

Ongerubriceerd en ongemeekt

ABDO

Ministerie van Defensie

Regelmatig blijkt dat buitenstaanders grote interesse hebben in kennis, informatie, materieel, goederen en objecten van het Ministerie van Defensie en de kennisinstututen en bedrijven die voor Defensie werken. Onoerbare 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 bedrijfsseigen "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

Inleiding.....	10
Eisen	11
Inleiding	17
Eisen	18
Inleiding.....	21
Eisen 22	
Inleiding.....	33
Eisen	34

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: risico = kans x 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. *BLV / 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 Staatsgeheimen en niet-Staatsgeheimen *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-Staatsgeheimen *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 *B1* genoemd. Opgemerkt wordt dat, in tegenstelling tot *B1*, een *TBB* niet gerubriceerd hoeft te zijn.

NL <i>Rubricering</i>	<i>TBB</i> 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;

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

- 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.

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 gedeponeerd 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.

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. *BI* / *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 *BI* / *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 Gerubriceerde Opdracht.	Procedure ABDO	●	●	●	●
2	Bij beëindiging van het contract vervallen alle bijbehorende autorisaties, de LvV en de VGB. 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.	Procedure ABDO	●	●	●	●
1.2	Inrichten van de beveiligingsorganisatie	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	Opdrachtnemer beschikt over een organisatiebreed, structureel gehandhaafd en breed gedragen beveiligingsbeleid, bekrachtigd door het hoogste bestuursorgaan.	Bijlage 3	●	●	●	●
2	Opdrachtnemer beschikt over een beveiligingsplan, opgesteld door de BF, goedgekeurd door BIV / MIVD en ondertekend door het hoogste bestuur, waarin de beveiligingseisen uit de ABDO 2017 zijn uitgewerkt in duidelijke, hanteerbare maatregelen en procedures.	Bijlage: 3	●	●	●	●
3	Opdrachtnemer heeft de in het beveiligingsplan beschreven maatregelen en procedures eenduidig geïmplementeerd in de organisatie.	Bijlage 3	●	●	●	●
4	Opdrachtnemer heeft, met voorafgaande schriftelijke instemming van BIV / MIVD, een beveiligingsfunctionaris (BF) benoemd en zonodig één of meerdere sub-BF'n, afhankelijk van de omvang van de BO, het aantal betrokken locaties en specialisten.	Bijlage 3	●	●	●	●

5	De BF 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 BF 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 BF 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 BF draagt zorg voor volledige medewerking bij controles, audits en onderzoeken bij <i>Opdrachtnemer</i> door BIV / MIVD.	Bijlage 4	●	●	●	●
6	De BF 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 BF voert voorts de taken uit als beschreven in bijlage 4: Taken en verantwoordelijkheden BF.	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, <i>Zeggenschap</i> 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 <i>Zeggenschap</i> , 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 screenen (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>) <i>Bijzondere Informatie (BI)</i> is overgedragen.	Bijlage 5	●	●	●	○

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

2	Na toestemming van BIV / MIVD tot uitbesteding heeft <i>Opdrachtnemer</i> in het contract met <i>Subcontractors</i> die in aanraking komen met een TBB, de ABDO 2017 bedongen. Een ingevulde RAL is hierbij verstrekt aan BIV / MIVD.	Bijlage 8	●	●	●	●	●
3	Na toestemming van BIV / MIVD (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 TBB, de in het betrokken land geldende beveiligingseisen bedongen. Een ingevulde RAL is hierbij verstrekt aan BIV / MIVD.	Procedure ABDO	●	●	●	●	●
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 ABDO 2017 bedongen.	Bijlage 8	○	○	○	○	○
5	Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan een BO zijn de werkzaamheden aan een TBB zoveel mogelijk gecentraliseerd. (<i>Opdrachtnemer</i> draagt de verantwoordelijkheid voor het voldoen aan de eisen van ABDO 2017 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 BO vooraf aan BIV / MIVD voor toestemming. Voor inschakeling van een buitenlands bedrijf is toestemming van <i>Opdrachtgever</i> en autorisatie door BIV / MIVD vereist.	Bijlage 8	●	●	●	●	●
1.8	Pers, internet, sociale media, publicatie, opnamen, etc.	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB4/DV	
1	<i>Opdrachtnemer</i> en zijn medewerkers maken zonder uitdrukkelijke voorafgaande toestemming van <i>Opdrachtgever</i> en BIV / MIVD op geen enkele wijze publiekelijk bekend welke BO zij voor de Nederlandse overheid, buitenlandse overheid en/of NAVO / EU uitvoeren.	Bijlage 3 / 6	●	●	●	●	●
2	Het maken van opnamen van een TBB, anders dan noodzakelijk voor de uitvoering van de BO, is ongeacht het middel, niet toegestaan zonder voorafgaande schriftelijke goedkeuring van de <i>Opdrachtgever</i> in overleg met BIV / MIVD.	Bijlage 6	●	●	●	●	●
3	<i>Opdrachtnemer</i> en zijn medewerkers maken contactgegevens en afspraken met de MIVD 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 Incident Response Procedure (IRP) opgesteld voor het behandelen van Beveiligingsincidenten. Deze is bekend bij allen die werken aan of toegang hebben tot een TBB.	Bijlage 9	●	●	●	●
2	Beveiligingsincidenten dienen binnen de normstelling genoemd in tabel "Classificatie" met behulp van de IRP aan BIV / MIVD te zijn bekend gesteld.	Bijlage 9	●	●	●	●
3	Gegevens t.a.v. toegang tot en inzicht in een TBB zijn vastgelegd en worden gedurende de aangegeven periode bewaard om achteraf onderzoek naar vermoede Beveiligingsincidenten mogelijk te maken.	Bijlage 9	6 maanden	6 maanden	3 maanden	3 Maanden
4	Informatie aangaande vastgestelde Beveiligingsincidenten wordt gedurende de aangegeven periode door de BF 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 BF 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 Beveiligingsincidenten.		●	●	●	●

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.

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 *VOG*. 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 voortdurende

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 Lijst van Vertrouwensfuncties (LvV) vastgesteld door de MIVD.	Bijlage 10	●	●	●	○	
2	Veiligheidsonderzoeken worden aangevraagd 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	Opdrachtnemer plaatst slechts medewerkers met de Nederlandse nationaliteit op <i>Vertrouwensfuncties</i> waarbij toegang tot een grote hoeveelheid BI (te bepalen door BIV / MIVD in overleg met <i>Opdrachtgever</i>) is vereist.	Bijlage 13	●	●	●	●
13	Een overzicht van alle de VGB, de VOG en verklaringen van bekendheid met de geheimhoudingsplicht is bij de BF aanwezig.	Bijlage 4	●	●	●	●
2.2	Geheimhoudingsverklaring	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	De BF 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 functionaris 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 Vertrouwensfunctie	Verwijzing	TBB 1/ZG	TBB 2/G	TBB 3/C	TBB 4/DV
1	De BF meldt ontheffing uit een <i>Vertrouwensfunctie</i> aan BIV / MIVD 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 BF heeft een toelichting gegeven op de ontheffingsverklaring, de (kopie) VGB ingenomen en zeker gesteld dat de medewerker geen TBB 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 BF passende maatregelen	Bijlage 15	●	●	●	○

	te nemen en BIV / MIVD hierover te informeren.						
	Grove nalatigheid of bewuste <i>Compromittatie van Staatsgeheime of 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 BO onverwijld gemeld aan de BF.	Bijlage 16	●	●	●	○	
2	Een <i>Vertrouwensfunctionaris</i> heeft een voorgenomen reis naar een risicoland onverwijld gemeld aan de BF.	Bijlage 16	●	●	●	○	
3	Indien bij een zakelijke reis een <i>Request for Visit</i> benodigd is, dient de <i>Vertrouwensfunctionaris (RFV)</i> , via de BF, een (elektronische) RFV ter goedkeuring in bij BIV / MIVD. Zonder goedgekeurd RFV kan de reis niet plaatsvinden.	Bijlage 16	●	●	●	○	
4	De BF brieft en debrieft <i>Vertrouwensfunctionarissen</i> die voorgenomen reizen naar risicolanden aan de BF hebben gemeld.	Bijlage 16	●	●	●	○	
5	De BF meldt aan BIV / MIVD 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 BF meldt, d.m.v. het formulier in bijlage 16 , aan BIV / MIVD zakelijk reizen en/of privéverblijf van een <i>Vertrouwensfunctionaris</i> naar of resp. in een risicoland.	Bijlage 16	●	●	●	○	

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 *Uitstel/tijd* 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. *Uitstel/tijd* 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 *Uitstel/tijd* 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. *B/V* / *M/VD* 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 *B/V* / *M/VD* 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 Authentication</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</i> / <i>MIVD</i> verstrekt.	Bijlage 18	●	●	●	●	●
14	Toegang tot een compartiment met een <i>TBB</i> door bezoekers zonder <i>Autorisatie</i> die niet beschikken over de Nederlandse nationaliteit is minimaal vijf werkdagen voor het bezoek gemeld via de <i>BF</i> aan <i>BIV</i> / <i>MIVD</i> . Zonder toestemming van <i>BIV</i> / <i>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 Authentication</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 "Clear Desk principe" en "clear screen 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 Signaleringsstelsel (IDS)</i> is geactiveerd. Tevens is een controle op insluipen 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	Compartmenten 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 streekmetaal 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 streekmetaal 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 TBB of een opbergmiddel met een TBB 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 TBB 4.	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 Authentication</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 TBB staat een terreinafscheiding met toegangscontrole.	Bijlage 19	●	●	●	●
19	Er is beveiligingsverlichting toegepast rondom het gebouw met een TBB.	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 TBB zijn voorzien van inijk 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 TBB is geplaatst, is voorzien van een IDSS.	Bijlage 20	●	●	●	
2	De aanliggende compartimenten van het compartiment met een TBB zijn voorzien van IDSS of een opbergmiddel met een TBB is zelf voorzien van IDSS.	Bijlage 20	●	●	●	
3	Het activeren en deactiveren van een IDSS kan alleen door middel van een Two-factor Authenticatie.	Bijlage 20	●	●	●	
4	Het IDSS functioneert 24 uur per dag en 7 dagen per week, tenzij Geautoriseerd personeel aanwezig is in het compartiment.	Bijlage 18/20	●	●	●	
5	IDSS-onderdelen zijn zodanig geplaatst dat Compromittatie van een TBB of pogingen daartoe worden ontdekt en een alarm genereren.	Bijlage 20	●	●	●	
6	De ruimte met een TBB is binnen het IDSS als aparte zone opgenomen. Deze zone is actief wanneer er geen Geautoriseerd personeel is in de ruimte.	Bijlage 18/20	●	●	●	
7	Doormelding van een IDSS voldoet aan de kwaliteit zoals gesteld in bijlage 19.	Bijlage 19	●	●	●	
8	Een alarm van een IDSS leidt tot een alarmopvolging binnen de in bijlage 21 gestelde Interventie tijd.	Bijlage 21	●	●	●	
9	Het IDSS signaleert en registreert uitval van de stroomvoorziening van de IDSS.	Bijlage 20	●	●	●	
10	Het IDSS beschikt over een gegarandeerde stroomvoorziening.	Bijlage 20	●	●	●	
11	Het IDSS is niet onopgemerkt te saboteren c.q. een Compromittatie 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 TBB. 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 (ETS of IDSS) 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 IDSS en het ETS 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 TBB terstond de BF.	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 TBB plaats door de BF of diens gemandateerde.	Bijlage 21	●	●	●	○
7	Alarmverificatie vindt aan de buitenzijde van het compartiment met een TBB 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 TBB.	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 TBB wordt uitsluitend buiten het compartiment gebracht als dit voor de voortgang van de werkzaamheden absoluut noodzakelijk is.	Bijlage 22	●	●	●	●
2	De BF stelt conform bijlage 22 voorschriften op voor het transporteren en verzenden van een TBB en houdt hier toezicht op.	Bijlage 22	●	●	●	●

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

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

6	BI is geregistreerd en van een uniek exemplaarnummer voorzien.	Bijlage 23	•	•	•	
7	<i>Rubriceringen en Merkingen</i> 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	•	•	•	•

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.

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

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 Informatiebeveiliging						
1	Er is beleid ten aanzien van cybersecurity.		○	○	○	○	
4.2	Organiseren van Informatiebeveiliging	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV	
4.2	Interne organisatie						
1	Er is een <i>Cyber Beveiligingsfunctionaris (Cyber-BF)</i> aangesteld. De <i>Cyber-BF</i> heeft, net als de <i>BF</i> , rechtstreeks toegang tot de Directie van de organisatie. De <i>Cyber-BF</i> kan deeltaken door derden binnen de organisatie laten uitvoeren.	Bijlage 24	●	●	●	●	
2	De <i>Cyber-BF</i> is namens de directie bevoegd tot het (laten) nemen van gepaste beveiligingsmaatregelen op het gebied van <i>Cyber-security</i> .	Bijlage 24	●	●	●	●	
3	De <i>Cyber-BF</i> houdt, namens de directie, toezicht op een veilige inrichting van de digitale infrastructuur binnen de organisatie.	Bijlage 24	●	●	●	●	
4	De <i>Cyber-BF</i> verstrekt de aan de organisatie toebehorende externe IP adressen en domeinnamen aan <i>BIV / MIVD</i> .	Bijlage 24	●	●	●	●	
5	De <i>Cyber-BF</i> 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 <i>TBB</i> .	Bijlage 24	●	●	●		
6	De <i>Cyber-BF</i> heeft te allen tijde inzicht in de gebruikte digitale <i>TBB</i> .	Bijlage 24				●	
7	De <i>Cyber-BF</i> voert voort de taken uit als beschreven in de bijlage.	Bijlage 24	●	●	●	●	
8	De <i>Cyber-BF</i> draagt zorg voor volledige medewerking bij controles van, audits op en onderzoeken aan de IT infrastructuur van de <i>Opdrachtnemer</i> door <i>BIV / MIVD</i> .	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 BIV / MIVD goedgekeurde Vercijfering 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 TBB 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 BIV / MIVD goedgekeurde oplossing(en) en middelen.								●
4.3	Veilig personeel								
4.3	Bewustzijn, opleiding en training ten aanzien van Informatiebeveiliging								
1	Het personeel dat betrokken is bij de behandeling van een TBB 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, Cyber-BF, IT-beheer en het overige personeel dat betrokken is bij de behandeling van een digitale TBB 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								
4.4	Inventariseren van ICT-bedrijfsmiddelen								
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 ICT-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	Systeemdokumentatie, 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	Verwijderbare Gegevensdragers 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 BIV / MIVD.		●	●	●	●	
4	In het Beveiligingsplan is beschreven op welke wijze gebruikers toegang hebben.		●	●	●	●	
5	Er is een basisadministratie van authenticatiegegevens van gebruikers, op basis waarvan de gebruikers vooraf zijn geïdentificeerd en geautoriseerd.		●	●	●	●	
4.5	Toegang tot netwerken en netwerkdiensten						
6	Beheer op afstand 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	Beheer op afstand van apparatuur is alleen toegestaan indien gebruik is gemaakt van door BIV / MIVD 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 privilegieniveau 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	Beheeren van speciale toegangsrechten							
14	Gebruikers hebben alleen bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is ("Need-to-know", "need-to-use").							
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.							

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 TBB-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 Cyber-BF 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 Cyber-BF 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 Cyber-BF 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</i> , <i>Authenticatie</i> - en autorisatiemechanisme hebben.							
51	Het is niet toegestaan om gebruik te maken van groepsaccounts.							

