren uitgevoerd. Bij afwezigheid van *Geautoriseerd* personeel blijft positief bewakingsrendement gewaarborgd.

Logging

Daar waar technische systemen beschikken over loggings zal deze functionaliteit gebruikt moeten worden. Hoelang de *Loggings* moeten worden bewaard, hangt af van de categorie van het *TBB*, waarvoor het systeem wordt ingezet en geldende wettelijke beperkingen. In de eisen Fysiek staan de minimale *Logging*seisen en bewaartermijnen. Bij een beveiligingsincident worden terstond de *Loggings* veilig gesteld en geldt een langere bewaartermijn, minimaal tot het moment dat het onderzoek naar het beveiligingsincident volledig is afgesloten. Meer informatie hierover is te vinden in **bijlage 9**.

Bijlage 18.1 PERSONEELSVERTROUWELIJK <i>(Indien ingevuld)</i> Bezoeker Autorisatie formulier	
--	--

In te vullen door ABDO bedrijf / to be completed by ABDO company

Bedrijfsnaam / Company name	
Beveiligingsfunctionaris / Security officer	
Te bezoeken locatie/ Location to be visit	

In te vullen door ABDO bedrijf of bezoeker / to be completed by ABDO company or visitor

Achternaam / Surname	
Voornamen (volledig) / First names (in full)	
Geboortedatum / Date of birth	
Geboorteplaats / Place of birth	
Nationaliteit / Nationality	
Paspoortnummer / Passportnumber	
Bij deze aanvraag dient een kopie paspoort te worden toegevoegd / For this application a copy of an identification card is required.	
Bedrijfsnaam / Company name	
Functie / Position	
Contactpersoon / Point of contact	
Datum of periode bezoek / Date or period of visit	
Doel bezoek / Purpose of visit	

Naam BF	BIV / MIVD
Handtekening	Handtekening
Datum	Datum

	Bijlage 19 Bouwkundige maatregelen	
--	--	--

Bouwkundige beveiligingsmaatregelen vormen de ruggengraat van de OBER-maatregelenmix. Het is derhalve van belang om de adequate bouwkundige maatregelen op het juiste beveiligingsniveau tijdig mee te nemen in nieuwbouwplannen of wijzigingen zodat implementatie tegen acceptabele kosten kan plaatsvinden. Voorbeelden van bouwkundige maatregelen zijn:

- stevige betonnen muren;
- versterkte deuren;
- braakwerend glas;
- versterkt hang- en sluitwerk;
- hekwerken en andere terreinaanpassingen.

Bouwkundige maatregelen vormen een barrière tegen onbevoegde personen die proberen toegang te krijgen tot een *TBB*. Denk daarbij aan inbraak, met als doel veelal diefstal, spionage of sabotage, maar ook aan abusievelijke toegang van ongeautoriseerde medewerkers. De effectiviteit van deze maatregelen is sterk afhankelijk van het gereedschap dat de indringer tot zijn beschikking heeft. Dit kan gezien worden als een zogenoemde daderprofiel. Meer informatie hierover kunt u vinden in **bijlage 25**. Deze bijlage is gerubriceerd en op te vragen bij uw accountmanager.

Uitsteltijd

De *Uitsteltijd* als gevolg van bouwkundige maatregelen is de tijd die een indringer nodig heeft vanaf het moment van detectie tot het moment dat de bouwkundige beveiliging van het *TBB* is doorbroken. De tijd die benodigd is voor het doorbreken van de verschillende barrières (bouwkundige schillen) start vanaf de detectie tot aan het bereiken van het *TBB*. Wanneer de *Interventietijd* korter is dan de *Uitsteltijd* is sprake van een positief bewakingsrendement.

Compartimentering

Gelijkwaardige *TBB* van één opdracht zullen zo veel mogelijk gezamenlijk in één compartiment verwerkt en opgeborgen zijn. Dit principe heet *Compartimentering*. Bouwkundige beveiligingsmaatregelen zijn het meest effectief als compartimenten waarin *TBB* worden verwerkt en opgeslagen zowel in aantal als in grootte kunnen worden beperkt.

Bouwkundige schillen

Rondom het *TBB*, 3-dimensionaal, dienen vloeren, muren en wanden, plafonds en openingen daarin ten behoeve van toegang, luchtverversing enzovoorts te voldoen aan de beveiligingseisen. Eén zwakke schakel kan zorgen dat de gehele beveiliging onvoldoende is, derhalve wordt vaak een schillenstructuur toegepast. Dit houdt in dat om het *TBB* het opbergmiddel een schil vormt, vervolgens het compartiment waarin het opbergmiddel staat, het gebouw waarin de compartiment zich bevindt en het afgescheiden terrein waarop het gebouw zich bevindt. Van buiten naar binnen is sprake van oplopende zwaarte van maatregelen.

De hoogst aanwezige *TBB*-categorie bepaalt de zwaarte van de te nemen maatregelen. Daarbij wordt opgemerkt dat aanwezigheid van veel *TBB* van een lage categorie kan leiden tot beveiliging op een hoger niveau.

Niet alleen de sterkte van de vloeren, wanden, plafonds enzovoorts bepaalt of een compartiment afdoende is beveiligd, ook de ligging heeft grote invloed. Een kluiskamer op de 5e verdieping van een flatgebouw van 10 verdiepingen is eenvoudiger te beveiligen dan een kamer op de begane grond die direct aan een drukke weg

Algemene Beveiligingseisen Defensie Opdrachten 2017

grenst. Bij het toewijzen van functionaliteiten aan compartimenten dient hiermee rekening te worden gehouden.

Bouwkundige schillen dienen zo veel mogelijk te overlappen teneinde de noodzakelijke vertraging te creëren die tijdige interventie mogelijk maakt. De volgende beveiligingsschillen worden onderkend:

- het opbergmiddel waarin het *TBB* is opgeslagen;
- een compartiment of deel van het gebouw waarin het *TBB* is opgeslagen/gelegen;
- de gevel van het gebouw waarin het compartiment zich bevindt;
- de terreinafscheiding rondom het gebouw waarin het compartiment zich bevindt.

Bij elke beveiligingsschil dient te worden bepaald of en welke organisatorische, bouwkundige, elektronische en reactieve maatregelen moeten worden genomen.

Indien een beveiligingsschil volgens de *ABDO* 2017 wordt vereist, maar niet kan worden gerealiseerd, dienen de daarop volgende beveiligingsschillen te worden versterkt met aanvullende beveiligingsmaatregelen. Een voorbeeld is dat het niet altijd mogelijk is een hekwerk te plaatsen. In dat geval wordt de daarop volgende beveiligingsschil, zijnde de gevel of het compartiment, zwaarder beveiligd.

Terrein

De eerste beveiligingsschil van bouwkundige maatregelen wordt veelal gevormd door het terrein. Een overzichtelijke plaatsing van het gebouw met zicht op wegen en fietspaden draagt bij aan het vergroten van de beveiliging. Cultuurtechnische infrastructuur zoals begroeiing, waterpartijen en sloten kunnen het indringers moeilijker maken. Aan de andere kant kunnen geplaatste (vuil)containers, ladders, fietsen- en rookhokken het inbrekers juist makkelijker maken.

Parkeervoorzieningen

Het verdient de voorkeur om parkeerplekken niet tegen het gebouw te plaatsen. Verdragende maatregelen kunnen zijn (betonnen) bloembakken, paaltjes e.d. Een afgesloten parkeerterrein zodat toezicht gehouden kan worden op het gebruik van het parkeerterrein is aan te bevelen.

Visueel en akoestisch beperkende maatregelen

Naast compartimentering zijn visuele (inkijkbeperkende) en akoestische (geluidsbeperkende) beveiligingsmaatregelen noodzakelijk. Dergelijke beveiligingsmaatregelen worden getroffen in vergaderzalen, briefingrooms en werkruimten waarin een *TBB*, wordt besproken of behandeld.

Inkijkbeperkende beveiligingsmaatregelen moeten voorkomen dat niet-gerechtigden, al dan niet met gebruik van optische hulpmiddelen, door waarnemen van buiten de werkruimte kennis kunnen nemen van een *TBB*. Deze maatregelen zijn noodzakelijk ongeacht de *Rubricering* en/of *Merking*.

Geluidsbeperkende beveiligingsmaatregelen moeten voorkomen dat niet-gerechtigden, al dan niet met gebruik van auditieve hulpmiddelen, door waarnemen (afluisteren) van buiten de werkruimte kennis kunnen nemen van een *TBB*. Deze maatregelen zijn noodzakelijk ongeacht de *Rubricering* en/of *Merking*.

Algemene Beveiligingseisen Defensie Opdrachten 2017

De geluidsbeperkende beveiligingsmaatregelen zijn zodanig dat het gesprokene niet buiten het compartiment doordringt:

- normale spraak niet hoorbaar is;
- harde stem nauwelijks hoorbaar of verstaanbaar is.

Daarnaast dient te worden voorkomen dat *Informatie*, die elektronisch wordt verwerkt of opgeslagen met behulp van speciale apparatuur wordt “afgeluisterd”. Het is derhalve niet toegestaan om dergelijke apparatuur (GSM, PDA, tablet enz.) mee te nemen in compartimenten waar *Bijzondere Informatie* wordt besproken. Deze compartimenten dienen te worden afgesloten wanneer niemand aanwezig is en zo vaak als nodig in overleg met *BIV / MIVD* op mogelijk aanwezige af luisterapparatuur te worden gecontroleerd.

Zie op de volgende pagina een overzicht aangaande normen op het gebied van braakwering.

Bijlage 19.1 Overzicht normen braakwering	
---	--

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-1887	Opklimbeveiliging
NEN 8131	Alarmsystemen - Inbraak- en overvalalarmsystemen. - Systeem- en kwaliteitseisen en toepassingsrichtlijnen, gebaseerd op de Europese normen voor inbraak- en overvalalarmsystemen
NEN-EN 50130	Alarmsystemen
NEN-EN 50136	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur
NEN-EN 50518	Monitoring en alarm ontvangstcentrales inclusief alle relevante onderliggende delen.

Zie op de volgende pagina een normentabel aangaande inbraakwerende maatregelen.