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 voort 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 TBB bevindt, zijn geplaatst in een ruimte die op TBB 4 niveau is beveiligd.	Bijlage 32							●
2	Systemen waarop zich een grote concentratie van TBB van Departementaal Vertrouwelijk bevindt, zijn geplaatst in een ruimte die op TBB 3 niveau is beveiligd.	Bijlage 32							●
3	Systemen waarop zich een grote concentratie van TBB van STG Confidentieel bevindt, zijn geplaatst in een ruimte die op TBB 2 niveau is beveiligd.	Bijlage 32						●	
4	Systemen waarop zich een grote concentratie van TBB van STG Geheim bevindt, zijn geplaatst in een ruimte die op TBB 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 TEMPEST maatregelen genomen. De maatregelen zijn vooraf afgestemd met BIV / MIVD.	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 BIV / MIVD 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 TBB 1, TBB 2 en TBB 3 systemen geeft de Cyber-BF toestemming. Bij TBB 4 systemen de lijnmanager.					●		●	●
4.7	Veilig verwijderen of hergebruiken van apparatuur								
10	Hergebruik van ICT-bedrijfsmiddelen is toegestaan mits het dezelfde TBB betreft en is gewist door gebruik te maken van de door BIV / MIVD 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 TBB opbergt op de daartoe bestemde plaats indien men de Informatie niet gebruikt. Deze informatie is altijd opgeborgen in een afsluitbare opbergmogelijkheid van het juiste TBB niveau.		•	•	•	•	•
13	Bij het afdrukken van een TBB op een printer in een andere ruimte dan het werkstation is gebruik gemaakt van de functie "beveiligd afdrukken" (bijvoorbeeld pincode verificatie).		•	•	•	•	•
14	Een werkplek (sessie) is voor (TBB1 en 2 na:5, TBB3 na:10, TBB4 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 ingesteld als er een grote operationele noodzaak is; - voordat een schermbeveiliging wordt uitgezet of ingesteld moet hiervoor toestemming verleend worden door de Cyber-BF; - de Cyber-BF onderhoudt een registratie van werkplek (sessie) en de noodzaak waarom ontheffing is gegeven.		•	•	•	•	•
4.8	Beveiliging bedrijfsvoering	Verwijzing	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV	
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 TBB 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 Cyber-BF is daarin opgenomen.		•	•	•	•	•
6	Instellingen van informatiebeveiligingsfuncties (b.v. securitysoftware) op het koppelvlak tussen vertrouwde en onbetrouwbare netwerken, zijn automatisch op wijzigingen gecontroleerd.		•	•	•	•	•
4.8	Capaciteitsbeheer						
7	Op basis van een risicoanalyse is bepaald wat de beschikbaarheidsis 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 Malware								
16	Bij het openen van bestanden zijn deze geautomatiseerd gecontroleerd op Malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, plaats.								
17	Inkomende en uitgaande e-mails zijn gecontroleerd op Malware. 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 Malware. Bij het aantreffen van Malware zijn deze in quarantaine geplaatst.								
19	In verschillende schakels van een keten binnen de infrastructuur van een organisatie is anti-Malware programmatuur van verschillende leveranciers toegepast.								
20	Er zijn maatregelen getroffen om verspreiding van Malware tegen te gaan en daarmee schade te beperken (bijv. quarantaine en Compartmentering).								
21	Er zijn continuïteitsplannen voor herstel na aanvallen met Malware 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 Scrubber-functionaliteiten.								
23	Afwijkingen van het normbeeld (anomalies) met betrekking tot sessies door perimeter devices zijn onderzocht op dreigingen zoals "covert channels". Monitoring op ongebruikelijke creaties, aanwezigheid en/of beëindiging van								

		processen teneinde infiltratie te onderkennen, vindt continu plaats.							
4.8		Back-up van informatie							
24		Er zijn geteste procedures voor back-up en recovery van informatie voor herinrichting en fourterstel 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 een 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 Monitoring systems ingericht die tenminste Packet Headers 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 Monitoring toegepast.					●
13	Een netwerkbased IDS of IPS is voorzien van actuele Signatures.					●
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 DMZ Proxy-server en/of sandbox toegepast.	Bijlage 35				●
4.9	Scheiding in netwerken					
16	Een netwerk waarop TBB zijn opgeslagen, heeft geen verbinding met een ander netwerk, tenzij door BIV / MIVD goedgekeurde procedures en middelen zijn toegepast.		●	●	●	
17	De Technische Infrastructuur 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 Malware 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 (Compartmentering) op basis van "Need-to-be", "Need-to-know" en "least privilege" principes.		●	●	●	●
4.9	Beleid en procedures voor informatietransport					
24	Alle TBB die zich niet binnen het daarvoor bestemde fysieke compartiment bevindt is vercijferd. De toe te passen Vercijfering is goedgekeurd door BIV /		●	●	●	●

	MIVD.							
25	Een TBB is alleen verzonden over een onbeveiligde verbinding wanneer door BIV / MIVD 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 Leverancier via een gescheiden kanaal geleverde checksum of certificaat.			●		●		●
27	Ontsluiting van TBB op een netwerk tussen verschillende bedrijfslocaties (WAN) is niet toegestaan.			●				
28	Ontsluiting van TBB op een netwerk tussen verschillende bedrijfslocaties (WAN) is alleen toegestaan indien de verbinding tussen de locaties van een door BIV / MIVD 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 Private Cloud-dienst (computing, opslag, transport) is toegestaan.	Bijlage 8						○
31	Private Cloud-dienst (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 / MIVD.	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 / MIVD.	Bijlage 34		●		●		●
4.10	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Verwijzing						
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. 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.		●	●	●	●	●	●
4			●	●	●	●	●	●
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	TBB 1 / ZG	TBB 2 / G	TBB 3 / C	TBB 4 / DV		
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	●	●	●	●	●	●

	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. 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.
Bedrijfsmiddel	Het extern uitvoeren van beheerwerkzaamheden op apparatuur intern de organisatie.
Beheer op afstand	De waarborg dat vanuit hun functie geautoriseerde gebruikers of systemen op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
Beschikbaarheid	De mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening. (VIR 94)
Betrouwbaarheid	Het beschermen van een TBB, BI in het bijzonder, tegen toegang of kennisname door niet-gerechtigden.
Beveiligen	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuity Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiliging	Beveiligingsfunctionaris (BF). De functionaris die is belast met de implementatie en uitvoering van de voorgeschreven beveiligingsmaatregelen.
Beveiligingsfunctionaris	

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

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	Broncode	Een computerprogramma in leesbare vorm zoals die door de programmeur in een programmeertaal is geschreven.
Beveiligingsplan	Opsomming van alle getroffen beveiligingsmaatregelen en/of de vindplaatsen daarvan welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht zijn. Een verzameling van technische beheersingsmaatregelen of instellingen voor de inrichting van een IT-middel gericht op een specifieke IT-dienst	BIV / MIVD	Bureau Industrieveiligheid (BIV) van de MIVD dat namens Defensie toeziet op de beveiliging van TBB bij Opdrachtnemers en de onderaannemers hiervan.
Beveiligingsstandaard	Een bilateraal verdrag dat de uitwisseling en wederzijdse bescherming van gerubriceerde informatie tussen twee landen faciliteert. 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 een of meer ministeries. Bijzondere Informatie(BI) is informatie die voorzien is van een Rubricering en op grond daarvan moet worden beveiligd.	BYOD / CYOD	Bring Your Own Device. De mogelijkheid voor een medewerker eigen apparatuur te gebruiken voor zakelijke toepassing
Beveiligingsverdrag	Bijzondere Opdracht. Een opdracht vanuit de overheid als Opdrachtgever aan een civiele partij als Opdrachtnemer waarbij een TBB betrokken is. Een zwarte lijst met bijvoorbeeld domeinen of IP adressen waarmee geen digitale communicatie mag plaatsvinden.	CA / RA	Choose Your Own Device. De mogelijkheid voor een medewerker te kiezen uit een aantal door het bedrijf aangeboden apparaten. Certificaat Autoriteit. De CA waarborgt de integriteit en authenticiteit van certificaten en garandeert de identiteit van de certificaatbezitter.
Bijzondere Informatie		CCTV	Registratie Autoriteit. De RA stelt vast aan wie een certificaat kan worden verstrekt en controleert de uitgifte ervan Closed Circuit Television. Een gesloten systeem van camera's als hulpmiddel bij het voorkomen en verwerken van incidenten.
BO		Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt. Het via een netwerk, op aanvraag beschikbaar stellen van hardware, software en gegevens.
Blacklist		Cloudcomputing	Software die ondersteunt bij het vinden van fouten in de broncode van software.
		Code Security Review	Infrastructuur (servers en andere componenten), als
		Command & Control (C2)	

server	doelwit gebruikt om Malware aan te verspreiden en/of deze aan te sturen, in het bijzonder botnets of APT's.	Cyber	een zekere mate van beveiliging vereist. 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).
Compartmentering	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.	Darknet	Deel van het World Wide Web waarvan de inhoud alleen met behulp van specifieke software (browser) en/of configuraties toegankelijk is.
Compromittatie	De ongeautoriseerde toegang tot of kennisname van een TBB, meestal BI.	DBB	Het Defensie Beveiligingsbeleid zoals omschreven in aanwijzing SG/003.
Configuration Item (CI)	IT-middel dat van belang is voor een te leveren IT-dienst	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.
COTS	Commercial of the Shelf. Een term om commerciële goederen en diensten aan te duiden die direct op de markt beschikbaar zijn.	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 webserver).
Cryptofunctie	Een vertrouwensfunctie waarin behandeling van of kennisname van CRYPTO, CRYPTO-SECURITY of CRYPTO CONTROLLED ITEM (CCI)-gemarakt materiaal noodzakelijk is.	DV	Departementaal Vrouwelijke Informatie is Bijzondere Informatie met de laagst mogelijke rubricering. DV wordt niet als Staatsgeheim aangemerkt maar behoeft wel een bepaald niveau van beveiliging.
CUI	Controlled Unclassified Information / Item. Een categorie informatie of goederen die in het kader van de Amerikaanse ITAR, hoewel ongerubriceerd,	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.	ETS	Elektronisch Toegangsbeheer Systeem.
		EU	Europese Unie.
Dienstverlener (service provider)	Een bedrijf dat diensten aanbiedt. De term service provider wordt vaak geassocieerd met internet- en telefoniediensten.	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 laatsgenoemde te verhogen.
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.	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.
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.).	FTP	File Transfer Protocol. Een protocol dat uitwisseling van bestanden tussen computers faciliteert.
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.	Gerubriceerde Opdracht	Een Defensieopdracht waarbij Bijzondere Informatie ter kennis van een externe organisatie moet worden gebracht of daarbij wordt gegenereerd.
	Zie Vercijfering.	Geheimhoudings- verklaring	De verklaring waarin men aangeeft bekend te zijn met voorschriften en verplichtingen aangaande het omgaan met een TBB, BI in het bijzonder.
	Een betrouwbare derde partij waar sleutels of Broncode zijn opgeslagen.	Goederen	Alle materiële en immateriële zaken (producten en diensten) die kunnen worden gebruikt om in behoeften te voorzien.
Encryptie		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.
Escrow Agent		Honeypot of Honeynet	Een computersysteem of -netwerk dat zich bewust

Hypervisor	kwetsbaar opstelt voor (worm)virussen en andere aanvallen, zodat de aanvaller en/of zijn eigenschappen zichtbaar worden. Een opstelling (software) die ertoe dient om meerdere besturingssystemen tegelijkertijd op een hostcomputer te laten draaien.	Integriteit	informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie. Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan.
Identificatie	Het kenbaar maken van de identiteit van een subject (een gebruiker of een proces).	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.
IDS(S)	Indringer Detectie en Signalering (Systeem).	Interventietijd	De tijd tussen detectie/verificatie van een poging tot inbraak en het ter plaatse ingrijpen door de bewaking, politie of defensiepersoneel.
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")	Introspectieve Capaciteit	Het vermogen van een IDS om de interne activiteiten van een systeem (netwerk) op legitimiteit te beoordelen en zonodig actie te ondernemen.
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.	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.
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.	IRP	Incident Response Procedure. Een procedure waarin is opgenomen welke stappen in onderzoek en afhandeling moeten worden uitgevoerd als een Incident wordt gemeld.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het	ITAR ICT-Bedrijfsmiddelen	International Traffic of Arms Regulations. 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

Logging	voor geld. 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

NAVO	dan alleen het enkele publiek bekende IP-adres zichtbaar is.
NBV	Noord Atlantische Verdrags Organisatie. 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 vrouwde 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

Opdrachtnemer	rechtspersoon of een buitenlandse instantie die een Bijzondere Opdracht (BO) verstrekt.		
OPG	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.	Penetratietest	software uitgeeft om fouten aan door hem vervaardigde software te repareren
Packet Headers	Opgave Persoonlijke Gegevens op basis waarvan een Veiligheidsonderzoek wordt uitgevoerd.	Phishing	Een toets op kwetsbaarheden van een of meerdere computersystemen met als doel de systemen beter te beveiligen.
Partner	Data die aan het begin van een digitaal blok is geplaatst, benodigd voor interpretatie van de te transporteren data.	Private Cloud-dienst	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.
Patch	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. Onderdeel van software dat de leverancier van	Privileged Accounts	Een vorm van Cloud-computing waarbij, op specifiek toegewezen (geïsoleerde) hard- en software, gegevens beschikbaar worden gesteld aan de opdrachtnemer.
			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.	Security MoU	deze zonnig onschadelijk maakt. Memorandum of Understanding. Een bilaterale overeenkomst tussen partijen waarin wederzijdse beveiligingsafspraken zijn vastgelegd.
PSI	Project Security Instruction. Een Document waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van een buitenlandse opdracht.	SG	De Secretaris-generaal van het betrokken ministerie.
Rijksdienst	De ministeries met hun directoren-generaal, centrale en stafdirecties, buitendienst en intern verzelfstandigde dienstonderdelen.	Signatures	Eigenschappen van Malware op basis waarvan herkenning kan plaatsvinden.
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.	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.
Rubricering	Het vaststellen en aangeven dat een TBB Bijzondere Informatie is of bevat, alsmede het bepalen en aangeven van de mate van beveiliging daarvan.	Staatsgeheim	Bijzondere Informatie waarvan de geheimhouding vanwege het belang van de Staat of zijn bondgenoten is geboden.
RAL	Rubriceringsaanduidingslijst. Een lijst die in het kader van een BO per onderwerp de rubricering van het daarop betrekking hebbende TBB aangeeft.	Staat Van Inlichtingen (SVI)	Staat van Inlichtingen op basis waarvan een Veiligheidsonderzoek wordt uitgevoerd.
RfV	RequestforVisit. Het verzoek aan de betrokken veiligheidsautoriteiten om toestemming voor een bezoek aan een defensielocatie of een bedrijf in het buitenland.	Subcontractor	Een bedrijf waaraan de Opdrachtnemer bepaalde werkzaamheden aan een TBB uitbesteed.
SAL	Security Aspect Letter. Een Document waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van kleinere buitenlandse projecten.	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).
Screening Scrubber	Zie Veiligheidsonderzoek. Een standalone systeem dat informatiedragers controleert op de aanwezigheid van Malware en	Technische Infrastructuur	Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkkapitaal, besturingssystemen voor netwerken en servers, database

Toeleverancier	management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden. Een bedrijf dat goederen levert aan een ander bedrijf dat die Goederen op zijn beurt verwerkt in een door de eindgebruiker gewenst product.	autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken.
TEMPEST	Het tegengaan van mogelijk compromitterende emissie van elektronische systemen die kan leiden tot het onbevoegd opvangen, verwerken en reproduceren van data.	Informatie die niet algemeen bekend mag worden (bron: van Dale)
Two-factor authenticatie	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).	In het kader van de BIR:2012 worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met departementaal vrouwelijk (volgens definitie uit VIRBI) en persoonsvrouwelijke informatie van risicoklassen 1 en 2 zoals gedefinieerd de toelichting op de WBP: AV23 Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Spanpoort	Een fysieke poort op een actieve component (router of switch) die het mogelijk maakt diagnose op een apparaat of netwerkverkeer te verrichten	Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CRDROMs, USB sticks, verwijderbare schijven, tapes of gedrukte media.
Uitsteltijd	De tijd tussen detectie/verificatie van een inbraak en Compromittatie van een TBB.	Een functie die in beginsel de mogelijkheid biedt de veiligheid of andere gewichtige belangen van de Staat te schaden.
unPrivileged accounts	Een gebruikersaccount dat over beperkt rechten beschikt zoals bijvoorbeeld; - Gebruiker accounts	Een persoon die op een vertrouwensfunctie geplaatst is.
Veiligheidsonderzoek	Het proces dat leidt tot afgifte, weigering, verlenging of intrekking van een VGB.	Een voorlichting met als doel het beveiligingsbewustzijn te vergroten.
Vercijfering	Het door middel van een algoritme zodanig wijzigen van informatie dat deze onleesbaar en onbegrijpelijk is voor niet-gerechtigden.	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.
Vertrouwd(e)	In overeenstemming met een door een bevoegde	Veiligheidsmachtingsniveau. Het voor de Vertrouwensfunctie vereiste niveau waarop het

Virtualisatie	Veiligheidsonderzoek moet worden uitgevoerd (A, B dan wel C). 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.	(Wiv) Wet veiligheidsonderzoeken (Wvo) Wetboek van strafrecht (Wvsv)	rechtsoptolger. De Wet veiligheidsonderzoeken zoals gepubliceerd 1996 (zie stb. 1996, 525) en gewijzigd in 2015 (zie stb. 2015, 208). 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.
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.	Wijziging Zeggenschap	Elke toevoeging, verandering of verwijdering in een IT-dienst of IT-middel. 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.
Voorlopige autorisatie	De verklaring van BIV / MIVD aan de Opdrachtgever dat er vanuit beveiligingsoogpunt geen bezwaar bestaat tegen een bedrijf als kandidaat Opdrachtnemer.	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.
VPN	Virtual Private Network. Een versijferde verbinding tussen twee systemen, waarbij de integriteit en de vertrouwelijkheid van de data gewaarborgd blijft.	Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen
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		

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	Systeemdocumentatie
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 (<i>GERUBRICEERD</i>)
40	Cryptofunctionaris

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

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.

Algemene Beveiligingseisen Defensie Opdrachten 2017

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.

Algemene Beveiligingseisen Defensie Opdrachten 2017

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 *Merkingen* gekoppeld aan *TBB*-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 ("Need-to-Know").
PERONEELS- VERTROUWELIJK	TBB 4	Aangebracht op <i>Informatie</i> met persoonsgegevens. Kennisname door niet-gerechtigden kan de belangen van een persoon schaden.
COMMERCIEEL 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.

Algemene Beveiligingseisen Defensie Opdrachten 2017

Bijlage 2

Tabel buitenlandse Rubriceringen

Nederland	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Departementaal 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 ΑΠΟΡΡΗΤΟ	ΑΠΟΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΟ	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ
<i>Denemarken</i>	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG

¹ Canada gebruikt geen equivalente *Rubricering*. Canada behandelt en beveilgt 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 TERJESZTÉÜ!
Ierland	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Island	ALGERT LEYNDARMAL	LEYNDARMAL	TRUNADARMAL	THJONUSTJSKJAL
Italië	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Kroatië	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Letland	SEVIŠKI SLEPENI	SLEPENI	KONFIDENCIĀLI	DĪNEŠTA 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	BEGRENSET
Oostenrijk	STRENG GEHEIM	GEHEIM	VERTRAULICH	EINGSCHRÄNKT
Polen	ŚCIŚLE TAJNE	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	MUITO SECRETO	SECRETO	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
Turkië	ÇOK GİZLİ	GİZLİ	ÖZEL	HİZMETE ÖZEL
Verenigd Koninkrijk ³	TOP SECRET	SECRET	NO EQUIVALENT TO CONFIDENTIAL	OFFICIAL-SENSITIVE
Verenigde Staten ⁴	TOP SECRET	SECRET	CONFIDENTIAL	
Zweden	KVALIFICERAT HEMLIG	HEMLIG	HEMLIG	HEMLIG
Zwitserland - Franstalig	TRÈS SECRET DÉFENSE	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	DIFFUSION RESTREINTE
- Duitstalig	STRENG GEHEIM	GEHEIM	VS - VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
- Italiaans- Riservato talig	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	

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 beveiligd 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 beheren 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	
--	---	--

Algemene Beveiligingseisen Defensie Opdrachten 2017

--	--	--

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 labels</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>Klksynchronisatie</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 Beveiligingsfunctionaris	
--	--	--

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 beveiligingselen 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 Beveiligingsfunctionaris

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 accepteert 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 _____

Algemene Beveiligingseisen Defensie Opdrachten 2017

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 accepteert 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 Zeggenschap en bedrijfsstructuur	
--	--	--

1. Initiele 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	

Algemene Beveiligingseisen Defensie Opdrachten 2017

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

Rubriceringsaanduidingslijst

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	Stafseisen						
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 zónodig 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 *Subcontractors* en/of *(Toe)leveranciers*

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 Beveiligingsfunctionaris
Datum

Algemene Beveiligingseisen Defensie Opdrachten 2017

Handtekening

<u>Alleen in te vullen door BIV / MIVD</u>	
Goedgekeurd door	Afgekeurd door
Datum	
Rubriceringsniveau	
<i>TBB op locatie Subcontractor</i>	
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	Behoeft						
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 Response 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 ⁵	Doel	Uitvoering
1. <i>Identificatie</i>	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 coördinatie 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.	I. Beschrijft - a. Het Beveiligingsincident. 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 Cyber 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 MIVD.
----	------------	------------	---

Bijlage 9.2 Incident Handling classificatie	
---	--

Categorie	Name	Omschrijving <u>Digitaal</u>	Omschrijving <u>Fysiek</u>	Time frame
Cat 0	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.
Cat 1	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.
Cat 2	<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 DoS 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
Cat 3	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 gemetigde besmetting op een niet geclassificeerd netwerk of host.	Geconstateerd is dat een maatregel uit een van de categorieën 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.
Cat 4	Ongeoorloofd gebruik	Een individu overtreedt de <i>ABDO</i> regels	Een individu overtreedt de <i>ABDO</i> regels.	Binnen 1 week.
Cat 5	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

Vertrouwensfuncties

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*.

Algemene Beveiligingseisen Defensie Opdrachten 2017

Bijlage 10.1 Model Lijst van Vertrouwensfuncties
--

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 Wva 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*

- <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>

- <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

WETSARTIKELLEN

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, € tweehonderdvijftig;

de tweede categorie, € tweeduzendtweehonderdvijftig;

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

Algemene Beveiligingseisen Defensie Opdrachten 2017

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.

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.

Algemene Beveiligingseisen Defensie Opdrachten 2017

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, waann de noodzaak om betrokkene bij de werkzaamheden in te zetten wordt toegelicht.	
7.	Rubricering van de opdracht:
Buitenlandse Rubricering:	
8.	"Eyes Only" merken?
ja	nee

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>

Algemene Beveiligingseisen Defensie Opdrachten 2017

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> _____ <i>Overige mededelingen :</i> _____ _____ _____			
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 (Indien ingevuld) Verklaring bij ontheffing uit een Vertrouwensfunctie

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	
Werkzaam 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
--

(Het formulier wordt te gebruiken door de afzender)

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.

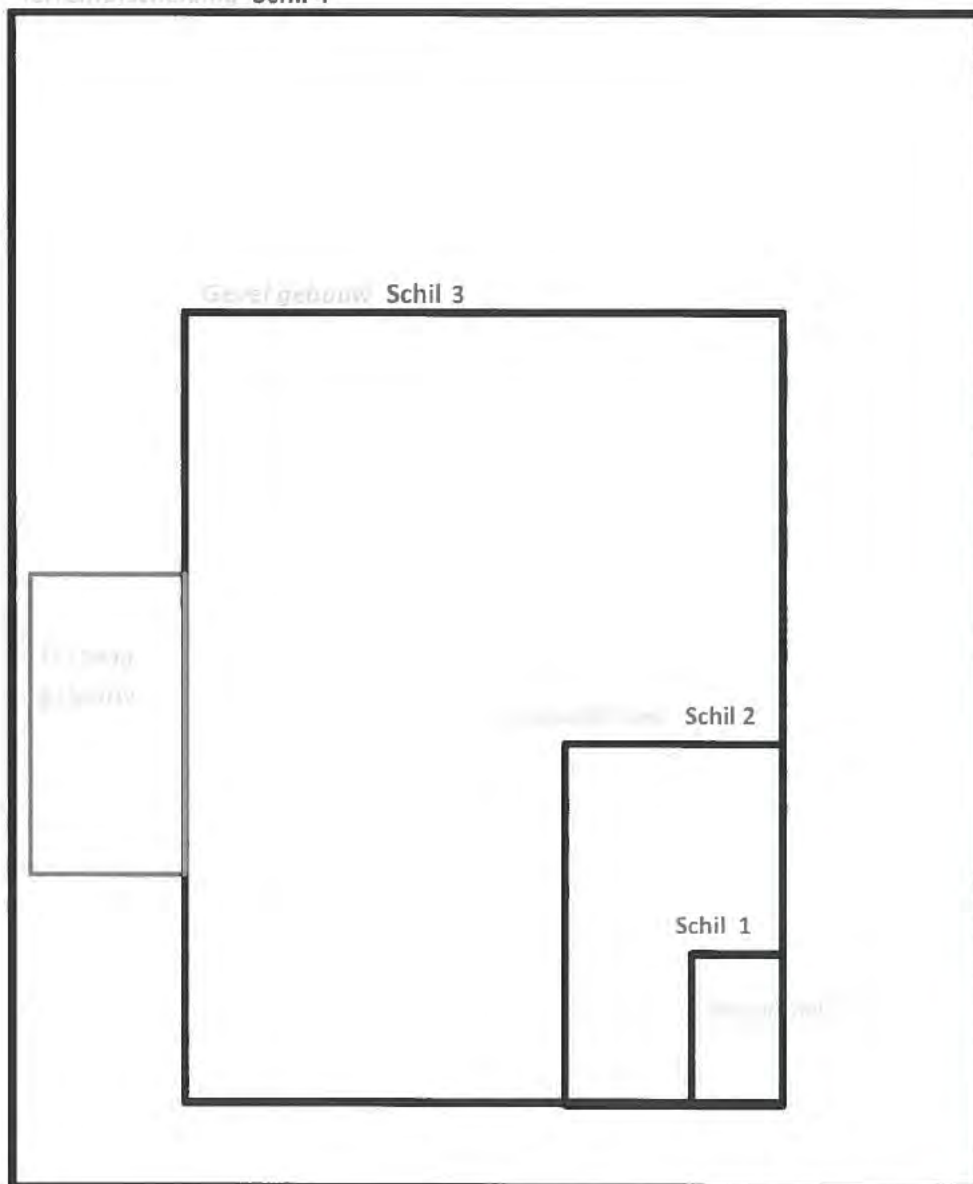
In de *ABDO* 2017 eisen zijn de minimaal vereiste beveiligingsmaatregelen opgenomen.

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

Terreinscheiding 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**.

Algemene Beveiligingseisen Defensie Opdrachten 2017

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 <i>BF</i>	<i>BIV / MIVD</i>
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.

Compartmentering

Gelijkwaardige *TBB* van één opdracht zullen zo veel mogelijk gezamenlijk in één compartiment verwerkt en opgeborgen zijn. Dit principe heet *Compartmentering*. 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. Een 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	
---	--

	<i>TBB 1</i> ZG	<i>TBB 2</i> G	<i>TBB 3</i> C	<i>TBB 4</i> 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

Camerabewaking 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 gevaldeerd alarm. Na de interventie kan worden teruggegaan naar de normale situatie als door de *BF* is vastgesteld dat het *TBB* niet is *Gecompromiteerd* 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 bewakingsrendement, 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.

Algemene Beveiligingseisen Defensie Opdrachten 2017

Alarmverificatie

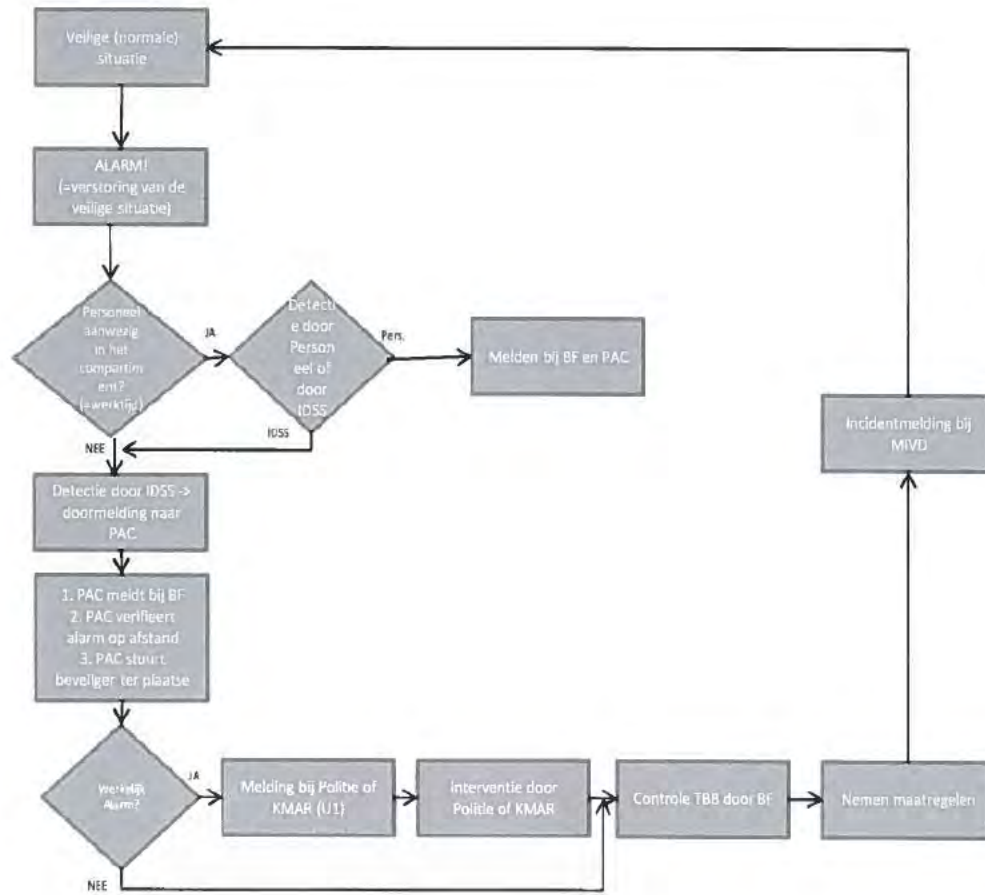
De alarmverificatie kan op een aantal manieren plaatsvinden:

- 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 TBB

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.

Algemene Beveiligingseisen Defensie Opdrachten 2017

	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*).

	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	DEPARTEMENTAAL VERTROUWELIJK	PERSONEELS VERTROUWELIJK	MEDISCH GEHEIM	COMMERCEEL VERTROUWELIJK	ONGERUBRICEERD & ONGEMERKT
- : Niet toegestaan								
V : Wel toegestaan								
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 BI naar het buitenland

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

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

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

Bijlage 23.2 Vernietiging van een TBB	
---	--

	TBB 1	TBB 2	TBB 3	TBB 4
	ZG	G	C	DV
Papier	Als TBB 2 én verbranden	Versnipperen L<25mm B<3mm	Versnipperen L<25mm B<3mm	Versnipperen L<30mm B<5mm
CD/DVD	Shredde en verbranden	Shredde	Shredde	Breken
Diskette	Shredde en verbranden	Shredde	Shredde	Breken
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.

Bijlage 23.2.1

Bewijs van overdracht te vernietigen *Informatie*

BEWIJS VAN OVERDRACHT VAN TE Vernietigen Informatie

Ondergetekende: _____

Functie: _____

Werknemer-ID: _____

Verzoekt de beveiligingsfunctionaris/ cryptobeheerder van: _____
(eenheid)

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

[illegible]

Voor overdracht

20 Voor overname

Handtekening

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:

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.

Aangegeven op welke wijze de vernietiging heeft plaatsgevonden

- Verbranding
- verpulvering c.q. verboddeling
- 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.

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

Datum _____

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.

1

(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 *Cyber-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 waardebepaling (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 *BYOD/CYOD*

Mobiele apparatuur zijn alle "devices" (apparaten) die geen statische plaats hebben. Een workstation 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 en 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 Systeemdokumentatie	
--	---	--

Systeemdokumentatie (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 systeemdokumentatie zal beveiligd moeten worden tegen inzage en gebruik door onbevoegden.

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

Systeemdokumentatie 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.

Bijlage 30 Labelen van gegevensdragers	
--	--

Het labelen van gegevensdragers heeft ten doel om diegene die met deze gegevensdragers werken direct en eenduidig er op te wijzen dat de gerubriceerde gegevensdrager apart behandeld moeten worden. Denk daarbij aan het niet mogen meenemen van de gegevensdrager of het niet in een willekeurig werkstation mogen stoppen van een USB-stick.

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 TBB

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

Logging en Monitoring

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

Virtualisatie en VLAN

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 (DMZ)

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 ongegrubeerde *Informatie* en (*STG.*) gerubeerde *Informatie*;
- de scheiding tussen gerubeerde *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 zogenaamde "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, beveiligingsels 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 ($Risico = Kans \times Schade$).

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 formulieren 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;

- volstrekte 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 volstrekte 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, € tweehonderdvijftig;

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 verwijdert 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



Vragen format "HIS / AIS DELIGHT"

Nummer	Vraag:	Vermelden: Hoofdstuk/ Paragraaf/ Bijlage nummer	Antwoord:
1	Leverancier wordt geacht reeds bekend te zijn met het overeengekomen gebruik. Het is echter uiterst onredelijk om binnen de geboden periode te verwachten dat Leverancier een gedegen analyse heeft gedaan, samen met haar interne specialisten, van alle door defensie aangeleverde documenten, wensen en eisen.	Arbit 4.2	De invoering van het gewenste AIS/HIS is mede wettelijk bepaald. Gelet op het gestelde in de vraag, heeft aanbestedende dienst (=AD) besloten een tweede nota van Inlichtingen te starten. Deadline voor het stellen van vragen voor deze Nvl 2 wordt 22-07-2019 om 17.00 uur.
2	Hier lijkt sprake te zijn van levering van een fysiek product, terwijl de overeenkomst betrekking heeft op software. Voorstel: dit artikel verwijderen en aanvullende afspraken maken over het leverings- en/of implementatieproces.	Arbit 6.1	Bij het afsluiten van de overeenkomst kan dit artikel als niet van toepassing worden verklaard.
3	Niet wederkerig en onmogelijk om in de fase van functionele uitvraag te beoordelen wat de uiteindelijke impact gaat zijn van dit artikel. Eerst vaststellen wat 'maatwerk voor Defensie' is en wat 'standaardprogramma van leverancier' is.	Arbit 8	De standaard programmaatuur blijft eigendom van de leverancier. De ingevulde data daartegen zijn, en blijven eigendom van het Ministerie van Defensie
4	Dit dient eerst te worden nagegaan. Tot die tijd kunnen we niet akkoord gaan met dit artikel.	Arbit 10.1	Ik zie de resultaten met belangstelling en vertrouwen tegemoet
5	Het overeengekomen gebruik zou moeten blijken uit alle aangeleverde documentatie van defensie aan leverancier. Zie ook artikel 4. leverancier, wordt geacht te weten wat het overeengekomen gebruik is. Aangezien leverancier slechts enkele dagen de tijd heeft gekregen om zich te verdiepen in alle aangeleverde documentatie, voorwaarden en technisch eisen en wensen, kan leverancier vooralsnog niet akkoord gaan met dit artikel.		Zie hierbij naar de beantwoording op de vraag betrekking hebbend op Artikel 4.2
6	Aansprakelijkheid niet zonder meer akkoord.	Arbit 12.3	Dit is geen vraag. Hier kan de AD ook geen antwoord op geven.
7	Dit gaat ver. Leverancier gaat niet zondermeer akkoord met het delen van haar polis.	Arbit 26.2 en 26.3	Er wordt slechts en uitsluitend op verzoek gevraagd naar het overleggen van bewijs van betaling en niet naar de inhoud van de polis
8	leverancier kan hier niet mee akkoord gaan. Bij overmacht is er geen sprake van een toerekenbare tekortkoming, dus geen reden voor ontbinding. Zowel de Opdrachtgever als de Wederpartij dragen dit risico.	Arbit 29.3	AOID?
9	Niet zondermeer akkoord met frase: "... sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Wederpartij."	Arbit 30.2 Arbit 30.3	Dit is niet onderhandelbaar. De veiligheid van het land is niet gediend bij een mogelijk buitenlandse overname met banden naar buitenlandse inlichtingendiensten.

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

10	Een overeenkomst voor bepaalde tijd mag in beginsel niet tussentijds opgezegd worden. Met onmiddellijke ingang is bovendien onredelijk. Minimaal dient een redelijke opzegtermijn van toepassing te zijn.	Arbit 30.6	AOID?
11	Dat lijkt onredelijk. Defensie krijgt het Gebruiksrecht voor de duur van de Overeenkomst.	Arbit 43.1	Op het moment dat AD voor een kortere periode (bijvoorbeeld 5 jaar) gebruiksrecht verwerft, vervalt de verplichting voor gewijg.
	Dit is niet zondermeer akkoord.		Om de continuïteit van de bedrijfsvoering te verzekeren, mag Opdrachtgever Standaardprogrammatuur die bij hem in gebruik is kopiëren en installeren zo vaak als hij dat om die reden nodig acht. Opdrachtgever mag dus Programmatuur kopiëren zonder dat hij inbreuk maakt op het intellectuele eigendomsrecht daarop van Wederpartij.
12	Niet zondermeer akkoord. leverancier levert standaard 'as-is'.	Arbit 43.3	In de bijbehorende Overeenkomst dient met het oog daarop nauwkeurig te worden vastgelegd welke betalingsmodel (named of concurrent user, site enz.) bij het verkrijgen van het Gebruiksrecht is afgesproken, wie de administratie van het totaal aantal in omloop zijnde Gebruiksrechten gaat bijhouden, hoe dat gaat gebeuren en op welke wijze Opdrachtgever een eventueel verschuldigde aanvullende Vergoeding, aan Wederpartij dient te voldoen. Opdrachtgever dient zich ook daarom vooraf zorgvuldig door Wederpartij te laten informeren over de totale kosten die naar redelijke verwachting van Wederpartij voor Opdrachtgever aan het gebruik van de Standaardprogrammatuur verbonden zullen zijn.
13	Vooralsnog niet akkoord, omdat leverancier nog niet in de gelegenheid is geweest om dit te valideren.	Arbit 43.5	AD koopt met 12 maanden garantie. Dat betekent dat fouten binnen garantie hersteld moeten worden door leverancier, ongeacht of er sprake is van een servicecontract.
14		Arbit 44	AD wil voorkomen dat de gegevens onbruikbaar en ontoegankelijk maakt, door de programmatuur na beëindiging van het contract.