Bijlage 19.2 Normentabel inbraakwerende maatregelen	
---	--

	TBB 1 ZG	TBB 2 G	TBB 3 C	TBB 4 DV
Organisatorische maatregelen	Beveiligingbeleid	Beveiligingbeleid	Beveiligingsplan	Beveiligingsplan
	Beveiligingsplan	Beveiligingsplan		
	PSI	PSI		
Bouwkundige maatregelen	Maatwerk	Hang en sluitwerk NEN5096, Weerstandsklasse 4	Hang en sluitwerk NEN5096, Weerstandsklasse 3	Hang en sluitwerk Afsluitbaar
	Maatwerk	Inbraakwerendheid 10 min. NEN-EN 1627, Weerstandsklasse 4	Inbraakwerendheid 5 min. NEN 5096, Weerstandsklasse 3	Inbraakwerendheid 3 min. NEN 5096, Weerstandsklasse 2
Electronische maatregelen	Maatwerk	Inbraakalarminstallatie conform NEN 8131; Grade 4	Inbraakalarminstallatie conform NEN 8131; Grade 3	Inbraakalarminstallatie conform NEN 8131; Grade 2
	Maatwerk	Alarmtransmissie volgens NEN 50136-1 naar PAC	Alarmtransmissie volgens NEN 50136-1 naar PAC	Alarmtransmissie volgens NEN 50136-1 naar PAC
Bergmiddelen				
bij reactietijd <15 min	Maatwerk	NEN 1143; Grade 4	NEN 1143; Grade 2	Afsluitbaar opbergmiddel
bij reactietijd 15-60 min	N.v.t.	NEN 1143; Grade 5	NEN 1143; Grade 4	Afsluitbaar opbergmiddel
bij reactietijd 60-240 min	N.v.t.	N.v.t.	NEN 1143; Grade 5	
Reactieve maatregelen (alarmopvolging)	Directe interventie	Door PAC naar particuliere bewakingsdienst, aangevuld met Politie (prioriteit 1)	Door PAC naar particuliere bewakingsdienst, aangevuld met Politie (prioriteit 1)	Door PAC naar particuliere bewakingsdienst.
	Alarmtransmissie volgens NEN 8131; DP4(AL3)	Alarmtransmissie volgens NEN 8131; DP4(AL3)	Alarmtransmissie volgens NEN 8131; DP3(AL2)	Alarmtransmissie volgens NEN 8131; SP2(AL1)

	Bijlage 20	
	Elektronische maatregelen	

Elektronische beveiligingsmaatregelen worden gebruikt om een compartiment, een opbergmiddel of een beperkt toegankelijk gebied te *Beveiligen*, daar toegang toe te verlenen of voor het verifiëren van een alarmering. Onder elektronische beveiligingsmaatregelen vallen alle materiële voorzieningen op elektronisch, elektrotechnisch of optisch gebied die een observerende, sturende, signalerende of alarmerende functie hebben. Bijvoorbeeld: *Camerasystemen (CCTV)*, diverse soorten detectoren, toegangbeheersystemen, alarmcentrales, etc. Beveiligingspersoneel heeft de beschikking over anti-overvalmaatregelen waaronder alarmeringsmiddelen.

Elektronische systemen worden onderscheiden naar functionaliteit in drie soorten:

- een *Indringer Detectie en Signaleringsystemen (IDSS)*;
- een *Elektronische Toegangsbeheersystemen (ETS)*;
- een *Camerasystemen (CCTV)*.

In een security managementsysteem of 'alarminstallatie' kunnen deze drie functionaliteiten worden gecombineerd.

IDSS

Het *IDSS*, wordt ingezet ter ondersteuning van de *Beveiliging* van een *TBB*. Het doel van een *IDSS* is het vroegtijdig detecteren en signaleren (alarmeren) van een (poging tot) ongeautoriseerde toegang tot een compartiment met het *TBB*. Een alarmering via een *IDSS* dient te allen tijde tot een alarmopvolging te leiden binnen de gestelde *Interventietijd*. Bij *TBB 3* en hoger is de aanwezigheid van een vorm van *IDSS* verplicht.

Het *IDSS* is aan een security management systeem (of equivalent) van een particuliere alarmcentrale (PAC) gekoppeld, zodat als gevolg van *IDSS*-alarmeringen interventie plaatsvindt.

ETS

Het *ETS* wordt vanaf *TBB 3* of hoger toegepast, eventueel in combinatie met een handmatige toegangscontrole. Het *ETS* is een hulpmiddel om ervoor te zorgen dat alleen geautoriseerde personen toegang hebben tot een compartiment, een opbergmiddel of een beperkt toegankelijk gebied. Het *ETS* verschaft tevens informatie waarmee onderzoek naar beveiligingsincidenten gedaan kan worden (bijvoorbeeld logging).

CCTV

Camerasbewaking speelt een rol in de preventie en in het verwerken van incidenten. Camera's kunnen een afschrikwekkende werking hebben en kunnen een middel zijn om een alarmmelding te genereren en verifiëren. Camera's zijn net als overige registratieapparatuur niet toegestaan in compartimenten waar met *Bijzondere Informatie* wordt gewerkt. Wel is het mogelijk een *Camerasysteem* ter beveiliging van toegang tot dergelijke compartimenten te gebruiken.

	Bijlage 21 Reactieve maatregelen	
--	--	--

Reactieve maatregelen

Voor de beveiliging van *TBB* is de reactie op (vermeende) beveiligingsincidenten van grote waarde. Zo snel mogelijk moet na een incident de normale, beveiligde situatie hersteld worden. De stappen die ondernomen moeten worden zijn afhankelijk van bepaalde factoren. Als het bijvoorbeeld gaat om de opvolging van een *IDSS*-alarm is het zaak dat het alarm zo snel mogelijk wordt geverifieerd. De politie komt namelijk pas in actie indien er sprake is van een gevalideerd alarm. Na de interventie kan worden teruggegaan naar de normale situatie als door de *BF* is vastgesteld dat het *TBB* niet is *Gecompromitteerd* en de beveiligingsmaatregelen nog afdoende functioneren.

De taak van de *BF* in het proces van alarmopvolging kan door middel van een consignatierooster ook door een andere geautoriseerde persoon worden waargenomen. Veelal worden hier personeelsleden voor geselecteerd die op korte reisafstand wonen.

Het is van belang om voor alle *TBB* een goede tijdpadanalyse te maken om zo vast te stellen wat het bewakingsrendement is. Voor een *TBB 1* en een *TBB 2* is de norm dat er sprake moet zijn van positief bewakingsrendement. Dat betekent dat te allen tijde interventie plaatsvindt voordat de dader het *TBB* heeft kunnen compromitteren. De optelsom van de *Uitsteltijd* die door de OBER-beveiligingsschillen wordt opgebouwd moet dus worden vergeleken met de tijd die het een dader kost om het *TBB* te compromitteren. Een *TBB 3* en een *TBB 4* vereist geen positief bewakingrendement, echter interventie dient binnen twee uur voor een *TBB 3* plaats te vinden.

Proces alarmopvolging

In het processchema bijgevoegd in de bijlage 21.1 zijn de stappen benoemd die bij alarmopvolging doorlopen moeten worden als zich een beveiligingsincident voordoet zoals ongeautoriseerde toegang, inbraak en insluiping. Er wordt onderscheid gemaakt tussen de periode dat er personeel aanwezig is in het compartiment met het *TBB* en de periode dat het compartiment is afgesloten (en dus “op alarm” staat). Deze periodes komen veelal overeen met de reguliere werktijd, hoewel de situatie dat het compartiment niet op alle werkdagen bezet is, niet ongewoon is.

Van personeel dat aanwezig is in een compartiment op het moment dat een verstoring van de beveiligde situatie plaatsvindt (bijvoorbeeld: er loopt een vreemd persoon het compartiment binnen en die probeert het opbergmiddel te openen) wordt verwacht dat het adequaat reageert. Hierbij staat de eigen veiligheid voorop, in ieder geval zal het incident zo snel mogelijk bij de *BF* gemeld moeten worden en indien van toepassing bij een aangesloten Particuliere Alarmcentrale (PAC). Een Particuliere Alarm Centrale beschikt over een justitiële erkenning en voldoet aan de NEN-EN 50518 norm.

In elk geval is het van groot belang dat de indringer (dader) zo vroeg mogelijk wordt gedetecteerd zodat de alarmopvolging zo snel mogelijk wordt geactiveerd.

Alarmverificatie

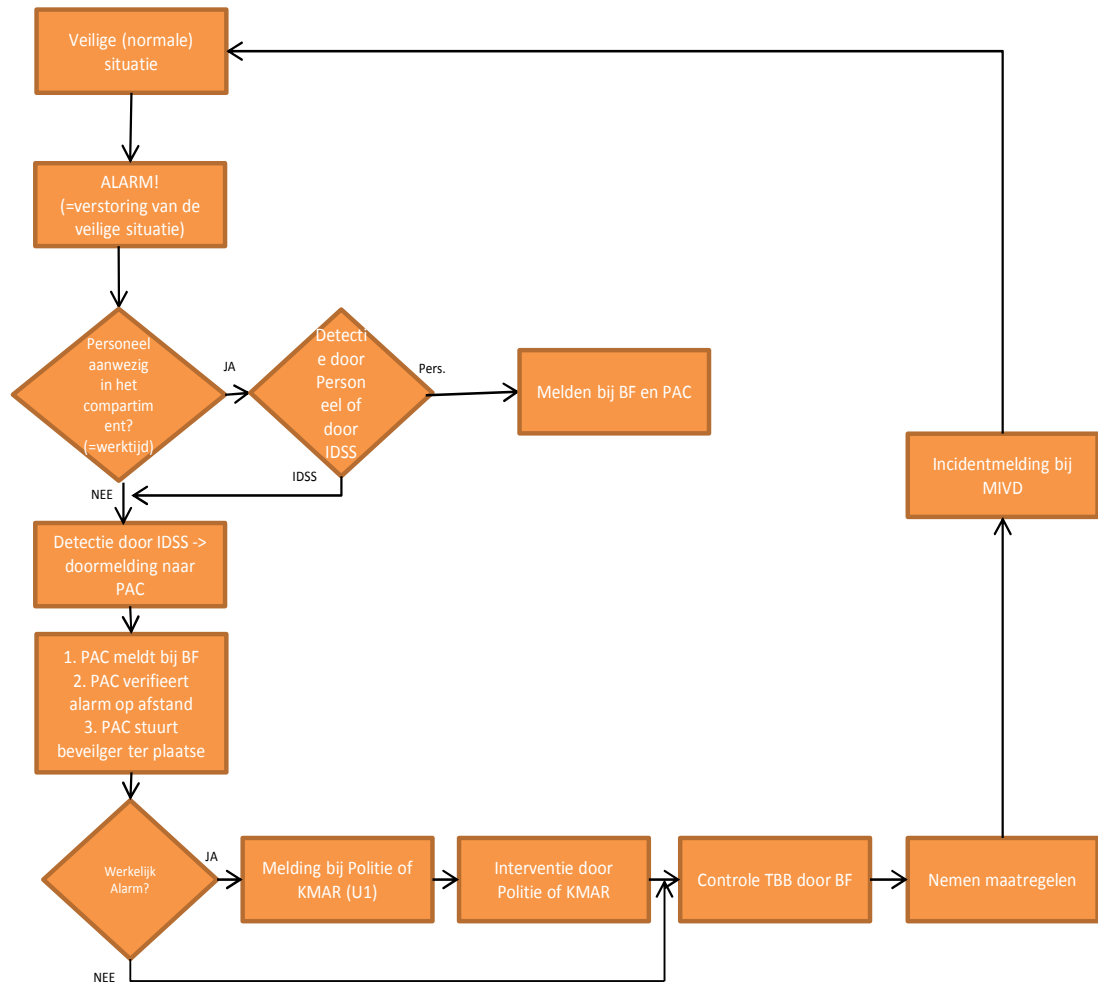
De alarmverificatie kan op een aantal manieren plaatsvinden:

- inluisteren via technische middelen die gekoppeld zijn aan het *IDSS*;
- meekijken via technische middelen die gekoppeld zijn aan het *IDSS*;
- beveiligingspersoneel dat op locatie inspecteert op sporen van braak;
- een combinatie van het bovenstaande.