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

15	De frase "dan wel aanpassingen in Standaardprogrammatuur specifiek ten behoeve van Opdrachtgever." graag verwijderden.	Arbit 48.2	Wanneer bij contractering mocht blijken dat er geen sprake van Maatwerk, dan mag dit artikel vervallen.
16	Vooralsnog niet akkoord, aangezien nog onduidelijk is hoeveel maatwerkprogrammatuur ontwikkeld moet gaan worden.	Arbit 59	Zie beantwoording Artikel 48.2
17	Het betreft hier een inspanningsverplichting, dus niet akkoord met ontbinding.	Arbit 76.1	Het betreft een resultaatsverplichting. Zie hiervoor de functionele uitvraag hoofdstuk 1, 2e alinea (blz 5)
18	Niet zondermeer akkoord. Het blijven inspanningsverplichtingen. Hersteltijden variëren en zijn zeer afhankelijk van de complexiteit van het probleem.	Arbit 76.2	Zie beantwoording ARBIT Artikel 76, 1
19	Niet zondermeer akkoord. Er zijn oorzaken buiten de macht van leverancier, zoals lokale infra en netwerken, die de storing kunnen veroorzaken. Dit kan leverancier niet altijd signaleren. leverancier is enkel bereid om de kosten te dragen van het testen indien Defensie kan aantonen dat leverancier de oorzaak van de storing redelijkerwijs had moeten kunnen signaleren en verhalen.	Arbit 78	Akkoord met deze beperking
20	Toevoegen: dit moet schriftelijk overeengekomen zijn en Afnemer mag hiervoor additionele kosten in rekening brengen bij Defensie.	Arbit 82	Akkoord met deze toevoeging
21	Niet zondermeer akkoord. Innovatief Onderhoud maakt vooralsnog niet per definitie deel uit van de Overeenkomst of de Onderhoud overeenkomst. Indien Defensie Innovatief Onderhoud wenst af te nemen, dienen Partijen aanvullende afspraken te leveren	Arbit 84.5	AD mag geen last hebben van vernieuwingen in de programmatuur. Dat wil zeggen het moet werken onder alle omstandigheden, ook als leverancier een nieuwe versie met innovaties uitbrengt.
22	Deze marktoplossing dient uiterlijk 31 december 2020 in gebruik te zijn genomen ... Dit is niet realistisch en zal moeten worden bijgesteld, afhankelijk van de tekendatum, medewerking huidige leveranciers e.d.. Is dus van veel factoren afhankelijk. Hooguit zal een deel opgeleverd zijn.	Inleiding	
23	2.1.4 Operationele omstandigheden Terugkerend op veel plekken en ook in de uitvragen: het offline kunnen werken onder diverse omstandigheden. Dit lijkt in het algemeen een forse uitdaging. Hoe dringend is deze eis.	Context	

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

24	5.4.1 Dienst A.04.01.12 De gebruikersinterface (GUI) van de dienst is via een webbrowser te benaderen (webbased). ☒ Een lichte client is benodigd. Hoe dringend is deze eis en waarom is dit zo belangrijk.	Architectuur van de dienst	
25	deze als wens is gemarkeerd, dient opdrachtnemer binnen 18 maanden aan de normen te voldoen. Naaast onze huidige certificeringen/normeringen, waaraan we voldoen, gaat het om onderstaande lijst. NEN 7521:2014 Toegang patiëntgegevens ISO 27017:2015 Cloud dienst ISO 27032:2012 Guidelines for cybersecurity ISO24760 Framework for identity management ISO 29146:2016 Framework for access management ISO27018:2019 Code of practice for protection of personally identifiable information ISO 20000 Service Management ISO 25010:2011 System & software quality models ☒ Vraag: hoe strikt/bindend is dit?	Certificeringen en normeringen	
26	Er wordt gevraagd om een beschrijving van ons service management systeem én actuele en deugdelijke versies van het improvement plan en management review. Het is onrealistisch om te voldoen aan de eis dat het systeem in alle gevallen binnen 1 uur weer operationeel is. ☒ Vraag: Is dit bespreekbaar?	Certificeringen en normeringen	
27	Er zijn vragen m.b.t. de mogelijkheden voor export naar pdf en csv. ☒ Waarom zou je buiten het HIS werken als alles er in kan?	Diversen	
28	e-Health is amper benoemd. Denk aan afspraken maken, e-consults, herhaalrecepten. ☒ Wat is de rol van de patiënt? Kunnen we die rol vergroten?	Diversen	

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

29	Medicom bevat slimme protocollen en de module Medicom Smart. Het systeem denkt al mee i.p.v. reactief? ☐ Hoe kunnen we dit terug laten komen in het PvE?	Diversen	De scope vande aanbesteding is reeds vastgesteld. Eisen en Wensen kunnen in deze fase niet worden toegevoegd.
30	Veel diensten via papier. ☐ Waarom niet digitaal? (verwijzingen e.d.)	Diversen	
31	Triggers & alerts, er zijn vragen naar reactieve triggers. ☐ Waarom niet pro-actief?	Diversen	
32	Rapportage mogelijkheden, nu minimaal benoemd. ☐ We vermoeden dat populatiemanagement erg belangrijk is binnen de gesloten populatie van defensie?	Diversen	
33	Integraties. ☐ Wat is medisch noodzakelijk en waar voorziet Medicom/Pharmacom al in. Dus integratie met Sharepoint lijkt niet noodzakelijk, aangezien functionaliteiten al in Medicom zitten.	Diversen	
34	Add-ons NHG-docs wordt gevraagd, wij bieden MedicomSmart	Diversen	
35	5.4.1. diensten is OS-afhankelijk. Niet verwerkt in onze producten maar wel mogelijk. ☐ Hoe komt deze vraag in dit PvE? Hetzelfde geldt voor interfaces, dit is niet nodig. Juiste afstemming rondom hardware en OS wél.	Diversen	
36	De LCC lijkt al snel uit te komen rond de 5 miljoen. ☐ Wat kan Defensie over deze prijsstelling melden?	Diversen	Daarover doet AD geen mededelingen
		Prijzen	

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

37	In de begeleidende mail van Comparex d.d. 19 juni 2019 staat dat de leverancier bij inschrijving automatisch akkoord gaat met de voorwaarden gesteld in de meegeleverde ARBIT. Wij kunnen hier niet mee akkoord gaan, bijlage 5 kunnen we niet zonder meer getekend retourneren. In de ARBIT staan te veel zaken die niks met het onderhoud op HIX of met de dienstverlening hieromtrent te maken hebben. ChipSoft hanteert voor al haar klanten gelijke condities, omdat een situatie waarin iedere klant eigen, afwijkende onderhouds-, service- en garantievoorwaarden heeft, een onbeheersbare situatie in de dagelijkse bedrijfsvoering van ChipSoft ontstaat. Denk hierbij aan: de afstemmingsproblemen die ontstaan in de uitvoering van de service, het onderhoud en in de administratieve afhandeling van de contracten, SLA en werkzaamheden. Als uitgangspunt gaan we uit van de Mantelovereenkomst van ChipSoft. Deze Mantelovereenkomst wordt aangevuld met een Nadere Overeenkomst, hierin komen specifieke afspraken tussen Ministerie van Defensie en ChipSoft te staan (hierin kunnen ook specifieke onderdelen uit de ARBIT opgenomen worden). Deze Nadere Overeenkomst prevaleert boven de Mantelovereenkomst. Uitgangspunt van ChipSoft is om te allen tijde te komen tot een wederkerig en evenwichtige Overeenkomst welke is toegespitst op het specifieke onderhoud en dienstverlening van ChipSoft op HIX. Graag willen wij u ook attenderen op het feit dat wij HIX reeds leveren aan het CMH in Utrecht waar wij een zelfde constructie al mee hebben afgesloten. Wij nemen dan ook aan dat er de mogelijkheid bestaat om te komen tot een gezamenlijk gedragen, wederkerig en evenwichtig contract inclusief praktische zaken zoals planning, betalingscondities, et cetera. Is deze aanname juist?	Begeleidende mail "Functionele uitvraag 113284 17534444 HIS / AIS (DELIGHT)/ ChipSoft dd. 19 juni 2019" tevens bijlage 5. akkoord verklaring conceptovereenkomst	
38	In het bestek zijn veel eisen en wensen opgenomen. Volgens uw bestek zou het beantwoorden van een eis met "nee" reden zijn voor het terzijde leggen van de ingediende aanbieding. Wij gaan er echter vanuit dat bij het beantwoorden van de functionele vragen de mogelijkheid bestaat om een eis met "nee" te beantwoorden aangevuld met een toelichting. Ondanks dat er met "nee" geantwoord is zal dit niet leiden tot uitsluiting. Kunt u dit bevestigen?	Toelichting en onder andere 00 HIS Delight FU (def) Hfdstk 2 paragraaf. 2.7	Bij de beantwoording van eisen zijn 3 mogelijkheden: Ja voldoet, 2 voldoet niet 3 anders met daarbij een toelichting. Nee heeft als nadeel dat dit leidt tot uitsluiting. Daarom wordt geadviseerd om in voorkomende gevallen: anders te beantwoorden, met daarin een toelichting hoe alsnog aan de gestelde eisen kan worden voldaan.

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

39	De dienst conformeert zich aan NHG-tabel gebruikersvoorschrift. Vraag: ChipSoft voldoet hier deels aan. Namelijk door koppelingen worden de voorschriften geconverteerd van en naar NHG-gebruiksvoorschrift. Is dit wat er bedoeld wordt met deze eis?	Hoofdstuk 4/ paragraaf 4.2.1/nummer F.02.01.16	
40	Het is mogelijk om Voorlichting Eerste Uitgifte Protocol digitaal vast te leggen. Vraag: Hoe ziet dit protocol er uit?	Hoofdstuk 4/ paragraaf 4.2.1./Nummer F.02.01.30	
41	Het is mogelijk om Voorlichting Gebruik Protocol digitaal vast te leggen. Vraag: Hoe ziet dit protocol er uit?	Hoofdstuk 4/ paragraaf 4.2.1./Nummer F.02.01.31	
42	Met welke kerngegevens kunnen wij t.b.v. de pricing rekenen? Wat is bijvoorbeeld het aantal werkplekken, named users/ concurrentusers?	Bijlage 6. Inschrijvingsbijlet	
43	Wat wordt er bedoeld met de "cost driver"?	Bijlage 6. Inschrijvingsbijlet	Deze is vervallen. Met de nota van inlichtingen wordt een nieuw bijlet verzonden.
44	• Het niet voldoen aan één eis als knock out criteria, zeker ook in combinatie met het geformuleerde pakket van wensen en eisen, gunningscriteria en puntentoekenning.		AD kan deze opmerking niet beantwoorden omdat het geen vraag betreft. AD heeft bovendien geen idee wat de bedoeling hiervan is.
45	• HIS/AIS-decentraal vs HIS/AIS-centraal. (F.05.01.01 + A.04.01.11) Is de juiste interpretatie van de vraag dat er een online omgeving en een offline omgeving moet zijn die met elkaar moeten communiceren en synchroniseren? Hier zijn veel vragen over, wij kunnen bijvoorbeeld een volledige SAAS oplossing leveren, perfect instaat om any place, any time en met any device te werken. Dit lokaal (offline) laten functioneren behoort wellicht tot de mogelijkheden (is weliswaar niet de usp van een SAAS oplossing) maar vereist mogelijk wel een aanvullende set wensen en eisen en of functionaliteiten (nu niet beschreven) die afgetoetst moeten worden en niet éénzijdig in een vraag en antwoord proces van een aanbesteding als deze doorlopen kunnen worden. Opdrachtgever vereist al zekerheden vooraf en opdrachtnemer moet in de aanbidding al reeds toezeggingen doen met financiële en juridische consequenties. Op deze wijze kan het wel eens erg ingewikkeld worden voor opdrachtgever om binnen budget en tijd gewenst invulling te realiseren.		

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

46	• V.01.01.04 ER is geen vergelijkbare referentie te overhandigen met de situatie van Defensie en als deze al bestaat mogelijk slechts bij één marktpartij en dat is meestal niet wenselijk in een procedure zoals deze. Wel zijn er gelijkende referentie qua omvang patiënten etc. Waar moet een referentie aan voldoen om door defensie als waardige referent te dienen?		
47	• De buiten NL georiënteerde activiteiten van opdrachtgever, vereisen mogelijk specifieke communicatie beveiliging etc. Voor lokale NL eerstelijnszorg zijn er meerdere infrastructuur providers (zoals KPN E zorg) die zorg dragen voor beveiligde communicatie. HIS en AIS leveranciers sluiten bij voorkeur hierop aan met standaard koppelvlakken gebaseerd op NL standaarden. Welke positie hebben deze leveranciers in dit aanbestedingstraject? Of verwacht u van aanbieders, dat zij ook een dergelijke rol gaan invullen, dat lijkt ons niet wenselijk.		
48	• F.01.01.07 Ruiters is een term die verschillende leveranciers op verschillende manier gebruiken met niet altijd één uniforme definitie.		
49	• F.01.10.30 Er worden hier mogelijk eisen gesteld die in conflict zijn met de AVG en privacy wetgeving. Zeker als de behandelend arts en apotheker verschillende personen zijn. Nadere uitleg is gewenst.		
50	• 4.8.1 Praktijkdossier: Hier lijkt het er op dat Defensie heel veel functionaliteit die ze nu gewend zijn, willen kopiëren naar een generieke oplossing die nu in de ICT markt voorhanden is voor de burger zorg. Veel van deze gevraagde functionaliteit is nu niet aanwezig in de mainstream systemen. Dit zou veel maatwerk betekenen. Of workarounds maar we lezen dit als zijnde een knock-out.		
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			
61			

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

62			
63			
64			
65			
66			
67			
68			
69			
70			
71			
72			
73			
74			
75			

Vragenformat "HIS / AIS DELIGHT"

Vragen format "HIS / AIS DELIGHT"

Nummer	Vraag:	Vermelden: Hoofdstuk/ paragraaf/ Bijlage nummer
1	Dient het systeem onder operationele omstandigheden beschikbaar te zijn voor de cliënten?	2.1.4
2	"Bepaalde informatie"; wat bedoelt u daarmee?	F02.01.33
3	Is het een wens van Defensie om zelf de 1e lijns support op te vangen?	Geen paragraaf
4	Hoe hard is de eis dat de hosting zelf door Defensie gedaan wordt ?	Geen paragraaf
5	Welke tabellen wil Defensie zelf beheren?	F08.03.03
6	Leverancier vraagt met welke kerngegevens te kunnen rekenen t.b.v. de pricing? Wat is bijvoorbeeld het aantal werkplekken, named users/ concurrentusers?	Bijlage 6. Inschrijvingsbijlet

Vragenformat "HIS / AIS DELIGHT"

Antwoord:	
Alleen als de cliënten onder operationele omstandigheden toegang hebben tot het openbare internet zullen zij toegang hebben tot het systeem via het self-service portaal patient.	
Met 'bepaalde informatie' wordt die informatie bedoeld die tussen apotheek en huisarts uitgewisseld moet worden voor het veilig kunnen leveren van farmaceutische zorg (zoals labwaarden, <i>verplichte indicaties, zwangerschap, etc.</i>)	
Ja, ServiceDesk Defensie (SDD) is de 1e lijn voor de Defensie medewerkers die gebruik maken van de dienst. Dit geldt zowel voor HIS/AIS centraal als HIS/AIS decentraal. Zie Eis S.07.01.02	
Defensie vraagt een oplossing voor zowel een HIS/AIS centraal (back-end-omgeving van de leverancier die wordt afgenomen als een dienst, zie paragraaf 7.1.2 diensten) als een HIS/AIS decentraal. Voor het decentrale deel wordt er om een oplossing gevraagd die voldoet aan wens A.05.01.06. Het Defensie domein wordt door Defensie beheert	
Defensie wil alleen de zelfgemaakte tabellen die de praktijk gebruikt voor het beheren van de patientendossiers zelf beheren. Niet de systeem tabellen die nodig zijn om het systeem te laten werken.	
Defensie geeft de voorkeur aan een prijsstellingsmethode waarbij de Leverancier rekent met het aantal ingeschreven patiënten (circa 40.000). Het betreft dan alle militairen, aangevuld met ongeveer 1500 niet-militairen voor wie Defensie de huisartsenzorg levert. Er zijn weliswaar momenteel 55.000 actieve dossiers (zie PvEW), maar dit zijn niet allemaal actieve eerstelijns patiënten van de militaire gezondheidszorg.	