De alarmverificatie kan ook plaatsvinden door eigen geautoriseerd personeel dat consignatiediensten uitvoert en dicht bij het bedrijf woont. Deze personen moeten wel gegarandeerd beschikbaar zijn en goede instructies hebben meegekregen. Gelet op de eigen veiligheid van dit personeel heeft alarmverificatie door een professioneel beveiligingsbedrijf de voorkeur. Technische alarmverificatie (inluisteren/meekijken) binnen het compartiment waarin zich een *TBB* bevindt, is niet toegestaan. Technische alarmverificatie in de omliggende ruimten daarentegen is wel toegestaan en zelfs gewenst. Directe doorschakeling van een PAC naar een politiemeldkamer middels bijvoorbeeld “Live View” is voor deze ruimten eveneens gewenst. Voor personeel dat belast is met de alarmopvolging is het van belang dat zij niet in het bezit zijn van de code en sleutelcombinatie van de opbergmiddelen van een *TBB*. Ook dienen zij geen toegang te hebben tot het compartiment. Dit om te voorkomen dat men onder dwang toegang moet verlenen aan een mogelijke indringer.

Bijlage 21.1

Proces alarmopvolging



	Bijlage 22 Transport en verzenden van een fysieke <i>TBB</i>	
--	--	--

Naast de beveiligingsmaatregelen ter bescherming van een *TBB* binnen het compartiment is het noodzakelijk dat het *TBB* ook adequaat wordt beveiligd tijdens fysiek transport en verzending, waarbij het transporteren dan wel verzenden van een *TBB* tot een minimum moet worden beperkt.

Tijdens transport of verzending is een *TBB* kwetsbaarder dan wanneer het zich op een beveiligde locatie bevindt. Men kan immers niet terugvallen op de OBER-maatregelen die het *TBB* beschermen in de normale situatie binnen het compartiment. De verhoogde kwetsbaarheid houdt een verhoogde kans op verlies of diefstal van het *TBB* in. Bij internationaal transport en verzending neemt de kwetsbaarheid nog verder toe.

Tijdens het transport en verzending dient het *TBB* dusdanig verpakt te zijn dat *Compromittatie* in voorkomend geval kan worden vastgesteld. Daarnaast dienen zoveel mogelijk maatregelen te worden genomen ter voorkoming van verlies of diefstal. Een afsluitbaar transportmiddel is dan ook essentieel. Indien zich onverhoopt toch een beveiligingsincident voordoet, dient de *BF* en daarna *BIV / MIVD* onmiddellijk te worden geïnformeerd en wordt onderzoek naar het incident conform het “Incident Handling” proces opgestart.

Transport

Onder transport van een *TBB* wordt verstaan het fysiek en gecontroleerd vervoeren daarvan, met inbegrip van informatiedragers (zoals USB-sticks). *TBB*-transporten dienen vooraf te worden gemeld bij de *BF* en indien het *Staatsgeheimen* betreft ook bij *BIV / MIVD*. De *BF* stelt voorschriften op voor het transporteren en houdt hier toezicht op. Transporten kunnen plaatsvinden met eigen transportmiddelen en geautoriseerd personeel of met inschakeling van een door *BIV / MIVD* goedgekeurd transport- of koeriersbedrijf dat als *Subcontractor* moet worden aangemeld bij *BIV / MIVD*. Transport van een *TBB* 1 geschiedt altijd door tussenkomst van *BIV / MIVD*.

Indien internationaal transport van een *TBB* niet mogelijk is met eigen transportmiddelen en geautoriseerd personeel of met inschakeling van een door *BIV / MIVD* goedgekeurd transport- of koeriersbedrijf, kan gebruik worden gemaakt van de zogenaamde “*Government-to-Government*”-procedure. Dit houdt in dat de te verzenden *TBB* aan *BIV / MIVD* wordt aangeboden ter doorgeleiding naar de betrokken buitenlandse overheidsinstantie die in voorkomend geval op zijn beurt voor aflevering bij de geadresseerde kan zorgdragen. Internationaal transport van een *TBB* vindt altijd pas na goedkeuring van het transportplan door *BIV / MIVD* plaats.

Naast de eisen en maatregelen voor *Beveiliging* van *TBB*-transport in de *ABDO 2017* kunnen specifieke bi- of multi-laterale afspraken zijn gemaakt voor internationaal transport van een (buitenlands) *TBB*. Deze afspraken zijn doorgaans vastgelegd in een *PSI*. Over het transport van een buitenlands *TBB* dient *BIV / MIVD* vooraf te worden geïnformeerd.

Internationaal transport van een *TBB* vindt pas plaats na goedkeuring van het transportplan (bijgevoegd in deze bijlage) door *BIV / MIVD* en de beveiligingsautoriteit of equivalent in het ontvangende land.

Verzenden

Onder verzenden van een *TBB*, in het bijzonder *BI*, wordt het fysiek aanbieden daarvan verstaan aan een postbedrijf dat zorgdraagt voor doorgaans ongecontroleerd vervoer naar de eindbestemming. Het *TBB*, in het bijzonder *BI*, gaat dubbel verpakt volgens **bijlage 22.4** op in de massa overige te vervoeren poststukken. Bij verzending per post van *BI* vanaf *TBB* 3 en hoger dient dit volgens verpakt volgens **bijlage 22.4** aangetekend te worden verstuurd met een track en trace nummer waardoor het te achterhalen is waar het poststuk zich bevindt. Deze verzendingen dienen geregistreerd te worden door de *BF*. De ontvangende partij beschikt als bedrijf over een geldige ABDO autorisatie of is het Ministerie van Defensie. Verzending van een *TBB* 1, in het bijzonder *BI*, per post is niet toegestaan.

Op de volgende pagina's is een transportplan en eisen omtrent verpakken en verzenden van een *TBB*, in het bijzonder *BI* opgenomen.

	Bijlage 22.1	
	Transportplan	

Please approve the following Transportation Plan for the Netherlands:

International transportation plan for the Netherlands

Cont'd

E	Routing of consignment:	
E 1	Date / time of Departure	
E 2	Date / estimated time of Arrival	
E 3	Routes to be used between point of origin, point of export, point of import and ultimate destination:	
E 4	Methods of transport for each portion of the consignments	
E 5	Freight Forwarders / Transportation Agents to be used	
E 6	Customs of Port Security Contacts	

F	Authorized courier:	
F 1	Name(s) and identification of authorized Courier	

G	Security Officers's signature, date and stamp of the requesting facility:	
----------	--	--

H	Signature, date and seal of the releasing NSA / DSA:	
----------	---	--

I	Signature, date and seal of the receiving NSA / DSA:	
----------	---	--

Bijlage 22.2 Verzenden van een BI in het binnenland	
---	--

Binnenland (geldt eveneens voor internationaal equivalent BI).

- : Niet toegestaan
V : Wel toegestaan

	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	DEPARTEMENTAAL/ VERTROUWELIJK	PERSONEELS VERTROUWELIJK	MEDISCH GEHEIM	COMMERCEEL VERTROUWELIJK	ONGERUBRICEERD & ONGEMERKT
Normale verzending:								
Wijze van transport (keuze uit):								
ABDO geautoriseerde koerier	-	V	V	V				
Aangetekende civiele postverzending	-	V	V	V				
Normale civiele postverzending	-	-	-	V	V	V	V	V
Verpakken (keuze uit):								
Veiligheidsenveloppe + buitenenveloppe	-	V	V					
Dubbele enveloppe waarbij de binnenenveloppe is verzegeld.	-	V	V					
Opmerkingen:								
Ontvangstbewijs	-	V	V					

Bijlage 22.3 Verzenden van een <i>BI</i> naar het buitenland	
--	--

Naar het Buitenland (geldt eveneens voor internationaal equivalent *BI*).

	<i>Stg.</i> ZEER GEHEIM	<i>Stg.</i> GEHEIM	<i>Stg.</i> CONFIDENTIEEL	DEPARTEMENTAAL VERTROUWELIJK	PERSONEELS VERTROUWELIJK	MEDISCH GEHEIM	COMMERCIEEL VERTROUWELIJK	ONGERUBRICEERD & ONGEMERKT
- : Niet toegestaan V : Wel toegestaan								
Normale verzending:								
Wijze van transport (keuze uit):								
Begeleide diplomatieke zending	V	V	V					
ABDO geautoriseerde koerier	-	V	V	V				
Aangetekende civiele postverzending	-	-	-	V				
Normale civiele postverzending	-	-	-	-	V	V	V	V
Suitengewone verzending ivm groote:								
Wijze van transport uit								
Nederlands / bondgenootschappelijk transport	V	V	V					
Verpakken (keuze uit):								
Dubbele enveloppe waarbij de binnenenveloppe is verzegeld.	V	V	V					
Veiligheidsenveloppe + -koffer	V	V	V					
Veiligheidsenveloppe + buitenenveloppe	V	V	V					
Pakket omwikkeld met pakpapier en Veiligheidstape	V	V	V					
Opmerkingen:								
Ontvangstbewijs	V	V	V	V				

Verzendingen van een *BI* naar het buitenland vindt plaats na overleg met *BIV* / *MIVD*.

	Bijlage 22.4 Verpakken van <i>BI</i>	
--	---	--

Verpakken van *BI*

Indien *BI* wordt verzonden, wordt deze *BI* verpakt in zorgvuldig geadresseerde enveloppen c.q. pakketjes. In het geval van het verzenden van *TBB 2* of hoger of internationaal equivalent gerubriceerde informatie, *ATOMAL*, *SAR*, *COMINT* of *CRYPTO* wordt een ontvangstbewijs ingesloten.

Het verpakken van *BI* en internationaal equivalent gerubriceerde *Informatie* kan op twee manieren geschieden waarbij optie 1 de voorkeur heeft, te weten:

1. een veiligheidsenvelop als binnenenveloppe met een normale enveloppe als buitenenveloppe, of;
2. dubbele enveloppen waarbij de naden van de binnen enveloppe worden verzegeld met veiligheidstape.

Ongeacht de wijze van verpakken draagt de binnen enveloppe te allen tijde de rubricering en de eventuele merking die de ingesloten *BI* als geheel draagt.

Op de binnenenveloppe wordt de geadresseerde alsmede de afzender vermeld. Wanneer de binnenenveloppe *CRYPTO* is gemerkt, wordt op de binnenenveloppe vermeld: **UITSLUITEND TE OPENEN DOOR DE CRYPTOBEHEERDER** of **ONLY TO BE OPENED BY THE CRYPTOCUSTODIAN**. Op de buitenenveloppe wordt de geadresseerde alsmede de afzender vermeld, maar geen *Rubricering*.

Indien de *BI* niet in een veiligheidsenveloppe past, wordt er gebruik gemaakt van een pakketje, koker voor tekeningen e.d. Op het pakketje c.q. koker wordt de hoogste *Rubricering* van het geheel aangebracht en het geheel wordt zodanig gesloten dat openen zonder verbreken van de sluiting niet mogelijk is. Hiertoe wordt gebruik gemaakt van Defensie veiligheidstape en/of kabelverzegelhuis. Op het pakketje wordt de geadresseerde alsmede de afzender vermeld. Wanneer de zending *CRYPTO* is gemerkt, wordt op de binnenverpakking tevens vermeld: **UITSLUITEND TE OPENEN DOOR DE CRYPTOBEHEERDER** of **ONLY TO BE OPENED BY THE CRYPTOCUSTODIAN**. Het geheel wordt vervolgens omwikkeld met inpakpapier met vermelding van geadresseerde en afzender.

In het geval dat gebruik wordt gemaakt van een stalen kist, wordt deze stalen kist verzegeld met een kabelverzegelhuis (stalen draad met verzegelhuis).

BI wordt niet verzonden, indien:

- doorhalingen of overschrijvingen van het adres voorkomen;
- het adres in potlood is geschreven;
- de binnen (veiligheids)envelop en/of het pakket sporen dragen dat deze zijn geopend en vervolgens weer afgesloten zijn.

Het is niet toegestaan om *BI* post, indien onbestelbaar op het aangeven adres, achter de desbetreffende geadresseerde aan te sturen indien deze niet meer werkzaam is op de locatie.

Indien het een zending van *Cryptomiddelen* betreft, wordt contact met de verzendende *Cryptobeheerder* opgenomen. De *Cryptobeheerder* geeft instructies hoe nu verder te handelen.

Ontvangstbewijzen

Een ontvangstbewijs wordt (in de binnenenveloppe) bijgesloten wanneer *BI* op *TBB 2* of hoger gerubriceerde of internationaal equivalent gerubriceerde *Informatie*, *ATOMAL*, *SAR*, *COMINT* of *CRYPTO* wordt verzonden.

Dit bewijs vermeldt het kenmerk en het eventuele exemplaarnummer van het document en de eventuele bijlage(n).

De ontvanger (die beschikt over het juiste screeningsniveau) zendt het ontvangstbewijs ondertekend en gedateerd terug naar de afzender. De afzender ziet er op toe dat hij het ontvangstbewijs terug ontvangt en doet, indien dit niet binnen redelijke termijn plaatsvindt, navraag. Heeft dit geen resultaat dan stelt de afzender zijn/haar *BF* op de hoogte. De *BF* doet navraag naar de zending. Indien de zending niet is aangekomen dient dit als beveiligingsincident te worden behandeld.

Onder redelijke termijn wordt verstaan:

- binnen Nederland: 2 weken;
- binnen Europa: 3 weken;
- buiten Europa: 1 maand.

	Bijlage 23 Fysieke opslag, verwerking, ontwikkeling en vernietiging	
--	---	--

Registratie

Bijzondere Informatie (BI), met het niveau van *TBB 3* en hoger, en de fysieke en/of digitale toegang daartoe dienen te worden geregistreerd. Dit geldt zowel voor de ontvangen *BI* van het Ministerie van Defensie als voor de producten **en** documentatie die op basis daarvan zijn gegenereerd. Hierbij zijn de *RAL*, de *PSI* en/of bijzondere contractvoorwaarden leidend.

Bij de *BF* of een daartoe aangewezen en geautoriseerd persoon dient een actueel overzicht voorhanden te zijn van de *BI* vanaf *TBB 3* en hoger, waar deze zich bevinden en wie deze *BI* onder zijn of haar beheer heeft. De *BF* of een daartoe aangewezen en geautoriseerd persoon dient een actueel overzicht te hebben van alle *Bijzondere Opdrachten (BO)* vanaf het niveau van *TBB 4*. Voor *TBB 3* en hoger geldt tevens dat een registratie wordt bijgehouden van wie toegang heeft gehad tot dan wel werkzaamheden heeft verricht aan dan wel inzage heeft gehad in de *BI*. Een dergelijke zorgvuldige registratie van *BI* en toegang daartoe is essentieel voor de *Beveiliging*. Op basis daarvan kan te allen tijde controle plaatsvinden of de *BI* nog aanwezig en afdoende beveiligd is.

Labeling

Het is van belang dat een *BI* op de juiste wijze wordt voorzien van (unieke) kenmerken, *Rubricering* en *Merkingen* die aangeven op welke wijze het *BI* moet worden behandeld en opgeslagen. Meer over de juiste wijze van het aanbrengen van kenmerken, *Rubriceringen* en *Merkingen* is opgenomen in bijlage 23.1.

Reproductie van BI

Voor de voortgang van de *BO* kan het noodzakelijk zijn dat er reproducties moeten worden gemaakt van *BI*. Uiteraard dient dit beperkt te worden tot het absoluut noodzakelijke. Immers hoe meer reproducties hoe groter de kans op *Compromittatie*. Voor het reproduceren van *BI* gelden dan ook strenge normen die moeten worden nageleefd. Het reproduceren van een *BI* is niet toegestaan zonder voorafgaande toestemming van de *Opdrachtgever*.

Voor reproducties van een *BI* of delen daarvan gelden uiteraard dezelfde beveiligingsnormen als voor het origineel. Bij documenten waarin *BI* aanwezig is wordt bij voorkeur de rubricering per alinea toegekend. Hierdoor kunnen onduidelijkheden worden voorkomen. Naast het origineel moeten ook de reproducties worden geregistreerd en voorzien van unieke kenmerken, *Rubriceringen* en *Merkingen* als het gaat om *Staatsgeheimen*.

Ook de middelen die gebruikt worden voor reproducties zoals printers, scanners en kopieermachines dienen op dezelfde wijze te worden beveiligd en bevinden zich dus in het compartiment. Deze apparatuur moet eveneens voldoen aan de eisen zoals gesteld in hoofdstuk 4. Tevens kan bij BIV / MIVD een 'beveiligingsbeleid voor de Multifunctional' worden opgevraagd die meer informatie geeft over het behandelen van deze Multifunctional in het kader van *BI*.

Vernietiging van *BI*

Als *BI* niet meer benodigd is voor de *BO* of als de *BO* is beëindigd, dient het te worden vernietigd of te worden teruggegeven aan de *Opdrachtgever*. Onnodige opslag van *BI* leidt tot een verhoogde kans op *Compromittatie* en vergt een blijvende, wellicht niet langer noodzakelijke inspanning met betrekking tot *Beveiligen*.

Voor vernietiging van een *BI* gelden eisen. Essentieel hierbij is dat na vernietiging geen *Informatie* meer herleidbaar is.

Het vernietigen wordt uitgevoerd volgens een door de *BF* ingericht proces. Vernietigen geschiedt altijd onder toezicht van een geautoriseerd persoon waarbij functiescheiding strikt is toegepast. Er dient te allen tijde een Proces Verbaal van vernietiging te worden opgemaakt dat door de *BF* wordt geregistreerd en beheerd. Zie **bijlage 23.2** voor meer over vernietiging en de bijbehorende formulieren.

Algemene Beveiligingseisen Defensie Opdrachten 2017

	Bijlage 23.1 Labeling van een TBB	
--	---	--

Informatie	Rubricering	Rubricerings-tekst	Methode van aanbrenging	Plaats Rubricering / Merking
Document	Gehele document is gerubriceerd en/of gemerkt.	<i>Rubricering</i> en/of <i>Merking</i> in hoofdletters (alleen op eerste pagina of in colofon: vermelding van vaststeller <i>Rubricering</i> , datum vaststelling en de geldigheidsduur).	- Handgeschreven. - Geprint. - Gestempeld.	- Boven- en onderkant van elke bladzijde. - Op omslag. - Op bijlagen. (Aanbrengen exemplaar- en bladzijdenummering, zie hoofdstuk 4).
Document	Bijlage is hoger gerubriceerd en/of gemerkt dan hoofd-document.	Hoogste <i>Rubricering</i> en/of <i>Merking</i> in hoofdletters. (In colofon: vermelding van vaststeller <i>Rubricering</i> , datum vaststelling en de geldigheidsduur)	- Handgeschreven. - Geprint. - Gestempeld.	Op de omslag hoofddocument: <hoogste <i>Rubricering/Merking</i> > met toevoeging zonder bijlage (x) < <i>Rubricering/Merking</i> > of <ongerubriceerd/ongemerkt>. Op de bijlage(n) aan de boven- en onderkant van elke bladzijde. (Aanbrengen exemplaar- en bladzijdenummering, zie hoofdstuk 4).
Document	Verschillende <i>Rubriceringen</i> in één document.	(SZG): alinea met <i>Stg. ZEER GEHEIM</i> gerubriceerde <i>Informatie</i> (SG): alinea met <i>Stg. GEHEIM</i> gerubriceerde <i>Informatie</i> (SC): alinea met <i>Stg. CONFIDENTIEEL</i> gerubriceerde <i>Informatie</i> (DV) alinea met <i>Departementaal VERTROUWELIJK</i> gerubriceerde <i>Informatie</i>	- Handgeschreven. - Geprint. - Gestempeld.	Hoogste <i>Rubricering</i> aan boven- en onderkant van elke bladzijde. Afkorting <i>Rubricering</i> aanbrengen aan het begin van iedere alinea. (Aanbrengen exemplaar- en bladzijdenummering, zie hoofdstuk 4).
Elektronische media (incl. verwijderbare harde schijven)	Alle <i>Rubriceringen</i> en/of <i>Merkingen</i> .	Hoogste niveau van <i>Rubriceringen</i> en/of <i>Merkingen</i> in hoofdletters.	Gegevensdrager graveren, inbranden of beschrijven met watervast stift, of sticker met <i>Rubricering / Merking</i> , kleur of lint/label.	Stickers of (graveer-) tekst zichtbaar plaatsen. Zo mogelijk beide zijden van een sticker of (graveer-) tekst voorzien.
Werkstations	Alle <i>Rubriceringen</i> en/of <i>Merkingen</i> .	Hoogste niveau van <i>Rubriceringen</i> en/of <i>Merkingen</i> in hoofdletters.	Sticker met <i>Rubricering / Merking</i> .	Stickers zichtbaar plaatsen op systeemkast en bovenzijde beeldscherm.
Laptops	Alle <i>Rubriceringen</i> en/of <i>Merkingen</i> .	Hoogste niveau van <i>Rubriceringen</i> en/of <i>Merkingen</i> in hoofdletters.	Sticker met <i>Rubricering / Merking</i> .	Stickers zichtbaar plaatsen op buitenzijde scherm/klep.

Zie volgende pagina voor een overzicht van manieren van vernietigen van een TBB.

Bijlage 23.2 Vernietiging van een <i>TBB</i>		
--	--	--

	TBB 1	TBB 2	TBB 3	TBB 4
	ZG	G	C	DV
Papier	Als <i>TBB 2</i> én verbranden	Versnipperen L<25mm B<3mm	Versnipperen L<25mm B<3mm	Versnipperen L<30mm B<5mm
CD/DVD	Shredde en verbranden	Shredde	Shredde	Breaken
Diskette	Shredde en verbranden	Shredde	Shredde	Breaken
Harde schijf	Shredde en verbranden	Shredde	Shredde	Doorboren
USB stick	Shredde en verbranden	Shredde	Shredde	Doorboren
Overig	Shredde en verbranden	Shredde	Shredde	Vernielen

Zie volgende pagina voor een bewijs van overdracht bij vernietiging wanneer een *TBB* extern wordt vernietigd.