Programma van Eisen en Wensen

Project Vervanging ZIS & R-EPD MRC

Versie	1.0
Datum	26-08-2020
Status	Definitief

Colofon

	Defensie Gezondheidszorg Organisatie
Locatie	[Redacted]
Postadres	[Redacted]
Contactpersoon	[Redacted]
Versie	1.0
Opdrachtgever	Voorzitter Stuurgroep ZIS/EPD MRC
Auteur	[Redacted]
Projectnummer	CDS.IV.447.13

Inhoud

Inhoud	3
1 Inleiding	7
1.1 Achtergrond.....	7
1.2 Doel	8
1.3 Schematische weergave van de beoogde dienst	9
1.4 Leeswijzer	9
2 Context	11
2.1 Organisatie	11
2.1.1 Organisatiebeschrijving	11
2.1.2 Situatieschets	11
2.1.3 Reguliere omstandigheden	12
2.2 Revalidatiezorg	12
2.3 Processen	12
2.3.1 Primair revalidatieproces	12
2.3.2 Proces Orthopedie Techniek Aardenburg (OTA)	15
2.4 Kengetallen.....	16
2.4.1 Patiëntenpopulatie.....	16
2.4.2 Zorgprofessionals	16
2.5 Beveiligingseisen	16
2.6 Toepasselijke civiele en militaire wet- en regelgeving	17
3 Algemene eisen en wensen.....	18
4 Functionele eisen en wensen	19
4.1 Revalidatiezorg	19
4.1.1 Dossierinvoer algemeen.....	19
4.1.2 Afdrukken en inscannen.....	20
4.1.3 Historie	20
4.1.4 Gebruiksvriendelijkheid.....	20
4.2 Behandelplannen/ voorschriften	21
4.2.1 Aanmelden en overdracht gegevens.....	21
4.2.2 Voorschriften en doelen.....	21
4.2.3 Diagnosevastlegging en behandelingenregistratie	22
4.3 Disciplinedossiers	22
4.3.1 Disciplinedossier (specialistische dossiers)	22

4.3.2	Invoer- en weergavemogelijkheden.....	22
4.3.3	Overzicht belangrijke gegevens.....	23
4.3.4	Inzage en afscherming.....	23
4.3.5	Scores en berekeningen	24
4.3.6	Verpleegkundige view	24
4.4	Klinimetrie	25
4.4.1	Research studies.....	25
4.4.2	Inzage en weergave	25
4.4.3	Metingen en berekeningen	25
4.4.4	Onderhoud en leverancier	26
4.5	Diagnostiek.....	26
4.5.1	Gegevensuitwisseling ten behoeve van diagnostiek.....	26
4.6	Medicatie.....	26
4.6.1	Elektronisch voorschrijf systeem (EVS)	26
4.6.2	Toedieningsregistratie.....	27
4.7	Rapportage en verslaglegging	27
4.7.1	Dagrapportage/ Statusvoering	27
4.7.2	Doelrapportage	28
4.7.3	Sjablonen	28
4.7.4	Verslagen	28
4.8	Correspondentie.....	29
4.8.1	Externe inkomende correspondentie.....	29
4.8.2	Brieven en documenten generen	29
4.8.3	Communicatie	29
4.9	Dossieroverdracht	31
4.9.1	Dossieroverdracht	31
4.10	Monodisciplinaire zorgtrajecten	31
4.10.1	Monodisciplinaire zorgtrajecten	31
4.11	Zorgplanning.....	31
4.11.1	Planningsondersteuning.....	31
4.11.2	Agenda Management	32
4.11.3	Resourceplanning	32
4.11.4	Voorschriften- en zorgpadenplanning.....	33
4.11.5	Spreekuren- blokkenplanning	34

4.11.6	Perspectieven en doorsneden.....	35
4.11.7	Orders / Acties ten behoeve van planning	35
4.11.8	Correspondentie met betrekking tot planning.....	35
4.12	Zorg Administratie	36
4.13	Teamcommunicatie	37
4.13.1	Plannen Multidisciplinair overleg (MDO)	37
4.13.2	Vorbereiden MDO	37
4.13.3	Bespreken en besluitvorming MDO	37
4.13.4	Verslaglegging MDO	37
4.13.5	Interdisciplinair	38
4.13.6	Behandelcommunicatie.....	38
4.13.7	Informatieverstrekking	38
4.14	Ordermanagement.....	38
4.15	Patiënten portaal.....	39
4.16	Management rapportage	40
4.17	Generieke Services	41
4.17.1	Document Management	41
4.17.2	Workflow Management	41
4.17.3	Standaard Teksten.....	42
4.18	Integraties & Add-ons.....	42
4.18.1	Integraties.....	42
4.19	Gebruiksvriendelijkheid.....	43
4.19.1	Gebruiksvriendelijkheid.....	43
4.20	Wet & Regelgeving & Standaarden	44
4.20.1	Wetgeving.....	44
4.20.2	Normen & Regelgeving.....	45
5	Architectuur eisen en wensen.....	46
5.1	Algemeen.....	46
5.2	MRC locatie	46
5.3	Architectuur van de dienst	46
5.3.1	Dienst.....	46
5.3.2	Interfaces.....	47
5.3.3	Datacontrols	47
5.4	Technische architectuur	47

5.4.1	Devices & Werkplek.....	47
5.4.2	Randapparatuur	48
6	Transitie eisen en wensen	49
6.1	Inleiding	49
6.1.1	Transitieonderdelen	49
6.1.2	Beknopte omschrijving huidige ZIS/R-EPD	49
6.2	Plan van Aanpak Transitie	50
6.3	Projectmanagement.....	50
7	Afkortingen.....	51
8	Begrippenlijst.....	54
	Bijlage A Verificatiegesprekken	55
A.1	Algemeen	55
A.1.1	Inleiding	55
A.2	Verificatiegesprekken.....	55
A.2.1	Planning.....	55
	Bijlage B Proof of Concept.....	56
B.1	Algemeen	56
B.1.1	Inleiding	56
B.1.2	Doelstelling.....	56
B.2	Procedure	56
B.2.1	Proces PoC.....	56
B.2.2	Planning.....	56
B.2.3	Faciliteiten	56
B.3	Beschrijving Proof of Concept	56
B.3.1	Inleiding	56
B.3.2	Doorlopen casuïstiek.....	57
	Bijlage C Performance Indicatoren.....	58
	Bijlage D Technische eisen MRC.....	60
D.1	Technische eisen ZIS/R-EPD	60
	Bijlage E Project Start Architectuur	61

1 Inleiding

Het Ministerie van Defensie (hierna: Defensie) staat voor kwalitatief hoogwaardige medische zorg voor haar militairen. Een adequaat werkende informatievoorziening is hiervoor essentieel. Om dit te kunnen waarborgen, is Defensie gestart met het vernieuwen van de digitale informatievoorziening van de militaire gezondheidszorg.

Het Militair Revalidatiecentrum Aardenburg (MRC) maakt gebruik van Ecaris voor de administratieve registratie (ZIS) en van het Revalidatie Elektronisch Patiënten Dossier voor het dossier van de patiënt. Defensie is voornemens deze twee systemen te vervangen door een standaard marktoplossing op voorwaarde dat de betrouwbaarheid van de IV gewaarborgd blijft. Deze marktoplossing dient uiterlijk 30 september 2021 in gebruik te zijn genomen en te voorzien in een Ziekenhuis Informatiesysteem (ZIS), een elektronisch patiëntendossier voor de revalidant (R-EPD) en een (bij voorkeur geïntegreerd) medicatie voorschrijf systeem. Defensie streeft daarbij naar een totaaloplossing die als dienst kan worden geleverd voor het reguliere zorgdomein. De dienst wordt in dit document het 'ZIS/R-EPD' genoemd en wordt gebruikt onder reguliere omstandigheden.

Met deze vernieuwing van de zorg-IT wil Defensie de revalidatie zorgprofessionals binnen Defensie beter ondersteunen en aansluiten op standaarden in de civiele revalidatiezorg.

Dit Programma van Eisen en Wensen (PvEW) richt zich specifiek op de functionaliteiten van een Ziekenhuis Informatiesysteem (ZIS) en een Revalidatie Elektronisch Patiënten Dossier (R-EPD). Het omvat de functionele en niet-functionele eisen en wensen die Defensie stelt aan de beoogde totaaloplossing voor de geïntegreerde revalidatiezorg (ZIS/R-EPD).

1.1 Achtergrond

In navolging van de zorgplicht van de Minister van Defensie kan iedere militair in werkelijke dienst een beroep doen op kwalitatief hoogwaardige medische zorg. De zorg wordt geleverd tijdens inzet en daarbuiten, zowel in Nederland als in het buitenland. De Divisie Defensie Gezondheidszorg Organisatie (DGO) ondersteunt de geneeskundige zorgverlening aan de krijgsmachtdelen en draagt daarmee bij aan de inzetbaarheid van de militair. In Nederland verzorgen de DGO-onderdelen het grootste deel van de militaire gezondheidszorg (MGZ). Ook de operationele geneeskundige eenheden verzorgen een deel van de MGZ.

Behalve aan militairen verleent de MGZ in een aantal gevallen ook aan andere groepen mensen militaire zorg, te weten:

- Burgermedewerkers van Defensie;
- Gezinsleden van militairen en burgermedewerkers;
- Buitenlandse militairen en hun gezinsleden;
- Passanten/bezoekers van een Defensielocatie;
- Lokale bevolking (bij uitzendingen);
- Leerlingen van het ROC Veiligheid en Vakmanschap (VEVA)
- Burgers (alleen in het revalidatiecentrum).

In de Militaire Ambtenarenwet is vastgelegd dat militairen verplicht gezondheidszorg afnemen bij Defensie. Dit is nodig om te allen tijde de inzetbaarheid van de krijgsmacht te beoordelen en te borgen. Om adequaat en kwalitatief verantwoord zorg te verlenen, is een betrouwbare informatievoorziening, bedrijfsvoering en procesinrichting essentieel. Onder een betrouwbare informatievoorziening verstaan wij 'het veilig voorzien in juiste en volledige informatie op de juiste plaats en tijd aan de juiste persoon'. Investeren in een optimale inrichting van de bedrijfsvoering en

de ontwikkeling en toepassing van digitale medische informatievoorziening zijn nodig om kwalitatief en doelmatig te functioneren en de ontwikkelingen in de veranderende omgeving te kunnen blijven volgen.

1.2 Doel

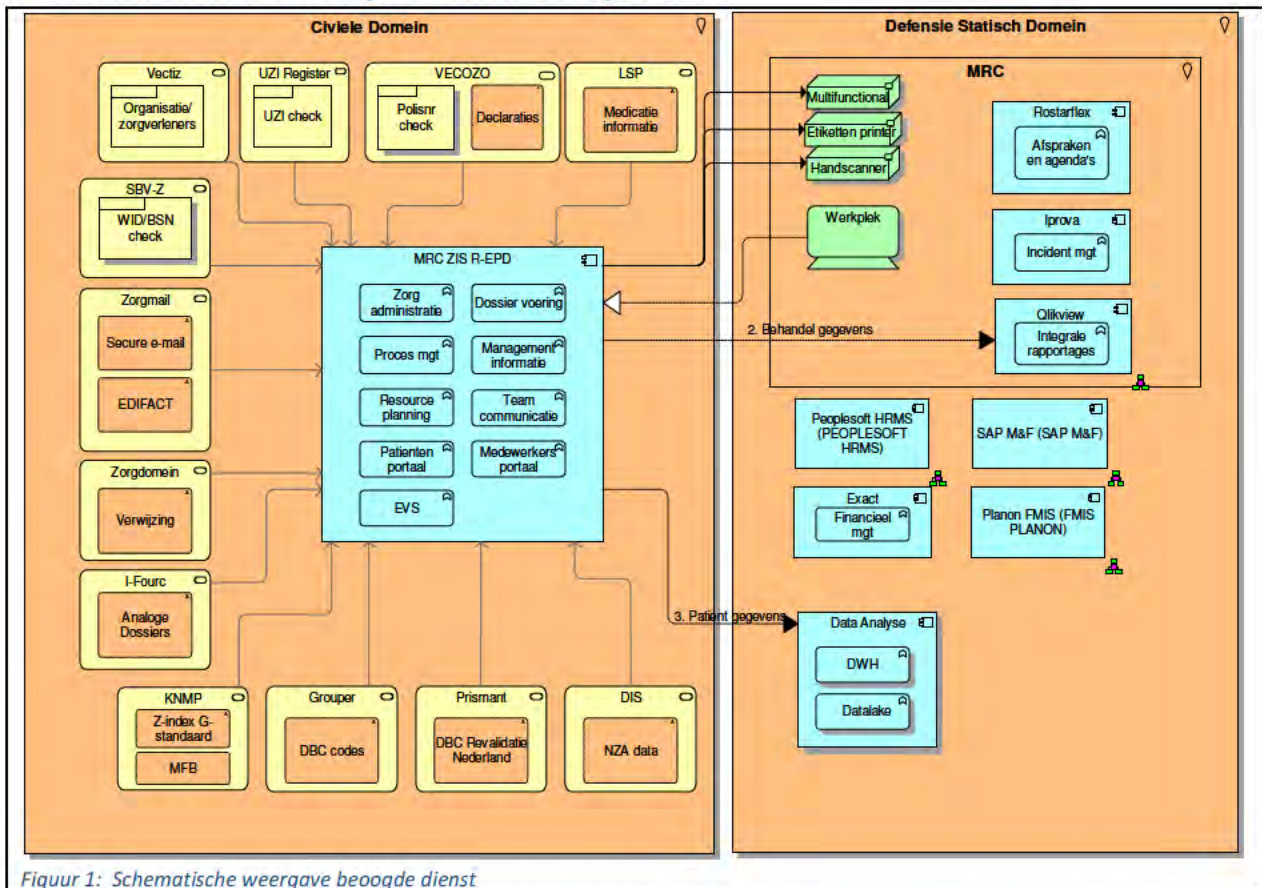
In het kader van de IV-vernieuwing beoogt Defensie een standaard marktoplossing in gebruik te nemen die de functionaliteiten bevat zoals deze in de civiele revalidatiezorg gebruikelijk zijn en die haar ontzorgt. Defensie is voornemens deze oplossing als een dienst af te nemen, waarbij de externe dienstverlener een substantieel deel van het beheer uitvoert. Defensie zoekt een dienstverlener die innovatief is en de mogelijkheden heeft en biedt om samen met Defensie de dienst op de wensen van Defensie in te richten en te koppelen aan de Defensie Infrastructuur en civiele zorginfrastructuren.

Voor Defensie is het belangrijk dat de oplossing kan voorzien in ondersteuning in alle mogelijke vormen van zorg op locatie (denk hierbij ook aan de specifieke oefenruimtes), én het de bedrijfsvoering ondersteunt in haar streven naar bewaking, beheersing en continue verbetering in en van de zorgketen.

Defensie hecht er grote waarde aan de in de civiele zorg gebruikelijke standaarden te volgen en te voldoen aan van toepassing zijnde vigerende wet- en regelgeving. Daarbij beoogt Defensie een oplossing in gebruik te nemen die faciliteert in de communicatie en de gegevensuitwisseling met andere zorgprofessionals binnen en buiten de militaire gezondheidszorg en de militaire en civiele patiënt. De dienst, gefaciliteerd in het civiele domein, is voor de zorgprofessional toegankelijk vanuit het defensie domein, via de standaardwerkplek van Defensie/MRC, op de zorgcentra in Nederland. Daarbij moet de beoogde oplossing voldoen aan de civiele- en de defensie beveiligingseisen.

In het vervolg van dit document geldt dat wanneer wordt gesproken over het systeem, de dienst of het ZIS/R-EPD, altijd wordt bedoeld op een oplossing inclusief (al dan niet geïntegreerd) EVS. Dus ook wanneer het EVS niet specifiek wordt genoemd, dient de eis gelezen te worden als tevens geldend voor het EVS.

1.3 Schematische weergave van de beoogde dienst



Figuur 1: Schematische weergave beoogde dienst

De licht blauw gekleurde vakken in bovenstaande figuur maken onderdeel uit van de beoogde dienst.

De beoogde dienst dient Defensie het volgende op te leveren:

- een ZIS/R-EPD-dienst die in de civiele zorg gebruikelijk is;
- een ZIS/R-EPD-dienst die aansluit op de ontwikkelingen in de civiele zorg;
- een ZIS/R-EPD-dienst die voldoet aan relevante vigerende wet- en regelgeving en best practices in de civiele zorg;
- integratie met en verzorgen van externe functionaliteiten (zorgservices) en add-ons;
- enkele specifieke functionaliteiten voor Defensie (wellicht, en dan bij uitzondering);
- integratie met de IT-infrastructuur en enkele gespecificeerde applicaties van Defensie;
- een continue, veilige en innovatieve dienstverlening; en
- een beheersbare en bestuurbare dienstverlening.

1.4 Leeswijzer

Dit document beschrijft het PvEW voor de verwerving van de beschreven dienst.

Het PvEW is onderverdeeld in rubrieken en is als volgt opgebouwd:

- Inleiding en aanbestedingsprocedure (hoofdstuk 1);
- Nadere duiding van de context waarin de dienst wordt gebruikt (hoofdstuk 2);
- Rubriek 1: Algemene eisen en wensen aan de te verwerven dienst (hoofdstuk 3);
- Rubriek 2: Functionele en kwalitatieve eisen en wensen vanuit de business (hoofdstuk 4);
- Rubriek 3: Eisen en wensen architectuur (hoofdstuk 5);
- Rubriek 4: Eisen en wensen transitie (hoofdstuk 6).

Elke rubriek van het PvEW omvat minimale eisen ('knock-out criteria') waaraan de Leverancier dient te voldoen en wensen die aan de dienst en de Leverancier worden gesteld. Ook zijn een aantal open vragen opgenomen. De eisen, wensen en open vragen zijn uniek genummerd. De nummering van de eisen en wensen is gebaseerd op de hierboven genoemde rubrieken en de paragrafen waarin de rubrieken zijn onderverdeeld.

Leveranciers wordt gevraagd om voor alle eisen, wensen en open vragen aan te geven of de door de Leverancier aangeboden dienst voldoet. Dit dient bij de eisen en wensen met een JA of een NEE te worden aangegeven. Hierbij kan de Leverancier in een toelichting in een separaat beoordelingsformulier aangeven op welke wijze de dienst invulling geeft aan de eis of wens. Let op: het opnemen van een toelichting is verplicht bij open vragen en indien dit expliciet is aangegeven. Maar ook indien het de voorkeur van de Leverancier heeft, kan een toelichting op het antwoord worden toegevoegd bij de betreffende vraag in de bijlage Beantwoordingsformulier PvEW Project Vervanging ZIS/R-EPD.