Ondertekende: _____ Werknemer-ID: _____ Functie: _____

Verzoekt de beveiligingsfunctionaris/ cryptobeheerder van: _____ (eenheid)

De volgende informatie te vernietigen uit het archief van: _____ (eenheid)

[illegible]

20 _____ Voor overname

Handtekening

¹ Bijvoorbeeld: papier, harddisk, DVD, USB-stick enz.

Bijlage 23.2.2

Proces Verbaal van vernietiging



Ministerie van Defensie

PROCESVERBAAL VAN Vernietiging

Op heden _____ 20____, werden ten overstaan van

1. _____ rang en functie _____

2. _____ rang en functie _____

de aan ommezijde of in bijlage vermelde informatie door middel van:

_____ ¹

te _____ vernietigd.

1. _____
(handtekening)

2. _____
(handtekening)

Bij vernietiging van gerubriceerde informatie dient nauwlettend te worden toegezien, dat uit de resten geen informatie meer kan worden gereconstrueerd.

¹ Aangegeven op welke wijze de vernietiging heeft plaatsgevonden

- Verbranding
- verpulvering c.q. verbrokkeling
- verbranding gevolgd door verpulvering
- versnippering
- versnippering gevolgd door verbranding
- oplossing met behulp van chemicaliën
- verwijdering d.m.v. wissen of overschrijven

	Bijlage 24 De taken en verantwoordelijkheden van de (sub-)Cyber-Beveiligingsfunctionaris	
--	--	--

De Cyber-Beveiligingsfunctionaris en sub-Cyber-Beveiligingsfunctionaris

De *Cyber-Beveiligingsfunctionaris* (*Cyber-BF*) is belast met de dagelijkse zorg voor de cyber security en kan bij deze werkzaamheden terzijde worden gestaan door één of meer aangewezen *sub-Cyber-Beveiligingsfunctionarissen*, bijvoorbeeld als vervanger bij afwezigheid van de *Cyber-BF* of één voor elke bedrijfslocatie of op grond van een bepaalde specialisatie binnen het digitale werkveld. De directie draagt aan *BIV / MIVD* de kandidaat (sub-)Cyber-BF voor die voldoet aan de eisen, taken en verantwoordelijkheden zoals gesteld in de *ABDO*. De *Cyber-BF* heeft rechtstreekse en onafhankelijke toegang tot de directie van de organisatie waar het Cyber-security aangaat. **(voor aanmelding Cyber-BF en sub-Cyber-BF zie bijlage 24.1)**

Minimale eisen voor de aanwijzing van een (sub-)Cyber-Beveiligingsfunctionaris

Als minimum eis dient een (sub-)Cyber-Beveiligingsfunctionaris:

- een Nederlandse nationaliteit te hebben en in dienst te zijn van het desbetreffende bedrijf;
- over voldoende autonomie, bevoegdheden, slagkracht en senioriteit te beschikken;
- gescreend te zijn op het hoogst geldende niveau van de *Bijzondere Opdrachten* die het bedrijf uitvoert;
- rechtstreekse en onafhankelijke toegang te hebben tot de CEO, directie of Raad van Bestuur;
- te beschikken over kennis ten aanzien van cybersecurity en IT-infrastructuren op het niveau van Certified Information Systems Security Professional (CISSP).

Taken en verantwoordelijkheden

In relatie tot een *ABDO Autorisatie* is de (sub-)Cyber-BF verantwoordelijk voor:

- het vaste aanspreekpunt vanuit de *Opdrachtnemer* zijn voor de *MIVD* en vertegenwoordigt hierbij de *Opdrachtnemer* voor wat betreft alle digitale beveiligingsaspecten en is bevoegd tot het nemen van de vereiste maatregelen en beslissingen;
- het opstellen van het cybersecuritygedeelte van het beveiligingsplan in relatie tot de *Bijzondere Opdrachten* en *TBB* conform de eisen van de *ABDO 2017*;
- de implementatie van noodzakelijke wijzigingen naar aanleiding van een verhoogd dreigingsbeeld of een incident, in het *Beveiligingsplan* binnen de gestelde termijn;

Algemene Beveiligingseisen Defensie Opdrachten 2017

- het op basis van de voortgang van *Bijzondere Opdrachten* en het op locatie hebben van een *TBB* regelmatig actualiseren van het (door *BIV / MIVD* ingestemde) cybersecuritygedeelte van het beveiligingsplan;
- periodiek toetsen van het cybersecuritygedeelte van het *Beveiligingsplan* aan de praktijk en dit schriftelijk rapporteren aan de directie en *BIV / MIVD*. Voor een totaalbeoordeling van de beveiliging stelt de *Cyber-BF* minstens eenmaal per jaar een rapport zelfinspectie op (**zie bijlage 37**) en stuurt dit aan de directie en *BIV / MIVD*;
- het geven van volledige medewerking bij controles, audits en onderzoeken bij *Opdrachtnemer* door *BIV / MIVD*;
- het melden, onderzoeken en treffen van maatregelen aangaande incidenten. Dit gebeurt volgens het Incident Handling proces (**zie bijlage 9**);
- voorlichting, in het kader van Security Awareness, aan vertrouwensfunctionarissen bij de start van een nieuwe *Bijzondere Opdracht*, periodiek gedurende *Bijzondere Opdrachten* aangaande *ABDO* procedures en de bijbehorende verantwoordelijkheden;
- op regelmatige wijze de sub-*Cyber-BF* op de hoogte te stellen van procedures en incidenten zodat deze de taken kan uitvoeren bij afwezigheid van de *Cyber-BF*;
- het door IT-beheer laten treffen van beveiligingsmaatregelen die beschikbaarheid, integriteit en vertrouwelijkheid van de *TBB* garanderen;
- het periodiek zich door IT-beheer laten informeren over de inrichting van beschikbaarheid, integriteit en exclusiviteit van de digitale infrastructuur binnen het bedrijf;
- het door middel van een registratie toezicht houden op locatie, uitgifte, inname en herkomst van alle door de organisatie in ontvangst of beheer genomen digitale *TBB*;
- het periodiek uitvoeren van controles uit op implementatie van de in het *ABDO* opgenomen beveiligingseisen;
- het, namens de directie, (laten) nemen van gepaste beveiligingsmaatregelen op het gebied van Cyber-security;
- het controleren van de verstrekte *Autorisaties* op juistheid;
- het periodiek inzicht hebben van ongeautoriseerde apparatuur en -software op de digitale infrastructuur en genomen maatregelen;
- het analyseren van beveiligingsrelevante issues van Loggings en zorgdragen voor Monitoring van activiteiten die een impact op de beveiliging hebben;
- het vrijgeven van geblokkeerde accounts;
- toestemming verlenen voor het uitzetten/uitstellen van schermbeveiliging;
- het onderhouden van een registratie voor het uitzetten/uitstellen van de schermbeveiliging op een werkplek(sessie) en de noodzaak waarom ontheffing is gegeven;
- het verlenen van toestemming om een lockout van een gebruikers-/beheeraccount op te heffen of het wachtwoord te resetten;
- het verlenen van toestemming voor ingebruikname van een groepsaccount;
- het verlenen van toestemming voor het, van locatie af, meenemen van apparatuur, informatie en programmatuur van de organisatie;
- het verlenen van goedkeuring voor wijzigingen aan *TBB* systemen;
- het inzicht hebben in alle externe koppelingen wanneer sprake is van beheer op afstand.
- het laten treffen van beveiligingsmaatregelen door IT-beheer om *Beschikbaarheid, Integriteit* en *Vertrouwelijkheid* van de *TBB* te garanderen.

Bijlage 24.1

Benoeming (sub-)Cyber-Beveiligingsfunctionaris

Benoeming (sub-)Cyber-Beveiligingsfunctionaris en toekennen van verantwoordelijkheden

Naar:

Bureau Industrie Veiligheid

Afdeling Contra-Inlichtingen en Veiligheid

Militaire Inlichtingen-en Veiligheidsdienst

Postbus 90701

2597 LS Den Haag

Benoeming (sub-)Cyber-Beveiligingsfunctionaris

Ik, _____ van _____
(hoogst bestuursorgaan, directie en / of eigenaar) (Bedrijf / Organisatie)

benoem, na instemming van BIV / MIVD, de hierna genoemde medewerker, als (sub-)Cyber-Beveiligingsfunctionaris conform de in de ABDO 2017 gestelde eisen.

Datum _____
(volledige naam van (sub-)Cyber-BF)

Handtekening _____
(Handtekening van hoogste bestuursorgaan, directie en / of eigenaar)

Ik, _____
(volledige naam van aangewezen (sub-)Cyber-BF)

Werknemer van _____
Functie _____

begrijp en accepteert hierbij de taken en verantwoordelijkheden van de (sub-)Cyber-BF, zoals beschreven in bijlage 24 van de ABDO 2017 en zal mij hieraan houden.

.

(handtekening van de (sub-)Cyber-BF)

Alleen in te vullen door BIV / MIVD

Goedgekeurd door _____ Afgekeurd door _____

Datum _____ Datum _____

Reden _____

	Bijlage 25 Goedkeuring gebruik van middelen	
--	---	--

In een aantal gevallen mogen alleen middelen gebruikt worden die zijn goedgekeurd door *BIV / MIVD*. Denk hierbij aan cryptomiddelen of specifieke software voor het beveiligen van verbindingen.

De goedkeuring van *BIV / MIVD* geldt automatisch ook voor de middelen die door het Nationaal Bureau voor Verbindingsveiligheid (*NBV*) van de *AIVD* zijn goedgekeurd. Deze middelen zijn door overheden ter evaluatie aan het *NBV* voorgelegd. De goedkeuring van het *NBV* geldt in principe voor de gehele overheid. Door de automatische goedkeuring van *BIV / MIVD* kunnen deze middelen ook gebruikt worden buiten de overheid, waar het een gerubriceerde opdracht van het Ministerie van Defensie aangaat. De lijst met goedgekeurde middelen van het *NBV* is op Internet bij de website van de *AIVD* beschikbaar.

Tevens geldt de goedkeuring van *BIV / MIVD* ook automatisch voor de middelen die door de Beveiligingsautoriteit (*BA*) van het Ministerie van Defensie zijn goedgekeurd.

Als laatste kan *BIV / MIVD* zelf middelen goedkeuren.

Op aanvraag is een lijst met middelen verkrijgbaar die op basis van bovenstaande goedkeuringen is samengesteld.

	Bijlage 26 De <i>Cyber</i>-security awareness training	
--	--	--

Bij een *Cyber*-security awareness-training wordt o.a. aandacht besteed aan de volgende zaken:

- de gerubriceerde opdracht inclusief de rubricering;
- het belang van de opdracht voor Defensie en de organisatie en de schade die ontstaat als de opdracht is gecompromitteerd;
- wie binnen de organisatie betrokkenen is bij de beveiliging van de gerubriceerde opdracht van Defensie (o.a. projectteam, *Cyber-BF*, IT-beheer);
- het *ABDO* als eisen set om de opdracht te beveiligen;
- het beveiligingsplan van de organisatie om dreigingen af te weren;
- algemene en specifieke dreigingen in het digitale domein (waaronder Phishing);
- uitleg over de maatregelen en het gebruik daarvan;
- uitleg over het gebruik van beveiligingsmiddelen;
- het melden van incidenten en hoe te handelen bij incidenten.

Meer informatie en beveiligingsadviezen zijn te vinden bij het Nationaal Cyber Security Centrum, www.ncsc.nl en de Algemene Inlichtingen en Veiligheidsdienst www.aivd.nl.

	Bijlage 27 Registratie van ICT-bedrijfsmiddelen	
--	---	--

Om onder andere onderzoek te kunnen doen nadat een netwerk of systeem is gecompromitteerd en om goed beheer van bedrijfsmiddelen uit te kunnen voeren is een goede, kloppende registratie van bedrijfsmiddelen noodzakelijk. Vaak wordt voor deze registratie een Configuratiemanagementdatabase (CMDB) gebruikt. In gevallen waarbij het gaat om een zeer klein netwerk of systeem kan ook met een spreadsheet worden volstaan.

Het heeft de voorkeur om bij het opzetten van de registratie van bedrijfsmiddelen voor de gerubriceerde opdracht van Defensie zo veel mogelijk van de reeds bestaande systemen en systematiek binnen de organisatie gebruik te maken.

De reikwijdte van de verplichte registratie van bedrijfsmiddelen is in principe beperkt tot die bedrijfsmiddelen die ingezet worden voor de gerubriceerde opdracht van Defensie.

Onder bedrijfsmiddelen verstaan we onder andere:

- hardware;
- software;
- gegevensverzamelingen;
- Diensten.

Van de bedrijfsmiddelen zijn tenminste de volgende gegevens geregistreerd:

- een unieke identifier ("ID");
- omschrijving van het bedrijfsmiddel;
- merk, type, fabrikant en leverancier;
- datum van indienststelling;
- fysieke locatie;
- gebruiker (voor zover aan een gebruiker toegekend, "op naam");
- classificatie voor de organisatie ten behoeve van waardebeoordeling (bijvoorbeeld toegekend aan project X of Y);
- TBB-niveau;
- onderhoudsgegevens. (status, historie, planning);
- bijzonderheden;
- configuratie, programmatuur.

De samenhang tussen de ICT-bedrijfsmiddelen is in kaart gebracht in een netwerktekening. Mogelijke elementen voor een netwerktekening zijn:

- netwerken;
- netwerksegmentatie;
- beheersegment;
- DMZ;
- gebruikersomgeving;
- gastennetwerk;
- dataopslag;
- hardware;
- software;

Algemene Beveiligingseisen Defensie Opdrachten 2017

- externe en -interne koppelingen;
- locatie;
- *Vercijfering.*

	Bijlage 28 Mobiele apparatuur en <i>BYOD/CYOD</i>	
--	---	--

Mobiele apparatuur zijn alle “devices” (apparaten) die geen statische plaats hebben. Een werkstation op het bureau heeft een statische, geregistreerde plek. Een laptop, smartphone, tablet e.d. hebben geen vaste plaats en zijn dus mobiele apparaten. Een “mobiel apparaat” is in deze context een device met eigen processorcapaciteit. Een usb-stick is dus geen mobiel apparaat, maar bijvoorbeeld een Raspberry-Pi wel.

Bring-Your-Own-Device (*BYOD*) is een benaming voor die apparatuur die doorgaans door de gebruiker zelf (privé) is aangeschaft en ingezet wordt voor bedrijfsmatige toepassingen. Hierdoor heeft de *Opdrachtnemer* geen volledige zeggenschap én beheer over het apparaat.

Choose-Your-Own-Device (*CYOD*) is een variant op *BYOD* waarbij de gebruiker een keuze heeft uit vooraf door de organisatie gekozen apparaten.

Doordat de *Opdrachtnemer* geen volledig beheer over het apparaat heeft, wordt aan het principe dat voor het beveiligen van TBB alleen gecontroleerde toegang toegestaan is, geweld aangedaan.

Er zijn softwareoplossingen die claimen aan de genoemde bezwaren tegemoet te komen. In speciale gevallen is het toegestaan deze oplossingen te gebruiken. Wanneer dit van toepassing is, is de oplossing beschreven in het beveiligingsplan en is de toepassing goedgekeurd door *BIV / MIVD*.

	Bijlage 29 Systeemdocumentatie	
--	--	--

Systeemdocumentatie (o.a. een Operations Manual) is een document of set van documenten die de implementatie van een systeem beschrijven om beheer te kunnen uitvoeren. Een gedegen documentatie is van belang om gefundeerd beveiligingsmaatregelen te kunnen nemen, om het systeem weer op te kunnen bouwen na een verstoring, om onderzoek te kunnen doen naar incidenten en als basis voor changemanagement. Vanuit de aard van de documentatie bevat deze o.a. beschrijvingen van beveiligingsmaatregelen en informatie die een mogelijke aanvaller kan gebruiken bij een geavanceerde aanval. Dit deel van de systeemdocumentatie zal beveiligd moeten worden tegen inzage en gebruik door onbevoegden.

De reikwijdte van de systeemdocumentatie is in principe beperkt tot die bedrijfsmiddelen die ingezet worden voor de gerubriceerde opdracht van Defensie.

Systeemdocumentatie beschrijft onder andere:

- doel en gebruik;
- beheeraccounts;
- aanpassingen ten opzichte van fabrieksinstellingen;
- screenshots van beheerinterfaces;
- samenhang tussen systemen;
- opbouw van systemen;
- technische beschrijving van hardware;
- welke services/processen starten onder welk account;
- systeemnamen;
- bestandsnamen en –plaatsen.

Als het met het oog op trekken van ongewenste aandacht niet mogelijk is om een gegevensdrager te labelen, kan gebruik gemaakt worden van onderstaand kleurensysteem (voor bijvoorbeeld een keycord). Dit moet dan beschreven zijn in het beveiligingsplan en zijn opgenomen in de gebruikersinstructies.

	Rood	TBB 1	STG. ZEER GEHEIM, NLD TOP SECRET, COSMIC TOP SECRET, TRÈS SECRET UE/EU TOP SECRET, ATOMAL, SAR, BOHEMIA, COMINT
	Blauw	TBB 2	STG GEHEIM, NLD SECRET, NATO SECRET, SECRET UE/EU SECRET, UN STRICTLY CONFIDENTIAL
	Groen	TBB 3	STG. CONFIDENTIEEL, NLD CONFIDENTIAL, NATO CONFIDENTIAL, CONFIDENTIEL UE/EU CONFIDENTIAL, UN CONFIDENTIAL
	Geel	TBB 4	DEPARTEMENTAAL VERTROUWELIJK, NLD RESTRICTED, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED, PERSONEELSVERTROUWELIJK, COMMERCIEEL VERTROUWELIJK, MEDISCH GEHEIM, INTERN BERAAD
	Wit	Ongerubriceerd	ONGERUBRICEERD, NATO UNCLASSIFIED, NLD UNCLASSIFIED, UN UNCLASSIFIED

	Bijlage 31 Gebruikers, IT-beheerders en accounts	
--	--	--

Een geautoriseerde gebruiker is iemand die door tussenkomst van de Cyber-BF is geautoriseerd om te mogen werken met bijzondere informatie in een IT-systeem. Er moet een noodzaak aanwezig zijn, het systeem te gebruiken ten behoeve van het uitvoeren van de gerubriceerde opdracht. Alle andere gebruikers binnen de organisatie zijn ongeautoriseerde gebruikers, deze mogen niet werken met het systeem. Als in het *ABDO* gesproken wordt over “gebruikers”, worden daar alleen “geautoriseerde” gebruikers bedoeld.

IT-beheerders zijn een bijzondere groep geautoriseerde gebruikers. Deze krijgen de beschikking over accounts waarmee het systeem beheerd wordt, veelal is het niveau van rechten van deze accounts op het niveau van “root” of “administrator”, waardoor er geen technische restricties mogelijk zijn tot welke informatie het account toegang heeft. Ook kan het mogelijk zijn dat IT-beheerders ongedetecteerd wijzigingen aan systemen kunnen aanbrengen. Daarom worden er extra beveiligingseisen gesteld aan de beheeraccounts en de beheerders zelf.

Een account in een IT-systeem is een verzameling gegevens die bepaalt tot welke bronnen dat account toegang heeft. Bij gebruikersaccounts is vastgelegd waar de gebruiker als natuurlijk persoon toegang toe heeft. In het kader van het *ABDO* wordt het gebruikersaccount van een IT-beheerder een beheerdersaccount genoemd. Eisen ten aanzien van gebruikersaccounts gelden dus ook voor beheerdersaccounts. Naast gebruikersaccounts kunnen systeemaccounts bestaan. Onder systeemaccounts verstaan we onder andere functionele, machine- en serviceaccounts.

Een groepsaccount is een gebruikersaccount wat door meerdere natuurlijke personen gebruikt wordt. Dit soort account wordt alleen in bijzondere gevallen gebruikt, waarbij uit een aparte administratie blijkt wie op welk moment dit account gebruikt heeft.

In sommige organisaties wordt gesproken over “privileged” en “unprivileged” accounts. Beheeraccounts kunnen worden beschouwd als “privileged”, gebruikersaccounts doorgaans als “unprivileged”.

In verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toebrengt heeft een gebruiker of een IT-beheerder geen rechten om de gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen.

Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

	Bijlage 32 Grote concentratie <i>TBB</i>	
--	--	--

In een aantal normen wordt verwezen naar een grote concentratie *TBB*, waarop zwaardere maatregelen van toepassing zijn.

Hieronder een aantal voorbeelden van situaties waarop deze normen van toepassing zijn:

1. Personeelsgegevens.
De personeelsgegevens van een enkele defensiemedewerker zijn personeelsvertrouwelijk gemerkt en dient te worden behandeld als DEPARTEMENTAAL VERTROUWELIJK. Wanneer deze gecompromitteerd raken is de schade in principe beperkt tot deze ene medewerker. De slagkracht van Defensie in zijn geheel wordt niet aangetast. Wanneer echter alle personeelsgegevens van een deel van de organisatie op straat komen liggen, kan de slagkracht van Defensie in zijn geheel wel in gevaar komen. Daarom zal een verzameling personeelsgegevens in voorkomende gevallen zwaarder beveiligd moeten worden. Dit is in alle gevallen maatwerk.
2. Meerdere opdrachten voor één *Opdrachtnemer*.
Op het moment dat een *Opdrachtnemer* meerdere gerubriceerde opdrachten uitvoert en de data hiervan op dezelfde infrastructuur verwerkt, kan er sprake zijn een grote concentratie van *TBB*. In geval van een *compromittatie* is de schade voor Defensie aanzienlijk groter. Dit kan er toe leiden dat een dergelijke verzameling in voorkomende gevallen zwaarder beveiligd moeten worden. Dit is in alle gevallen maatwerk.

Per opdracht wordt bepaald of er sprake is van een "grote concentratie" *TBB*. Dit wordt dan opgenomen in de *Rubriceringsaanduidingslijst (RAL)*. Daarnaast kan *BIV / MIVD* in voorkomende gevallen een verzameling *TBB* als "grote concentratie" aanmerken.