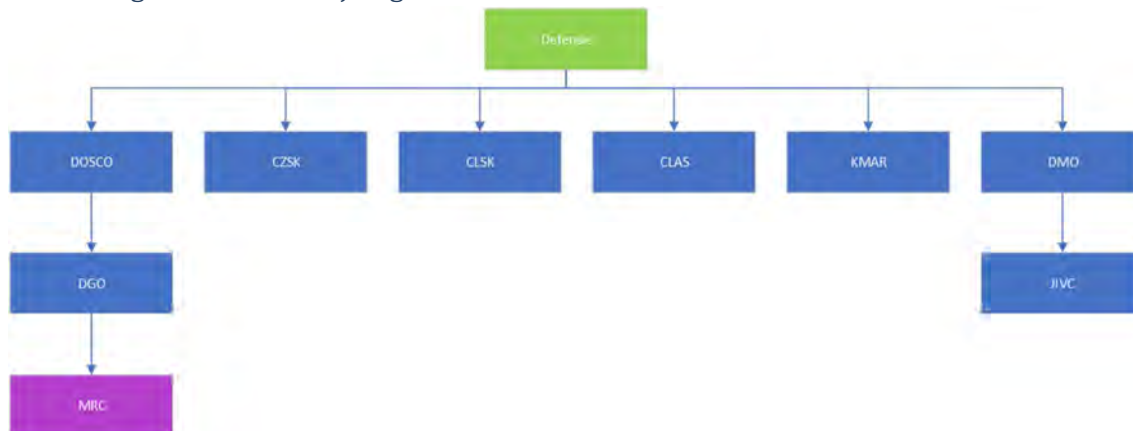
Verificatiegesprekken en een Proof of Concept zijn onderdeel van de aanbestedingsprocedure. In bijlage A Verificatiegesprekken en bijlage B Proof of Concept is hierover aanvullende informatie te vinden.

Op dit PvEW zijn de geheimhoudingsverplichtingen zoals beschreven in het aanbestedingsdocument (de Productgerichte Uitvraag, PU) van toepassing.

2 Context

2.1 Organisatie

2.1.1 Organisatiebeschrijving



Figuur 2 Organisatiebeschrijving

2.1.2 Situatieschets

Defensie beschermt wat ons dierbaar is. Militairen verdedigen Nederland, de (economische) belangen en bevriende landen. Ze komen op voor anderen en ondersteunen bij rampen. Zo draagt Defensie bij aan vrede, vrijheid en veiligheid in de wereld.

Waar onze militairen ook actief zijn, ze moeten kunnen rekenen op de beste medische zorg onder reguliere omstandigheden en eventueel na operationele inzet door een zorgprofessional van het MRC.

Het MRC is onderdeel van de DGO, dat onder het Defensie Ondersteuningscommando (DOSCO) valt. Daarnaast heeft ieder krijgsmachtdeel (met uitzondering van de Koninklijke Marechaussee) eigen operationele geneeskundige eenheden.

Naast de revalidatiezorg voor militairen levert het MRC óók zorg aan burgers, de civiele patiënt. Het revalidatiecentrum is aangesloten bij de brancheorganisatie Revalidatie Nederland en civiel erkend en gecertificeerd. Daarmee moet het MRC voldoen aan zowel militaire als civiele wetgeving.

Het DOSCO verricht een groot spectrum aan ondersteunende taken voor de krijgsmacht. Het zorgt bijvoorbeeld voor voedsel, gezondheidszorg, gebouwen, oefenterreinen, onderwijs en personeelsdiensten. Zo kunnen de Koninklijke Landmacht (CLAS), de Koninklijke Luchtmacht (CLSK), de Koninklijke Marine (CZSK) en de Koninklijke Marechaussee (KMAR) zich richten op hun hoofdtaken, operaties op zee, op land en in de lucht voor vrijheid, veiligheid en welvaart.

De belangrijkste wettelijke kaders voor de geïntegreerde zorgverlening onder zowel reguliere als operationele omstandigheden, vormen de Militaire Ambtenaren Wet (MAW) en de nadere uitwerkingen daarvan in het Algemeen Militair Ambtenaren Reglement (AMAR). Voor burgermedewerkers is het Burgerlijk Ambtenaren Reglement Defensie (BARD) van toepassing. Maar ook de civiele algemene wet- en regelgeving met betrekking tot de zorg is van toepassing, voor zover

de wet geen uitzondering kent voor Defensie of militairen. Een voorbeeld is dat Defensie afwijkende (langere) bewaartermijnen hanteert voor medische gegevens dan in de civiele zorg gebruikelijk is.

2.1.3 Reguliere omstandigheden

Het MRC levert (poli-) klinische Medisch specialistische zorg op een locatie in Doorn voor burgers en militairen. En op meerdere locaties buiten het revalidatiecentrum militair en civiele consulaire zorg. Revalidanten worden opgenomen in het verpleegcentrum, de Barak (verblijf voor revalidanten die ver van het revalidatiecentrum wonen) of komen voor dagbehandeling. In het verpleegcentrum en de Barak is plaats voor tachtig revalidanten. Daarnaast komen dagelijks ongeveer vijftig mensen voor dagbehandeling naar MRC Aardenburg.

2.2 Revalidatiezorg

Het MRC Aardenburg is gespecialiseerd in algemene, tweede-lijns revalidatie, vervaardiging van orthopedische hulpmiddelen en re-integratie in het arbeidsproces: arbeidsrevalidatie. Het centrum heeft een eigen Orthopedisch Instrumentmakerij. Ook wordt op indicatie revalidatiezorg geboden met virtuele middelen.

De revalidatiezorg wordt geleverd door een behandelteam dat bestaat uit:

- ergotherapeut;
- fysiotherapeut;
- logopedist;
- psycholoog;
- sporttherapeut;
- maatschappelijk werker;
- seksuoloog;
- verpleging;
- orthopedisch instrumentmaker.

2.3 Processen

2.3.1 Primair revalidatieproces

In onderstaande afbeelding wordt de as-is situatie van de volgende elkaar rakende processen getoond:

- Het proces voor aanmelding. Dat proces verzorgt o.a. activiteiten rondom de verwijzing;
- Het proces assessment waarin onder andere de intake plaatsvindt;
- Het behandelingsproces omvat alle activiteiten vanaf na de eerste observatie tot het moment van ontslag;
- De processen voor ontslag en nazorg zorgen voor de praktische en administratieve afhandeling na afronding van het behandelproces.

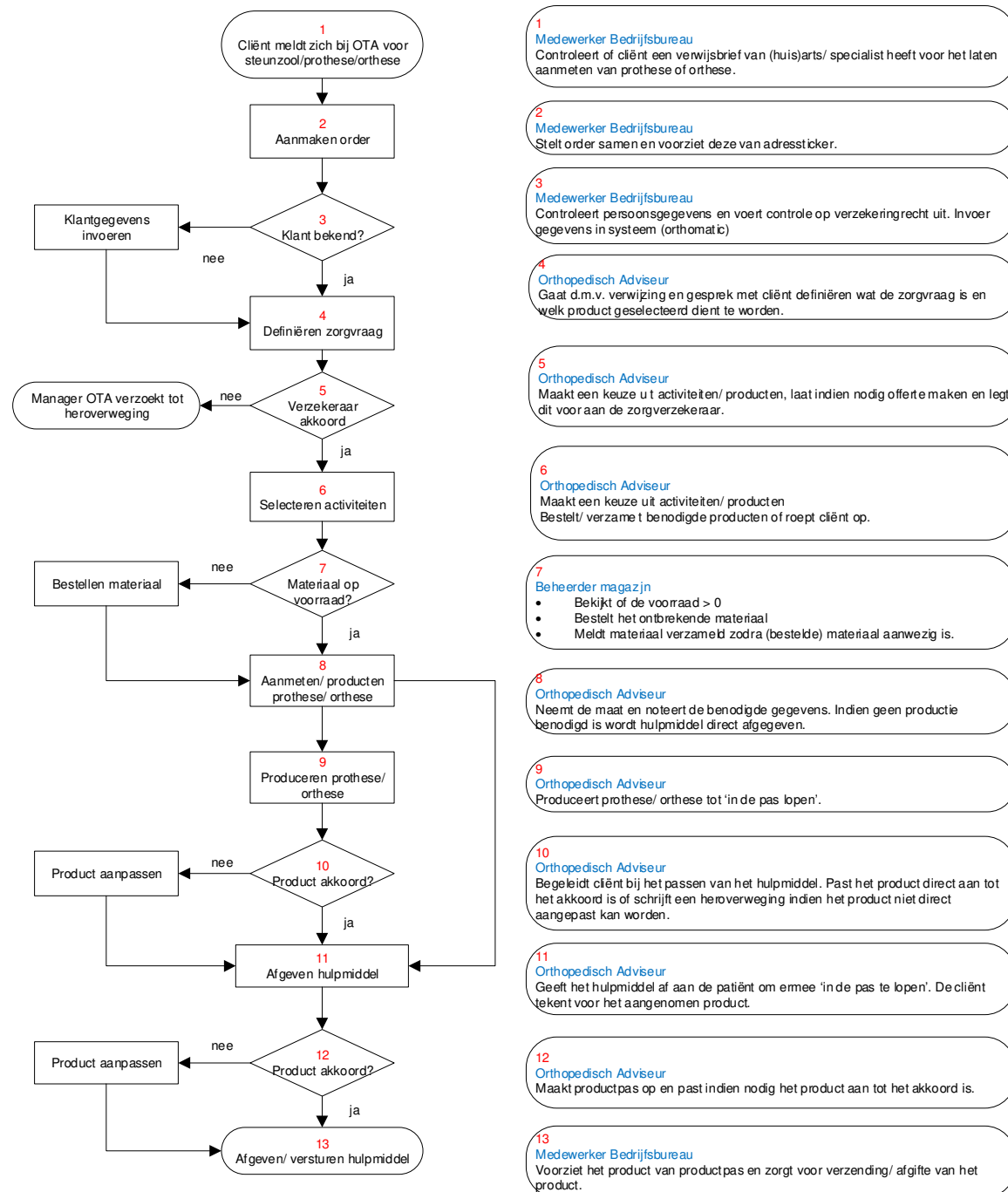


Figuur 3 primair revalidatieproces – Aanmelding en Assessment

Commercieel vertrouwelijk

2.3.2 Proces Orthopedie Techniek Aardenburg (OTA)

In onderstaande figuur wordt het as-is proces van Orthopedie Techniek Aardenburg getoond.



Figuur 5 Proces OTA

2.4 Kengetallen

De volgende kentallen zijn van toepassing op dit PvEW.

2.4.1 Patiëntenpopulatie

In beginsel levert Defensie gezondheidszorg aan Nederlandse militairen. Bij het MRC worden echter ook burger patiënten (ca 40% van de populatie in 2018) en medewerkers van de politie (ca 5% in 2018) behandeld. In totaal behandelde het MRC in 2018 circa 1700 unieke revalidanten.

2.4.2 Zorgprofessionals

In het MRC werken civiele (85%) en militaire (15%) zorgprofessionals samen om de juiste zorg te leveren aan de revalidanten

In onderstaande tabel is het aantal zorgprofessionals binnen het MRC weergegeven.

Functie	Aantal vte formatie	Aantal personen
1e Verpleegkundige Revalidatie	14,4	18
Activiteitentherapeut	2,1	3
Arbeidstherapeut	2	2
Diëtist	1	1
Ergotherapeut	8	12
Alg Mil Arts	1	1
Fysiother rev/Manueel Therapeut	1,5	2
Fysiotherapeut Revalidatie	16	23
Mdw Medicatie Verificatie MRC	0,8	1
GZ Psycholoog Revalidatie	3,7	5
Logopedist	2	4
Maatschappelijk werker MRC en Bedrijfsmaatschappelijk werker	3,3	4
Physician Assistant	3,2	4
Psychod Mdw/Cogn Re-int Thp	1,8	2
Sporttherapeut	7,6	11
Revalidatie Sport Trnr/coach	2	2
Transfer VPLK	1,6	2
Verzorgende	4,9	6
Revalidatie Therapie Ass	2	2
Virtual Reality Therapeut	1,9	3
VR Therapeut/Onderzoeker	1	1
Totaal	81,8	109

Tabel 1 Aantal zorgprofessionals MRC

2.5 Beveiligingseisen

Voor de te verwerven dienst gelden dezelfde eisen en wensen zoals deze in het kader van de verwerving voor de EGB zijn gesteld. Wij benadrukken dat deze eisen en wensen onderhevig zijn aan ontwikkelingen op het gebied van informatiebeveiliging en privacybescherming binnen de Rijksoverheid en de sector gezondheidszorg.

In het kader van het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) bepaalt Defensie het Betrouwbaarheidsniveau (BN) en het Te Beschermen Belang (TBB) van de gegevens in een IT-dienst. Hiervoor voert Defensie een VIR Efficiënt & Effectief analyse (VIR E&E) uit. VIR E&E is de methodiek die binnen de Rijksoverheid wordt gehanteerd voor het uitvoeren van een risicoanalyse in het kader van informatiebeveiliging. Met behulp van deze methodiek wordt bepaald hoe belangrijk de betrouwbaarheid van de gegevens in een IT-dienst is voor de organisatie.

Uitkomst van de VIR E&E analyse is de vaststelling van beveiligingsnormen waaraan de IT-dienst moet voldoen. Op basis daarvan worden de te treffen beveiligingsmaatregelen bepaald. Voor deze aanbesteding hanteert Defensie het uitgangspunt voorwaarde dat de leverancier ABDO (Algemene Beveiligingseisen voor Defensie Opdrachten, wordt nader toegelicht in de eisen) geautoriseerd dient te worden en zich conformeert aan de gestelde TBB-categorie. Defensie heeft zowel een VIR E&E analyse als een DPIA (Data Protection Impact Assessment) uitgevoerd om de set van beveiligingsmaatregelen te bepalen.

Om tot definitieve gunning van de te verwerven dienst te komen, voert Defensie nogmaals een VIR E&E en een DPIA uit op basis van de aangeboden dienst en de hierbij aangeleverde informatie.

Op grond van de dan vastgestelde TBB-categorie, stelt Defensie de definitieve set van de te implementeren beveiligingsmaatregelen vast. De eis dat Opdrachtnemer en de Leverancier de vastgestelde TBB-categorie accepteert en de hiervoor bepaalde set van beveiligingsmaatregelen implementeert, is opgenomen in hoofdstuk 6 Informatiebeveiliging en Privacy eisen en wensen en bepaalt daarmee de definitieve gunning.

2.6 Toepasselijke civiele en militaire wet- en regelgeving

De toepasselijke civiele en militaire wet- en regelgeving is opgenomen in dit PvEW.

3 Algemene eisen en wensen

Dit hoofdstuk beschrijft de algemene eisen en wensen die in de RFI van de dienst zijn gesteld.

Aanbestedingsprocedure			
Nummer	Details	Ja/Nee	E/W
V.01.01.01	De Leverancier werkt volledig mee aan de in de aanbesteding opgenomen verificatiegesprekken om Defensie een volledig beeld te geven van de aangeboden dienst en een volledige en juiste toelichting te geven op de beantwoording van het PvEW.		E
V.01.01.02	De Leverancier stemt in een Proof of Concept (PoC) op te leveren van de door haar aangeboden dienst, als onderdeel van de aanbesteding.		E
V.01.01.03	De Leverancier heeft in de afgelopen vijf jaar aantoonbaar ervaring opgedaan met de gevraagde dienst bij civiele zorgorganisaties.		W
V.01.01.04	De Leverancier heeft twee actuele referenties van vergelijkbare dienstverlening. <i>Indien met Ja is beantwoord, dient de Leverancier dit aantoonbaar te maken door het opleveren van een document waarin per referentie is beschreven:</i> • een omschrijving van de afgesproken en geleverde dienstverlening; • de klantorganisatie of opdrachtgever; • de datum waarop de dienstverlening is gestart; • de omvang van de dienstverlening onder meer in termen van functionaliteiten, aantal gebruikers (bijvoorbeeld van een cloud) en aantal patiëntendossiers; • een korte omschrijving van de afgesproken key performance indicatoren; • een recente klantwaardering over de dienstverlening; • de contactgegevens van de referentie organisaties.		E
V.01.01.05	De Leverancier geeft toestemming en heeft met de genoemde referentie organisaties afgesteld dat Defensie de referentie kan benaderen voor verificatie en nadere toelichting op de geleverde dienst.		E
V.01.01.06	De Leverancier conformeert zich aan de ARBIT 2016, inclusief ARBIT concept overeenkomst.		E
V.01.01.07	De Leverancier stemt in met het toevoegen van het beantwoorde PvEW aan het overeen te komen contract na gunning.		E

4 Functionele eisen en wensen

Dit hoofdstuk beschrijft de vereiste en gewenste businessfunctionaliteit van het MRC. De volgende onderwerpen worden beschreven:

- Revalidatiezorg;
- Zorgplanning
- Zorgadministratie;
- Teamcommunicatie;
- Procesmanagement;
- Stuur- managementinformatie;
- Informatie en communicatie;
- Generieke Services;
- Integraties en Add-Ons;
- Gebruiksvriendelijkheid;
- Wet- & Regelgeving & Standaarden.

4.1 Revalidatiezorg

4.1.1 Dossierinvoer algemeen

Dossierinvoer algemeen			
Nummer	Details	Ja/Nee/Anders	E/W
F.01.01.01	Het systeem ondersteunt verschillende methoden van gegevensinvoer: o.a. scannen, typen, kopiëren, gesproken tekst, import en mogelijkheid om tekst te kopiëren en plakken (drag & drop) uit bestanden, zulks te bepalen naar context en naar de behoefte van de gebruiker.		E
F.01.01.02	Auteur van invoer moet duidelijk zijn (functie en initialen). Invoer door stagiaires/co-assistenten ed. moet duidelijk te zien/onderscheiden zijn (invoerlogging).		E
F.01.01.03	Het systeem ondersteunt/ faciliteert tenminste de volgende specifieke terminologieën: ICF terminologie, Positieve gezondheidsterminologie, revalidatiegeneeskundige terminologie.		E
F.01.01.04	Het systeem ondersteunt maatwerk voor het vastleggen van militaire terminologie.		E
F.01.01.05	Het systeem ondersteunt het organisatorisch proces: bv alle noodzakelijke stappen (afnemen van vragenlijsten/testen) moeten zijn afgevinkt voor het dossier kan worden gesloten. Persoonlijke meldingen krijgen als je een stap nog niet hebt ingevuld.		E
F.01.01.06	Het systeem biedt een visuele weergave t.a.v. de plaats in het revalidatietraject waar de revalidant zich bevindt. Dit aan de hand van ijkpunten in het proces, bijv. een ontvangen verwijsbrief, een opgesteld behandelplan, in te vullen vragenlijsten/ klinimetrie, etc.		E
F.01.01.07	Vanuit het groepsdashboard wordt eenmalig ingevoerde tekst overgezet naar de dossiers van de afzonderlijke groepsleden. Dit om op efficiënte wijze verslag te kunnen doen van groepsbehandelingen, waarna per revalidant nog aanvullend kan worden geregistreerd in diens eigen dossier		E

F.01.01.08	In het dossier kunnen zowel korte als lange termijn (behandel)doelen vastgelegd worden ten behoeve van de behandeling. Dit is overzichtelijk getoond. Doelen formuleren gebeurt op cliënt/teamniveau maar soms ook op afdelingsniveau bv Verpleging. Op deze doelen zijn verschillende views mogelijk		E
F.01.01.09	Verplichte invoervelden / (openstaande) handelingen worden met kleurmarkeringen onderscheiden.		E
F.01.01.10	Het EPD is voorzien van een centrale plek waarin informatie gebundeld <u>aan de zorgverlener</u> wordt aangeboden. Het gaat hierbij om informatie die over de gehele caseload van de zorgverlener gaat (Je kan hierbij denken aan afspraken die de zorgverlener heeft, missende dossierstukken, afspraken die nog gerapporteerd of afgehandeld moeten worden).		E
F.01.01.11	Het systeem biedt de mogelijkheid signaleringen in te stellen. Bijvoorbeeld voor het verlopen van de DBC termijnen, zodat nog uit te voeren gesprekken/behandelingen kunnen worden ingepland binnen de huidige DBC.		E
F.01.01.12	Het is mogelijk pasfoto's aan het dossier toe te voegen op een eenvoudige manier (bij voorkeur rechtstreeks van camera).		E

4.1.2 Afdrukken en inscannen

Afdrukken en inscannen			
Nummer	Details	Ja/Nee/Anders	E/W
F.01.02.01	Overall in het dossier kunnen bijlages toegevoegd worden. Dit kan eenvoudig en direct in het systeem middels importeren of scannen van documenten.		E
F.01.02.02	Afdrukfuncties kunnen worden geactiveerd daar waar noodzakelijk voor het proces en zijn in te stellen per soort document.		E

4.1.3 Historie

Historie			
Nummer	Details	Ja/Nee/Anders	E/W
F.01.03.01	In het EPD is – binnen een dossier van een revalidant - het mogelijk om gebruik te maken van een uitgebreide zoekfunctie op historische data op onder andere specifieke terminologieën, datum, discipline of auteur.		E
F.01.03.02	Via het EPD heeft men eenduidig toegang tot een gescande historie vanuit verschillende digitale bronnen. De wijze waarop de digitale (gescande integrale cliënthistorie) kan worden ontsloten via het EPD is eenvoudig te beheersen.		W
F.01.03.03	Voor het gegevensbeheer voorziet het systeem in mogelijkheden voor het -binnen de technische mogelijkheden- verwijderen of niet meer tonen van gegevens om te kunnen voldoen aan de wet- en regelgeving omtrent bewaartermijnen, waarin onderscheid kan worden gemaakt tussen militaire en civiele dossiers.		E

4.1.4 Gebruiksvriendelijkheid

Gebruiksvriendelijkheid			
Nummer	Details	Ja/Nee/Anders	E/W

F.01.04.01	Het systeem ondersteunt / faciliteert het interdisciplinaire werken (interdisciplinaire procesformulieren kunnen worden gebruikt) en multi user (dwz: gelijktijdig in één dossier werken/registreren door verschillende medewerkers)		E
F.01.04.02	Er is een groepsdashboard. Dit is een overzicht dat gebruikt kan worden voor groepsbehandelingen en biedt inzicht in de deelnemers, de diagnose van afzonderlijke deelnemers, doelen per deelnemer en biedt een decursusfunctie.		E
F.01.04.03	EPD is primair gericht op het doorlopen van het revalidatietraject van de cliënt. De verschillende disciplines/ functiegroepen geven input vanuit een eigen overzichtelijk gebruikersprofiel en kunnen de informatie van collega's raadplegen wanneer mogelijk. Er is dus 1 interdisciplinair dossier maar er is een gefilterd gebruikersprofiel op basis van rollen en autorisatie.		E
F.01.04.04	Binnen een revalidantendossier is het mogelijk om inzake een specifiek interdisciplinair subproces verslag te kunnen doen, bv aanvraag van een WMO-voorziening of begeleiding psychosociaal. Zo wordt in één oogopslag duidelijk hoe ver het proces staat, wie relevante contactpersonen zijn etc.		E
F.01.04.05	Het is inzichtelijk wie betrokken is bij het behandelteam. Dit is gekoppeld aan de planning en het rooster van de cliënt.		E
F.01.04.06	Binnen een revalidantendossier kan vanuit een beknopt overzicht doorgeklikt worden op detailinformatie. Terughalen of lezen van informatie dient eenvoudig te zijn met selectiemogelijkheden op onder andere auteur, discipline en onderwerp.		E
F.01.04.07	De dienst ondersteunt de verslaglegging (spellingscontrole, formats, standaard zinnen, teksten kopiëren uit dossier).		E

4.2 Behandelplannen/ voorschriften

4.2.1 Aanmelden en overdracht gegevens

Aanmelden en overdracht gegevens			
Nummer	Details	Ja/Nee/Anders	E/W
F.02.01.01	Aanmeldingen kunnen middels verschillende elektronische verwerkingen (bijvoorbeeld multimedia, HL7 integratie) binnenkomen en verwerkt worden in het EPD.		E
F.02.01.02	Aanmeldingen kunnen ook handmatig worden verwerkt.		E
F.02.01.03	Bij elektronische aanmeldingen zijn de gegevens van de verwijzers inzichtelijk, het systeem neemt de gegevens over uit de aanmelding.		E

4.2.2 Voorschriften en doelen

Voorschriften en doelen			
Nummer	Details	Ja/Nee/Anders	E/W
F.02.02.01	Het is mogelijk om inzichtelijk te maken wat het actuele beleid m.b.t. een Cliënt is, op de verschillende domeinen. Dit zowel in het Cliëntendossier, als vanuit een planning.		E
F.02.02.02	Het toekennen van een behandelvoorschrift aan een patiënt, het vastleggen van afwijkingen op het standaardprogramma en de bijbehorende communicatie richting de planningsafdeling kunnen op dezelfde plek in het dossier worden ingevoerd.		E
F.02.02.03	Bij het invoeren van een diagnose en/of behandelprogramma (zorgpad) geeft het systeem een voorzet ten aanzien van		W

	klinimetrie. Deze kan de behandelaar accepteren of (gemotiveerd) negeren.		
--	---	--	--

4.2.3 Diagnosevastlegging en behandelingsregistratie

Diagnosevastlegging en behandelingsregistratie			
Nummer	Details	Ja/Nee/Anders	E/W
F.02.03.01	Voor een revalidant kan een hoofddiagnose aangegeven worden en één of meerdere secundaire diagnoses.		E
F.02.03.02	Binnen 1 diagnose kunnen meerdere behandelingen, behandelprogramma's, zorgpaden en losse activiteiten geregistreerd worden.		E
F.02.03.03	Toestemmingsformulieren kunnen eenvoudig voor akkoord digitaal worden ondertekend en verwerkt/opgeslagen worden op een eenduidige plek in het EPD.		E
F.02.03.04	Diagnosevastlegging kan worden ondersteund door ICD10.		E
F.02.03.05	De dienst ondersteunt de validatie van gegevens o.b.v. toegestane waarden waarbij o.a. gebruik gemaakt wordt van de standaarden zoals benoemd onder Diagnostiek & Codering (ICD10).		W

4.3 Disciplinedossiers

4.3.1 Disciplinedossier (specialistische dossiers)

Disciplinedossier (specialistische dossiers)			
Nummer	Details	Ja/Nee/Anders	E/W
F.03.01.01	In het EPD kan op niveau van gebruikersgroep, vb een team behandelaren, een Cliëntsamenvatting worden gedefinieerd, waardoor een Cliënt-georiënteerd overzicht van relevante gegevens kan worden aangeklikt.		E
F.03.01.02	Het dossier is primair ingericht op het te doorlopen revalidatietraject van de cliënt. De verschillende disciplines geven de input vanuit eigen gebruikersprofiel en kunnen de informatie van collega's raadplegen/ gebruiken daar waar nodig.		E
F.03.01.03	Het dossier bevat de huidige/ gangbare standaard landelijke formulieren/ klinimetrie, welke voor de afzonderlijke revalidant kan worden ingevuld en worden toegevoegd aan diens dossier.		W
F.03.01.04	Het MRC kan eigen formulieren, lijsten en meetinstrumenten ontwikkelen en toevoegen aan het EPD.		W

4.3.2 Invoer- en weergavemogelijkheden

Invoer- en weergavemogelijkheden			
Nummer	Details	Ja/Nee/Anders	E/W
F.03.02.01	Het moet mogelijk zijn te werken vanuit een vakgroep maar ook individuele trajecten en groepsbehandelingen.		E
F.03.02.02	Formulieren en sjablonen kunnen als brondocument gebruikt worden voor het vastleggen en presenteren van gegevens. Het moet mogelijk zijn deze sjablonen te muteren.		E
F.03.02.03	In een nieuwe versie van een formulier kunnen waarden uit een vorige formulier automatisch overgenomen worden.		W
F.03.02.04	Het versiegeschiedenis van formulieren wordt overzichtelijk weergegeven		W

4.3.3 Overzicht belangrijke gegevens

Overzicht belangrijke gegevens			
Nummer	Details	Ja/Nee/Anders	E/W
F.03.03.01	Het systeem moet de mogelijkheid bieden de revalidant in te kunnen delen in een bepaalde doelgroep, vb. militairen en burgers.		E
F.03.03.02	Het systeem moet de mogelijkheid bieden het trainingsniveau van de revalidant zowel gestructureerd als in vrije tekst vast te leggen.		E
F.03.03.03	Het EPD ondersteunt een 'Cliëntkaart', waarop belangrijke informatie (persoonsgegevens, leeftijd, risico's enzovoorts) snel in te zien is. Licht toe hoe dit opgebouwd is in het systeem.		E
F.03.03.04	De revalidatieartsen en behandelaren dienen een snel overzicht in het EPD te hebben op (de voortgang van) de behandeling en de Cliënt (zoals revalidatieplan/ proces/ ontslagdatum).		E
F.03.03.05	Het is direct inzichtelijk wat WEL ingevuld is en door wie. Dit bijvoorbeeld aan de hand van een filterfunctie die alleen gevulde velden laat zien.		E
F.03.03.06	Het is in het revalidantendossier duidelijk zichtbaar of betrokkene wel of niet gereanimeerd wil worden en over een wilsverklaring inzake levensbeëindiging beschikt.		E
F.03.03.07	Essentiële gegevens zoals NTBR, allergieën, bloedgroep, slikproblemen zijn binnen één klik zichtbaar inclusief een pop-up van de gegevens van degene die deze gegevens heeft vastgelegd en datum.		E
F.03.03.08	Basisgegevens (NAW, contactpersonen, foto) van de Cliënt en het dossieroverzicht voor het eigen specialisme zijn binnen het EPD met één klik benaderbaar.		E
F.03.03.09	Belangrijke relaties zijn weergegeven, ook vanuit professioneel perspectief.		E
F.03.03.10	De Gebruiker dient zowel binnen een revalidantendossier als tussen verschillende dossiers eenvoudig en snel te kunnen schakelen/ switchen. Hierbij denken we aan meerdere tabbladen open kunnen zetten, gegevens 'formulieren' gelijktijdig kunnen openen zodat men kan vergelijken).		E
F.03.03.11	In het EPD is het mogelijk aan te geven dat er een melding is gemaakt van een incident.		E

4.3.4 Inzage en afscherming

Inzage en afscherming			
Nummer	Details	Ja/Nee/Anders	E/W
F.03.04.01	Het systeem maakt omgang met vertrouwelijke informatie mogelijk. Delen van het systeem kunnen worden afgeschermd voor inzage door een ander discipline door middel van een in te richten autorisatiematrix.		E
F.03.04.02	Het systeem bevat één Cliëntendatabase waarin alle Cliënt gerelateerde informatie van de verschillende disciplines en afdelingen wordt opgeslagen (multidisciplinair dossiervoering).		E
F.03.04.03	Het systeem biedt de mogelijkheid om snel en eenvoudig informatie te filteren op behandelaar.		E
F.03.04.04	Toegang tot een dossier is voorbehouden aan de behandelaren die direct betrokken zijn bij de behandeling van de cliënt.		E
F.03.04.05	Het moet mogelijk zijn om bij (on)verwachte uitval een dossier over te nemen van een collega behandelaar. Reden van inzake		E

	moet dan worden vastgelegd, alvorens men het dossier kan inzien. Dit wordt gelogd.		
F.03.04.06	In het systeem is zichtbaar wie de hoofdbehandelaar is.		E

4.3.5 Scores en berekeningen

Scores en berekeningen			
Nummer	Details	Ja/Nee/Anders	E/W
F.03.05.01	Het systeem ondersteunt de mogelijkheid om op standaard beschikbare tekeningen/ afbeeldingen specifieke aantekeningen te maken.		E
F.03.05.02	Het systeem ondersteunt automatische berekeningen van scores op basis van ingevoerde gegevens in velden van formulieren/vragenlijsten.		E

4.3.6 Verpleegkundige view

Verpleegkundige view (VV)			
Nummer	Details	Ja/Nee/Anders	E/W
F.03.06.01	De user interface van de VV is in opzet en wijze van gebruik gelijk aan die van andere gebruikte dossiers.		E
F.03.06.02	Het systeem ondersteunt het dagelijkse werkproces van de verpleegkundigen en verzorgenden ten aanzien van opname/ontslag checklists die gevolgd dienen te worden bij opname, overdracht en het ontslag van een Cliënt.		E
F.03.06.03	Informatie over de Cliënt moet episode-georiënteerd kunnen worden gepresenteerd, bijvoorbeeld alleen uit de observatiefase.		E
F.03.06.04	Het is mogelijk om verpleegkundige registraties digitaal in te voeren (bijvoorbeeld User, Snaq Bartel, Nortol, def.lijsten, RR, vochtlijsten, TIME) en te delen met teamleden, ketenpartners en/of commissies.		E
F.03.06.05	De VV ondersteunt het gebruik van verpleeg plannen. Het systeem biedt inrichtingsmogelijkheden om de verpleegplannen gefilterd weer te geven.		E
F.03.06.06	De dienst biedt eenvoudige aanwezigheidsregistratie van de revalidant op het verpleegcentrum en overzicht.		E
F.03.06.07	Vanuit het systeem is digitale verpleegkundige overdracht, bijvoorbeeld naar een ziekenhuis, mogelijk middels "veilig mailen".		E

4.4 Klinimetrie

4.4.1 Research studies

Research studies			
Nummer	Details	Ja/Nee/Anders	E/W
F.04.01.01	Systeem biedt de mogelijkheid tot het extraheren van overzichtslijsten op verschillende niveaus bv Diagnosegroep, cluster enzovoorts.		E
F.04.01.02	Pilots die niet METC plichtig zijn, zijn herkenbaar gemerkt in het systeem.		W
F.04.01.03	Integratie van standaard klinimetrie testen, waarbij de testen automatisch afgerekend worden met de rechthebbende van de testen.		E

4.4.2 Inzage en weergave

Inzage en weergave			
Nummer	Details	Ja/Nee/Anders	E/W
F.04.02.01	Het systeem biedt de mogelijkheid voor alle behandelaars om klinimetrische gegevens in te zien.		E
F.04.02.02	Het systeem maakt op het niveau van de individuele revalidant een onderscheid tussen klinimetrie op hoofdlijnen die zichtbaar is voor alle behandelaars en klinimetrie in detail die zichtbaar is wanneer een behandelaar meer wil weten (middels een dashboard).		E
F.04.02.03	De dienst biedt de mogelijkheid om gegevens die bv op jaarbasis resultaten moeten genereren (kwaliteitsindicatoren/ uitkomstmaten) uit het systeem te extraheren (ook mogelijk t.a.v. de lopende behandelingen)		E
F.04.02.04	Verslaglegging van klinimetrie is eenvoudig te verwerken in brieven.		E

4.4.3 Metingen en berekeningen

Metingen en berekeningen			
Nummer	Details	Ja/Nee/Anders	E/W
F.04.03.01	Het is mogelijk om vanuit het systeem een programma (vb een webbrowser) te openen dat meetwaarden berekent op basis van de data analyses of databanken (bijvoorbeeld E-link, VRR of AMPS).		E
F.04.03.02	Het systeem biedt de mogelijkheid om rapporten te genereren, aan te passen, te printen of op scherm bekijken, zonder daarbij gebruik te hoeven maken van andere programma's als bijvoorbeeld Excel.		W
F.04.03.03	Het systeem biedt de mogelijkheid om zelf vragenlijsten te maken of aan te passen en berekeningen uit te voeren. Het biedt een eenvoudige functionaliteit om zelf testen of vragenlijsten te kunnen bouwen zoals bv performance lab, specifieke vragenlijsten voor militairen of bv voor pilots denk aan uitkomstenmaten.		E
F.04.03.04	Het systeem biedt de mogelijkheid voor digitale testlijsten die ingevuld kunnen worden door de cliënt, bijvoorbeeld via een portaal.		E
F.04.03.05	Een combinatie van testen (testbatterij) kan klaar gezet worden bv per diagnose, zorgpad of behandelprogramma.		E
F.04.03.06	Het is mogelijk om herhaalde metingen uit te voeren en het verloop van die metingen kan inzichtelijk worden gemaakt.		E