	Bijlage 33 <i>Logging en Monitoring</i>	
--	---	--

Logging en *Monitoring* zijn middelen om er achter te komen of een systeem is gecompromitteerd. Met *Logging* worden gebeurtenissen vastgelegd. Hiermee is het mogelijk om bijvoorbeeld op basis van afwijkingen in een normbeeld een indicatie te krijgen of er data lekt. Met *Monitoring* is het bijvoorbeeld mogelijk om op basis van Indicators of Compromise (IOC's) een indicatie te krijgen of er malware (waaronder Advanced Persistent Threats, APT's) aanwezig is op een systeem of netwerk. Als eenmaal een incident is geconstateerd of vermoed, kunnen *Logging* en *Monitoring* worden gebruikt om het incident te onderzoeken. Zo kan door *Logging* en *Monitoring* ook Command & Control (C2) verkeer worden onderkend.

In logfiles is in ieder geval de volgende informatie opgeslagen:

- gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling of updates;
- uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore;
- gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases);
- handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels;
- beveiligingsincidenten (zoals de aanwezigheid van *Malware*, testen op *Vulnerabilities*, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services);
- verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen);
- handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.

Een logregel bevat:

- een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
- de gebeurtenis;
- waar mogelijk de identiteit van het werkstation of de locatie;
- het object waarop de handeling werd uitgevoerd;
- het resultaat van de handeling;
- de datum en het tijdstip van de gebeurtenis.

In grote of complexe systemen is het raadzaam om *Logging* af te laten handelen door een Security Information and Event Management systeem (SIEM). Daarop zijn de systemen aangesloten die logberichten genereren. Een SIEM genereert vervolgens meldingen en alarmoproepen aan de beheerorganisatie.

	Bijlage 34 <i>Virtualisatie en VLAN</i>	
--	---	--

Denk bij implementatie/installatie van een gevirtualiseerde infrastructuur aan:

- alleen de noodzakelijke Operating System (OS) components en services zijn geactiveerd;
- verbindingen met onnodige fysieke apparaten vanuit Virtual Machines (VM's) zijn verboden;
- file sharing tussen host en gast OS is gedeactiveerd;
- het gebruik van resources door een VM is gelimiteerd;
- fysieke switch poorten verbonden met een virtuele trunk poort zijn altijd statisch geconfigureerd.
- een virtuele switch is niet verbonden met andere virtuele switches of fysieke switches;
- productie- en testomgevingen voor VM's zijn gescheiden;
- er is een firewall geplaatst en geactiveerd om de host te beschermen;
- gast en host OS's dienen regelmatig gepatcht te worden.

Aandachtspunten om een goede controle te borgen indien *Virtualisatie* wordt toegepast:

- maandelijks vindt controle plaats van de virtuele omgeving;
- individuele login pogingen worden wekelijks op onregelmatigheden gecontroleerd;
- er vindt centrale Logging plaats van het gast OS;
- VM 'sprawl' door het aanmaken en verspreiden van VM's is niet mogelijk;
- migraties van VM's zijn gelogd en begeleid;
- het gebruik van Introspectieve Capaciteit zoals Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) is aanbevolen.

Aandachtspunten ten aanzien van herleidbaarheid naar individuele gebruikers en systeemfuncties zijn:

- geen enkele administrator mag inloggen onder "administrator" of "root";
- administrators moeten inloggen onder een persoonlijk toegewezen account;
- netwerk toegang tot de host is beperkt tot administrators voor beheerstaken;
- netwerkbeheer is gescheiden van operationeel verkeer van het gast OS;
- gebruik *Two-factor* authenticatie voor toegang tot het host systeem;
- gebruik wachtwoorden voor toegang tot Basic Input/Output System (BIOS) en "bootloaders";
- beheer van "hypervisors" is beperkt tot administrators en is gecentraliseerd;
- gebruik *Vercijferde* communicatie voor het beheer van het host OS;
- gast OS's zijn uitgesloten van toegang tot het beheernetwerk.

VLAN's bieden de mogelijkheid om logisch gescheiden netwerken op fysiek gedeelde hardware te realiseren. Hierdoor kunnen bijvoorbeeld aparte netwerksegmenten aan specifieke functies worden toebedeeld. Denk bij de implementatie van VLAN's onder andere aan:

- opstellen van een VLAN-nummerplan/procesmatig registreren van uitgifte- en inname van VLAN's;
- zorgdragen voor correcte en actuele documentatie van de configuratie;
- het maandelijks controleren of de VLAN-scheiding in de configuratie nog steeds correct is;
- zorgdragen voor patchmanagement.

	Bijlage 35 Demilitarized Zone (<i>DMZ</i>)	
--	--	--

Een *DMZ* is een netwerksegment tussen een onbetrouwbare omgeving (zoals het internet) en het netwerk waarop zich *TBB* bevindt. In dit segment kunnen servers worden geplaatst die op basis van de inhoud van het verkeer, het verkeer controleren.

In de *DMZ* staan o.a. Network Perimeter Devices en wordt in- en uitgaand verkeer gecontroleerd en/of getermineerd bijvoorbeeld door een proxy en een malwarescanner. De Network Perimeter Devices dienen te beschikken over een spanport. De proxy logt individueel TCP sessies, blokkeert specifieke URL's, domeinnamen en IP adressen conform een Blacklist. Tevens staan in de *DMZ* servers die connectiviteit vanaf het internet en het vertrouwde netwerk toestaan.

Bijlage 36

TEMPEST

TEMPEST

Elektronische apparatuur zendt elektromagnetische straling uit. Bij het verwerken van *Informatie* op deze apparatuur bestaat het risico dat de verwerkte *Informatie* te herleiden is uit de uitgezonden elektromagnetische straling. Dit fenomeen (*Compromitterende emissie*) en de maatregelen die kunnen worden getroffen om dit te minimaliseren worden aangeduid met de term: *TEMPEST*.

Er moet rekening gehouden worden met drie vormen van compromitterende emissie:

- rechtstreekse elektromagnetische straling;
- doorgeleiding, als er sprake is van instraling op een elektrische geleider (bijvoorbeeld een verwarmingsbuis of waterleiding);
- variaties in de voedingsspanning als gevolg van het verwerken van gegevens.

Bij de verwerking van een *TBB* worden eisen gesteld op het gebied van *TEMPEST*. Door middel van fysieke maatregelen en aanpassing aan de digitale apparatuur worden de genoemde kwetsbaarheden tegengegaan. Welke maatregelen er nodig zijn is situatieafhankelijk.

Dreiging

Er ontstaat een dreiging, als gevolg van bovengenoemde compromitterende emissie, als een niet-geautoriseerd persoon in staat is om een (elektrisch/elektromagnetisch) signaal op te vangen en op te slaan en hieruit de verwerkte (beeld)*Informatie* weet te reconstrueren.

Maatregelen

De maatregelen om bovenstaande dreiging tegen te gaan kunnen worden onderverdeeld in vier categorieën:

Scheiding systemen en netwerken

Bij de implementatie van de maatregelen wordt rekening gehouden met:

- de scheiding tussen ongerubriceerde *Informatie* en (*STG.*) gerubriceerde *Informatie*;
- de scheiding tussen gerubriceerde *Informatie* onderling (Bijvoorbeeld *Stg.* GEHEIM en NATO SECRET).

Afstand

Maatregelen die vallen onder de categorie afstand zijn gericht op het maken van een inspecteerbaar en controleerbaar gebied rondom de stralingsbron. De afstand (in meters, 3D-benadering, uitgaande van de kortst gemeten afstand) vanaf de stralingsbron tot de grens van het controleerbaar gebied bepaalt de zogenoemde "Ruimte-zone". De inspecteerbare ruimte is de ruimte waarover de eigenaar zeggenschap heeft en zelfstandig controles kan uitvoeren. Het controleerbaar gebied is dat gebied om de inspecteerbare ruimte heen waar maatregelen zijn genomen om controle uit te oefenen op personeel en voertuigen die zich daar bevinden.

Apparatuur

Algemene Beveiligingseisen Defensie Opdrachten 2017

Maatregelen die vallen onder de categorie apparatuur zijn gericht op het minimaliseren van de hoeveelheid afgegeven straling.

Installatie

Maatregelen die vallen onder de categorie installatie zijn gericht op het minimaliseren van de kans op doorgeleiding of variatie in de voedingsspanning. Om deze vormen van *Compromitterende* emissie tegen te gaan zijn maatregelen vastgesteld ten aanzien van bekabeling, installatie-afstanden en filtering.

Werkwijze

De noodzakelijke maatregelen ten behoeve van het verwerken van gerubriceerde informatie worden in samenwerking met *BIV / MIVD* vastgesteld. Hiervoor kan het nodig zijn om metingen te verrichten aan de beoogde ruimtes. Het proces en de regelgeving rond TEMPEST maatregelen is gebaseerd op gerubriceerde NATO-regelgeving.

	Bijlage 37 Zelfinspectierichtlijnen	
--	---	--

Organisaties moeten op grond van het *ABDO* de voorgeschreven beveiligingsmaatregelen periodiek op actualiteit en doelmatigheid te controleren. Het zelfinspectierapport kan een leidraad zijn voor deze controle.

Binnen het zelfinspectierapport wordt elke, voor de opdracht relevante, beveiligingseis gewogen en eventuele opmerkingen opgenomen. Ook wordt aangegeven welke actie benodigd is. Op aanvraag is een leeg zelfinspectierapport beschikbaar.

Elke afwijking van een eis in het *ABDO* brengt een risico met zich mee. In het rapport wordt onderscheid gemaakt in: laag risico, midden risico, hoog risico.

Het risico word gekwantificeerd als het product van de kans en de schade die de afwijking (de bevinding) kan aanbrengen ($\text{Risico} = \text{Kans} \times \text{Schade}$).

Het gewicht (laag, midden, hoog) is vertaald naar de termijn waarop actie nodig is:

- Laag risico (groene gebied) : Binnen een jaar is actie gewenst.
- Midden risico (oranje gebied): Komend kwartaal actie gewenst.
- Hoog risico (rode gebied): Zo spoedig mogelijk actie gewenst.

	Bijlage 38 Identificatie van werkstations	
--	---	--

Alleen werkstations die door de organisatie worden beheerd en die specifiek ingezet worden ten behoeve van de opdracht waar het *ABDO* op van toepassing is, zijn onderdeel van de IT-Infrastructuur. Op deze werkstations zijn specifieke beveiligingsmaatregelen van toepassing. Om te voorkomen dat “foute” apparatuur aangesloten wordt aan het netwerk zal er een vorm van automatische identificatie van werkstations moeten plaatsvinden. Verschillende technologieën kunnen worden toegepast, denk bijvoorbeeld aan:

- MAC-authenticatie;
- gebruik 802.1X protocol;
- toepassen RADIUS-server;
- toepassen domain-member check in de Active Directory.

Een combinatie van technologieën heeft de voorkeur. Welke technologie in een specifieke situatie gebruikt moet worden is onder andere afhankelijk van de grootte en complexiteit van het netwerk, hoogte van rubricering en of er andere, compenserende, maatregelen genomen zijn.

	Bijlage 39 Daderprofiel DEPARTEMENTAAL VERTROUWELIJK	
--	--	--

Uitsluitend na toestemming van *BIV / MIVD* te verkrijgen.

	Bijlage 40 Cryptofunctionaris	
--	--	--

Cryptofunctionaris

De Cryptofunctionaris is belast met de zorg Cryptomiddelen.

Taken en verantwoordelijkheden

De Cryptobeheerder is verantwoordelijk voor:

- het autoriseren van gebruikers van cryptomiddelen;
- het registreren van in gebruik zijnde cryptomiddelen;
- het implementeren van de cryptografische technieken conform vigerende wet- en regelgeving én de richtlijnen van Defensie;
- het beheren van CCI-apparatuur;
- het uitgeven van CCI-apparatuur;
- het periodiek controleren en tellen van CCI-apparatuur;
- het toezicht houden op en rapporteren over de CCI-apparatuur;
- de opslag van CCI-apparatuur;
- de verpakking van CCI-apparatuur;
- het transporteren van CCI-apparatuur;
- de afvoer en het vernietigen van CCI-apparatuur.

De formuleren in deze bijlage zijn van toepassing bij het aanstellen van of ontheffen van een cryptofunctionaris.

Bijlage 40.1

Verklaring van bekendheid met de geheimhoudingsplicht voor *Vertrouwensfunctionarissen* in het kader van een *CRYPTO*-functie

Ondergetekende : _____
(naam en voorletters)

Geboren op : _____ te: _____

Aangewezen voor de functie van : _____

Verklaart hierbij dat hij/zij:

- met het oog op de *CRYPTO* werkzaamheden, waaronder wordt verstaan zowel de hantering van de middelen als de behandeling en de kennisneming van *CRYPTO*, *CRYPTO-SECURITY* of *CCI-gemerkt* materieel waarmee ik ben of zal worden belast;
- kennis heeft genomen van de voor het *CRYPTO* bedrijf voorgeschreven beveiligingsmaatregelen, zoals omschreven in het Verbindingsbeveiligingsvoorschrift Fysieke beveiliging (VBV 41000 A);
- met nadruk op de inhoud van de artikelen 2, 3, 4, 5, 23, 98, 98a, 98b, 98c, 272, 273 en 463 van het *Wetboek van strafrecht* is gewezen;
- volstreekte geheimhoudingsplicht ten aanzien van de door hem/haar te verrichten *CRYPTO* werkzaamheden is opgelegd;
- is medegedeeld, dat indien ik enige eed (belofte) heb afgelegd en/of enige verklaring heb ondertekend, ten gevolge waarvan ik in bepaalde omstandigheden een meldingsplicht zou hebben, dan wel een mededelingsplicht heb krachtens de verhouding waarin ik tot anderen sta of zal komen te staan, ik nimmer enige mededeling zal mogen doen, hetzij direct, hetzij indirect, omtrent mijn hierboven aangegeven werkzaamheden en de daaruit resulterende kennis;
- ter kennis is gebracht, dat de aan mij hiervoor opgelegde volstreekte geheimhoudingsplicht, indien dit noodzakelijk is om mijn taak naar behoren te vervullen, niet geldt ten aanzien van personen die gemachtigd zijn tot het verrichten van dezelfde *CRYPTO* werkzaamheden of uitdrukkelijk bevoegd zijn daarvan kennis te nemen.

Plaats : _____

Datum : _____

Handtekening : _____

Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst
Bureau Industrieveiligheid

Bijlage 40.1

Verklaring van bekendheid met de geheimhoudingsplicht voor *Vertrouwensfunctionarissen* in het kader van een *CRYPTO*-functie

WETSARTIKELEN

Art. 2, 3, 4, 5, 23, 98, 98a, 98b, 98c, 272, 273, 463 Wvs.

Art. 2. De Nederlandse Strafwet is toepasselijk op ieder die zich in Nederland aan enig strafbaar feit schuldig maakt.

Art. 3. De Nederlandse Strafwet is toepasselijk op ieder die zich buiten Nederland aan boord van een Nederlands vaartuig of luchtvaartuig aan enig strafbaar feit schuldig maakt.

Art. 4. De Nederlandse Strafwet is toepasselijk op ieder die zich buiten Nederland schuldig maakt:

1. Aan een der misdrijven omschreven in artikel 92-96, 97a, 98-98c, 105 en 108-110.

Art. 5. -1. De Nederlandse Strafwet is toepasselijk op de Nederlander die zich buiten Nederland schuldig maakt:

1. aan een der misdrijven omschreven in de Titels I en II van het Tweede boek, en in de artikelen 206, 237, 272, 273, 388 en 389.

2. aan een feit hetwelk door de Nederlandse strafwet als misdrijf wordt beschouwd en waarop door de wet van het land waar het begaan is, straf is gesteld.

-2. De vervolging kan ook plaatshebben, indien de verdachte eerst na het begaan van het feit Nederlander wordt.

Art. 23. -1 Hij die tot een geldboete is veroordeeld is verplicht tot betaling van het bij de rechterlijke uitspraak vastgestelde bedrag aan de staat binnen de termijn door het openbaar ministerie dat met de tenuitvoerlegging van het vonnis of arrest is belast, te stellen.

-2. Het bedrag van de geldboete is ten minste twee euro vijftig.

-3. De geldboete die voor een strafbaar feit ten hoogste kan worden opgelegd, is gelijk aan het bedrag van die categorie die voor dat feit is bepaald.

-4. Er zijn zes categorieën: de eerste categorie, € tweehonderdvijfentwintig;

de tweede categorie, € tweeduizendtweehonderdvijftig;

de derde categorie, € vierduizendvijfhonderd;

de vierde categorie, € elfduizendtweehonderdvijftig;

de vijfde categorie, € vijfenveertigduizend;

de zesde categorie, € vierhonderdvijftigduizend.

-5. Voor een overtreding, onderscheidenlijk een misdrijf, waarop geen geldboete is gesteld, kan de rechter een geldboete opleggen tot ten hoogste het bedrag van de eerste, onderscheidenlijk de derde categorie.

Art. 98. -1. Hij die een inlichting waarvan de geheimhouding door het belang van de staat of van zijn bondgenoten wordt geboden, een voorwerp waaraan een zodanige inlichting kan worden ontleend, of zodanig gegevens opzettelijk verstrekt aan of ter beschikking stelt van een tot kennisneming daarvan niet gerechtigd persoon of lichaam, wordt, indien hij weet of redelijkerwijs moet vermoeden dat het een zodanige inlichting, een zodanig voorwerp of zodanige gegevens betreft, gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.

-2. Met dezelfde straf wordt gestraft hij die een inlichting die van een verboden plaats afkomstig is en tot de veiligheid van de staat of van zijn bondgenoten in betrekking staat, een voorwerp waaraan een zodanige inlichting kan worden ontleend, of zodanige gegevens opzettelijk verstrekt aan of ter beschikking stelt van een tot kennisneming daarvan niet gerechtigd persoon of lichaam, indien hij weet of redelijkerwijs moet vermoeden dat het een zodanige inlichting, een zodanig voorwerp of zodanige gegevens betreft.

Art. 98a.-1 Hij die een inlichting, een voorwerp of gegevens als bedoeld in artikel 98, hetzij opzettelijk openbaar maakt, hetzij zonder daartoe gerechtigd te zijn opzettelijk aan of ter beschikking stelt van een buitenlandse mogendheid, een in het buitenland gevestigd persoon of lichaam, dan wel een zodanig persoon of lichaam dat

gevaar ontstaat dat de inlichting of de gegevens aan een buitenlandse mogendheid of aan een in het buitenland gevestigd persoon of lichaam bekend wordt, indien hij weet of redelijkerwijs moet vermoeden dat het een zodanige inlichting of zodanige gegevens betreft, wordt gestraft met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie.

-2. Indien de schuldige heeft gehandeld in tijd van oorlog dan wel in dienst of in opdracht van een buitenlandse mogendheid of van een in het buitenland gevestigd persoon of lichaam, kan levenslange gevangenisstraf of tijdelijke van ten hoogste twintig jaren of geldboete van de vijfde categorie worden opgelegd.

-3. Handelingen gepleegd ter voorbereiding van een misdrijf als omschreven in de voorgaande leden worden gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.

Art. 98b. Hij aan wiens schuld te wijten is dat een inlichting, een voorwerp of gegevens bedoeld in artikel 98, openbaar worden gemaakt of ter beschikking komt van een tot kennisneming daarvan niet gerechtigd persoon of lichaam, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

Art. 98c.-1. Met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie wordt gestraft:

1. hij die opzettelijk een inlichting, een voorwerp of gegevens als bedoeld in artikel 98, zonder daartoe gerechtigd te zijn, onder zich neemt of houdt;

2. hij die enige handeling verricht, ondernomen met het oogmerk om, zonder daartoe gerechtigd te zijn, de beschikking te krijgen over een inlichting, een voorwerp als bedoeld in artikel 98;

3. hij die tersluiks, onder een vals voorgeven, door middel van een vermomming of langs een andere dan de gewone toegang op of in een verboden plaats komt of tracht te komen, aldaar in dier voege aanwezig is, of zich op een van die wijzen of door een van die middelen vandaar verwijdt of tracht te verwijderen.

-2. De bepaling onder 3 is niet toepasselijk, indien de rechter blijkt dat de dader niet heeft gehandeld met het oogmerk bedoeld onder 2.

Art. 272.-1. Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

-2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

Art. 273.-1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die opzettelijk

1. aangaande een onderneming van handel, nijverheid of dienstverlening bij welke hij werkzaam is of is geweest, bijzonderheden waarvan hem geheimhouding is opgelegd, bekend maakt of

2. gegevens die door misdrijf zijn verkregen uit een geautomatiseerd werk van een onderneming van handel, nijverheid of dienstverlening en die betrekking hebben op deze onderneming, bekend maakt of uit winstbejag gebruikt, indien deze gegevens ten tijde van de bekendmaking of het gebruik niet algemeen bekend waren en daaruit enig nadeel kan ontstaan.

-2. Niet strafbaar is hij die te goeder trouw heeft kunnen aannemen dat het algemeen belang de bekendmaking vereiste.

-3. Geen vervolg heeft plaats dan op klacht van het bestuur van de onderneming.

Art. 463 De ambtenaar die zonder verlof van het bevoegd gezag afschrift maakt of uittreksel neemt van geheime regeringsbescheiden of die openbaar maakt, wordt gestraft met hechtenis van ten hoogste twee maanden of geldboete van de tweede categorie.

Bijlage 40.2

Verklaring van ontheffing uit een crypto functie

Ondergetekende: _____ (naam en voorletters)

Geboren op: _____ te _____

Ontheven uit de functie van: _____

verklaart,

dat ik de gerubriceerde en / of CRYPTO, CRYPTO-SECURITY of CCI-gemerkte informatie, die in de uitoefening van mijn functie te mijner kennis zijn gekomen, niet zal onthullen aan niet-gerechtigden;

dat ik besef, dat ik na beëindiging van het dienstverband dan wel de arbeidsovereenkomst onderworpen blijf aan de wettelijke en andere voorschriften inzake de geheimhouding van informatie en aan de in die voorschriften gestelde sancties op schending van de geheimhoudingsplicht;

dat ik geen gerubriceerde en / of CRYPTO, CRYPTO-SECURITY of CCI-gemerkte Documenten of materialen die mij in mijn functie ter beschikking zijn gesteld, meer onder mijn berusting heb.

Plaats : _____

Datum : _____

Handtekening : _____

Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst
Bureau Industrieveiligheid