F.04.03.07	Het is mogelijk om behandelinhoudelijke gegevens (bijv. uitkomsten van metingen) te combineren met procesmatige gegevens van de cliënt, bijvoorbeeld de duur van een behandeling. Dit bijvoorbeeld om te kijken of langer doorbehandelen effect heeft.		E
F.04.03.08	Actueel houden van meetinstrumenten: Standaard testen worden in het systeem up to date gehouden door de leverancier van het ZIS.		E

4.4.4 Onderhoud en leverancier

Onderhoud en leverancier			
Nummer	Details	Ja/Nee/Anders	E/W
F.04.04.01	Revalidatieprofessional wordt ondersteund ten aanzien van de uitleg en interpretatie van scores.		W
F.04.04.02	Het is mogelijk om klinimetrische gegevens en uitkomstmaten bij de doelrapportage te betrekken zonder dit handmatig te moeten invoeren.		E
F.04.04.03	De Leverancier onderhoudt met de aanbieders betaalde vragenlijsten contracten t.a.v. nieuwe releases. (bv SCL90)		E

4.5 Diagnostiek

4.5.1 Gegevensuitwisseling ten behoeve van diagnostiek

Gegevensuitwisseling ten behoeve van diagnostiek			
Nummer	Details	Ja/Nee/Anders	E/W
F.05.01.01	Voor de Revalidatie Intake/Quickscan dient een standaard pakket (ingesteld op diagnose) diagnostische instrumenten afgenomen te worden.		E
F.05.01.02	Er dienen overervingsmogelijkheden te zijn op objectniveau.		E
F.05.01.03	Labuitslagen zijn inzichtelijk vanuit het revalidantendossier.		W
F.05.01.04	Het systeem biedt mogelijkheden/ faciliteiten om externe gegevensbronnen te kunnen ontsluiten.		E
F.05.01.05	Aanvragen van lab en röntgen of andere intercollegiale handelingen kunnen vanuit het patiëntdossier aangemaakt en verzonden worden.		W
F.05.01.06	Klinimetrische gegevens kunnen geïntegreerd worden in het EPD (registratie aan de bron, verwerking van conclusies en testen dienen in de verslaglegging EPD/MDO overgenomen te worden zodat dubbele administratielast voorkomen wordt).		E
F.05.01.07	Er kan onderscheid aangebracht worden tussen hoofddiagnose en nevendiagnose maar ook parallelle hoofddiagnoses stellen is mogelijk.		E
F.05.01.08	Binnen één zorgtraject kunnen meerdere behandelingen en/of zorgpaden geregistreerd worden (parallel aan elkaar).		E

4.6 Medicatie

4.6.1 Elektronisch voorschrift systeem (EVS)

Elektronisch voorschrift systeem (EVS)			
Nummer	Details	Ja/Nee/Anders	E/W
F.06.01.01	Systeem heeft bij voorkeur een geïntegreerd EVS. Indien dit niet aanwezig of mogelijk is, wordt er een EVS geleverd door de		E

	leverancier en op een gebruikersvriendelijke manier gekoppeld (bi-directioneel, single sign on).		
F.06.01.02	Vanuit het systeem kunnen, zowel in de klinische (VV) als poliklinische setting, medicatielijsten worden benaderd voor het raadplegen-, muteren en voorschrijven van medicatie.		E
F.06.01.03	Bij de geïntegreerde of bijgeleverd EVS oplossing is het AMO via LSP te downloaden in het dossier van de patiënt. Handmatig dan wel in bulk.		E
F.06.01.04	Bij geen geïntegreerde of bijgeleverd EVS oplossing is de medicatie per revalidant eenvoudig te registreren in het dossier. (Registratielijsten in het EPD)		E
F.06.01.05	Het moet mogelijk zijn om deelrondes (medicatie) in te plannen.		E

4.6.2 Toedieningsregistratie

Toedieningsregistratie			
Nummer	Details	Ja/Nee/Anders	E/W
F.06.02.01	Registratie voor toediening van alle geneesmiddelen is mogelijk vanuit het EPD systeem.		E
F.06.02.02	Elektronische toedieningsregistratie (toedieningslijst) voor medicatie is mogelijk.		E
F.06.02.03	Medicatieverwerking dient eenvoudig binnen het EPD (dossier van een cliënt) geregistreerd te worden, om risico's te mijden en veiligheid te waarborgen.		E
F.06.02.04	In de toekomst moet het mogelijk zijn dat de revalidant via patiënten portaal zijn regie voert over de registratie van de toediening.		W
F.06.02.05	Er is een signaalfunctie op medicatiebewaking.		E

4.7 Rapportage en verslaglegging

4.7.1 Dagrapportage/ Statusvoering

Dagrapportage/ Statusvoering			
Nummer	Details	Ja/Nee/Anders	E/W
F.07.01.01	Het is voor alle behandelaars, inclusief verpleging, mogelijk om dagrapportage/ statusvoering per revalidant uit te voeren in het systeem op basis van een zelf te bepalen methodiek, in een vrij in te vullen tekstveld (bijvoorbeeld SOAP).		E
F.07.01.02	Voor de verpleging is het onderscheid tussen de verschillende diensten (dag, nacht, avond) duidelijk zichtbaar in het systeem.		E
F.07.01.03	Het systeem biedt de mogelijkheid voor de behandelaar om eigen (werk) aantekeningen of notities bij de revalidant te maken als geheugensteuntje.		E
F.07.01.04	Systeem biedt een groepsdashboard. Er kan gerapporteerd worden op groepsniveau/ vanuit een groepstherapie. <i>Licht toe op welke wijze dit vormgegeven wordt.</i>		E
F.07.01.05	Het systeem ondersteunt het 'dagrapport' om een overdracht van belangrijke informatie met betrekking tot (een groep) klinische revalidanten te doen naar een behandelteam per dag.		E

F.07.01.06	Het is mogelijk om standaard zinnen (autoteksten) en doelen op te nemen in het systeem om de rapportage en verslaglegging te vergemakkelijken/versnellen.		E
F.07.01.07	Een (vorm van) dossierlog in het systeem maakt zichtbaar dat andere behandelaren inzicht hebben gehad in rapportage van andere disciplines.		E
F.07.01.08	Het systeem biedt de mogelijkheid voor verwerking van vertrouwelijke informatie volgens geldende richtlijnen (o.a. beroepscode opgesteld door de NIP).		E
F.07.01.09	Het is mogelijk om, naast het chronologische interdisciplinaire overzicht, overzichtelijk rapportages per eigen discipline te selecteren en te lezen, zonder daarbij de rapportages van andere disciplines in te hoeven zien.		E

4.7.2 Doelrapportage

Doelrapportage			
Nummer	Details	Ja/Nee/Anders	E/W
F.07.02.01	Het systeem biedt de behandelaar de mogelijkheid om dagelijkse rapportages te koppelen aan de vastgestelde revalidatiedoelen in het dossier van de cliënt.		E
F.07.02.02	Het systeem biedt de mogelijkheid om behaalde revalidatiedoelen af te vinken, waarna deze zichtbaar blijven.		E
F.07.02.03	Het is mogelijk om bij niet behaalde doelen aan te geven wat hiervan de reden is (zowel gestructureerd als vrije tekst argumentatie).		E
F.07.02.04	Het is mogelijk om behandeldoelen interdisciplinair uit te voeren, zodat vanuit verschillende disciplines op eenzelfde wijze gehandeld wordt.		E
F.07.02.05	Het is mogelijk om klinimetrische gegevens / uitkomstmaten bij de doelrapportage te betrekken zonder dit handmatig te moeten invoeren.		E

4.7.3 Sjablonen

Sjablonen			
Nummer	Details	Ja/Nee/Anders	E/W
F.07.03.01	In het EPD is verslaglegging met gebruik van sjablonen mogelijk.		E
F.07.03.02	Geselecteerde sjablonen, autoteksten en afvinklijsten kunnen eenvoudig door de gebruiker zelf worden aangepast.		E
F.07.03.03	Tekstvelden kunnen gekoppeld worden aan een automatische actie, bv MDO bespreking op datum waardoor systeem automatisch een formulier opent.		E

4.7.4 Verslagen

Verslagen			
Nummer	Details	Ja/Nee/Anders	E/W
F.07.04.01	Het systeem biedt de mogelijkheid na secretariële bewerking het verslag iteratief aan de verslaglegger aan te bieden ter correctie.		E
F.07.04.02	Het systeem maakt onderscheid tussen gevalideerde en niet gevalideerde verslagen/rapporten.		W
F.07.04.03	Het systeem biedt de mogelijkheid om de brieven en verslagen elektronisch (EDIFACT) te versturen.		E

F.07.04.04	Het systeem biedt de mogelijkheid om de brieven en verslagen elektronisch te ondertekenen.		E
------------	--	--	---

4.8 Correspondentie

4.8.1 Externe inkomende correspondentie

Externe inkomende correspondentie			
Nummer	Details	Ja/Nee/Anders	E/W
F.08.01.01	De verwijfsbrief van de verwijzer (papier/elektronisch) kan in het EPD worden opgeslagen of automatisch aan het dossier worden gekoppeld.		E
F.08.01.02	Het systeem staat toe dat delen uit de verwijfsbrief van een revalidatiearts uit het ziekenhuis bij intake kunnen worden overgenomen in het dossier.		E

4.8.2 Brieven en documenten genereren

Brieven en documenten genereren			
Nummer	Details	Ja/Nee/Anders	E/W
F.08.02.01	Het systeem kan op verschillende momenten automatisch brieven genereren op basis van vastgestelde sjablonen.		E
F.08.02.02	Het systeem kan bij het genereren van een brief patiëntgegevens en behandelgegevens correct weergeven (volgens sjabloon).		E
F.08.02.03	Het systeem slaat automatisch de (gegenereerde) brieven op, op basis van vastgestelde sjablonen, op de juiste plek in het revalidantendossier.		E
F.08.02.04	Het systeem heeft een weergave van de status van de gegenereerde brieven. (oa voor de controle AO/IC)		E
F.08.02.05	Indien een brief wordt gegenereerd, is het mogelijk daar nog een correctie op uit te voeren voordat deze wordt verstuurd.		E
F.08.02.06	Het systeem genereert automatisch ontslag- en overdrachtsrapportages. Uit bestaande rapportages moet je kunnen aangeven welke tekst je in de overdrachtsbrief wilt hebben.		E
F.08.02.07	Het systeem biedt de mogelijkheid om uit het dossier een brief (naar bijvoorbeeld de volgende behandelaar, de zorgverzekeraar of de gemeente (WMO)) te genereren op basis van zelf te selecteren informatie uit het EPD.		E
F.08.02.08	Per dossier moet het mogelijk zijn een (deel) overzicht te printen met informatie.		E
F.08.02.09	Overzichtslijsten (bijvoorbeeld bedbezetting, MDO, catering (incl. diëtetiek), HL, opnamelijst, medische overdracht etc) zijn te genereren en voldoen aan de privacywet en regelgeving voor gebruik.		E

4.8.3 Communicatie

Communicatie			
Nummer	Details	Ja/Nee/Anders	E/W
F.08.03.01	Het systeem biedt interne zorgverleners de mogelijkheid met externe zorgverleners te communiceren (mail/chat/video).		E

F.08.03.02	Schriftelijke correspondentie met externe zorgverleners kan worden toegevoegd aan het dossier.		E
F.08.03.03	Het systeem biedt gebruikers de mogelijkheid alle elektronische patiënt gebonden correspondentie tussen zorgverleners onderling en tussen zorgverleners en de patiënt in een correspondentie-overzicht te raadplegen.		E
F.08.03.04	Het systeem faciliteert interdisciplinaire communicatie.		E
F.08.03.05	Het systeem is eenvoudig te hanteren en overzichtelijk tijdens het MDO, onder andere op het gebied van: - Betrokken teamleden - Revalidatiedoelstellingen - Huidig functioneringsniveau - Besprekpunten MDO - Organisatorische planning behandeltraject.		E
F.08.03.06	Het is duidelijk welke teamleden betrokken zijn bij het revalidatietraject en deze teamleden kunnen eenvoudig onderling communiceren over betrokken cliënt.		E
F.08.03.07	De communicatie met de revalidant verloopt middels een goed functionerend patiënten portaal.		E
F.08.03.08	De Ondersteunende afdelingen (o.a. front-office, backoffice, planbureau en human logistics) krijgen hun eigen autorisatie binnen het dossier zodat de zorgcommunicatie gefaciliteerd wordt.		E
F.08.03.09	De leverancier anticipeert op toekomstige ontwikkelingen in de interne en externe communicatie in de ketenzorg en verwerkt dat tijdig in de dienst.		E
F.08.03.10	Online behandelfunctionaliteit / taken vanuit EPD of andere bronsystemen moeten aan elkaar kunnen worden gekoppeld (vb. klinimetrie en/of RTO)		E
F.08.03.11	Vanuit het EPD moet het mogelijk zijn om op een veilige manier te communiceren tussen verschillende deelnemers: patiënten, artsen, verpleegkundigen, zorgmanagers van chronisch zieken, apotheken, laboratoria, betalers, consulenten, enzovoort.		E
F.08.03.12	Ondersteunen van communicatie en presentatie van data verkregen van medische apparaten conform gangbare standaarden zoals HL7. Communicatie met medische apparaten is ondersteund zoals passend voor de zorgsetting, zoals een kantoor of het huis van de patiënt. Voorbeelden zijn: vitale functies, pols- en bloeddrukmeter, saturatiegraad en fysieke inspanning.		E
F.08.03.13	Ondersteunen zorgservices op afstand zoals telehealth en op afstand bestuurde monitoren. Maakt behandeling op afstand mogelijk met monitoren en tweerichtingscommunicatie tussen MRC en patiënt. Promoot verantwoordelijkheid van de patiënt, zelfbeschikking en de mogelijkheid gezondheid in de eigen omgeving in de gaten te houden. Promoot persoonlijke gezondheid, welbevinden en preventieve zorg.		E
F.08.03.14	Het systeem voldoet aan de vigerende wet- en regelgeving inclusief de aanvullende bepalingen uit de 'Wet cliëntenrechten bij elektronische verwerking van gegevens' (1 juli 2020).		E

4.9 Dossieroverdracht

4.9.1 Dossieroverdracht

Dossieroverdracht			
Nummer	Details	Ja/Nee/Anders	E/W
F.09.01.01	Het is mogelijk om in het dossier het behandelend cluster en bijbehorende behandelaar te wijzigen.		E
F.09.01.02	Het is mogelijk om (onderdelen van) het dossier van een revalidant over te dragen naar een externe zorgverlener.		E
F.09.01.03	Voortgang (op basis van meetresultaten) is eenvoudig grafisch weer te geven en te voorzien van schriftelijke toelichting.		E

4.10 Monodisciplinaire zorgtrajecten

4.10.1 Monodisciplinaire zorgtrajecten

Monodisciplinaire zorgtrajecten			
Nummer	Details	Ja/Nee/Anders	E/W
F.10.01.01	Monodisciplinaire trajecten moeten als dusdanig herkenbaar gemaakt kunnen worden.		E
F.10.01.02	Registratie en verwerkingsafspraken (o.a. facturatie, aantal trajecten op jaarbasis) zijn eenvoudig in te richten.		E
F.10.01.03	Er is een workflow voor monodisciplinaire zorgtrajecten in te richten.		E

4.11 Zorgplanning

4.11.1 Planningsondersteuning

Planningsondersteuning			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.01.01	Bedrijfsregels en werkafspraken kunnen worden ingevoerd in het systeem. Bijvoorbeeld afspraken t.a.v. tijd tussen bepaalde therapieën of therapieën die niet in combinatie gepland mogen worden.		E
F.11.01.02	Het systeem kan o.b.v. ingestelde bedrijfsregels en beschikbaarheid van resources automatisch het dienstenpatroon invullen met patiënten en zorgprofessionals.		E
F.11.01.03	Het systeem ondersteunt het werken en plannen (van oa bedbezetting) in een klinische setting.		E
F.11.01.04	Het systeem geeft planningsconflicten (zoals dubbele afspraken) aan en heeft de mogelijkheid om oplossingen aan te bieden.		E
F.11.01.05	Het is mogelijk om een proefplanning te maken en deze weer terug te zetten naar de oorspronkelijke planning.		E
F.11.01.06	Planning Poli artsen: Het systeem biedt de mogelijkheid om binnen gestelde parameters (zoals aandachtsgebied en beschikbaarheid) afspraken in het systeem te vinden en vast te leggen. Dit zowel voor één behandelaar als voor een groep behandelaren (bv MDO).		E
F.11.01.07	Het systeem biedt de mogelijkheid om duidelijk zichtbaar te maken als een afspraak niet verzet mag worden.		E

F.11.01.08	Afspraakmutaties. Het is per afspraak mogelijk de mutatiehistorie in te zien, waarbij duidelijk is wat de mutatie was en door wie deze is gedaan.		E
F.11.01.09	Het is duidelijk weer te geven voor de arts/ therapeut wanneer het een startend revalidatietraject betreft (nieuwe opname).		W
F.11.01.10	De dienst biedt een eenduidig wachtlijststelsel dat aan de door de branche voorgeschreven eisen voldoet betreffende de informatie verstrekking (Treeknorm).		E

4.11.2 Agenda Management

Agenda Management			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.02.01	Het systeem kent agendafunctionaliteit voor iedere afzonderlijke cliënt, medewerker en therapiemiddel of resource (ruimten, specifieke apparaten).		E
F.11.02.02	In het systeem kunnen resources/middelen (bijvoorbeeld een bepaalde ruimte of het zwembad) worden vastgelegd met specifieke kenmerken (bijv. maximale groepsgrootte, onderhouds interval) voor gebruik en planning.		E
F.11.02.03	Weergave: Het systeem biedt de mogelijkheid om de planning visueel weer te geven in de vorm van een gebruikersvriendelijke agenda of rooster, waarbij agenda's over elkaar en naast elkaar te zien zijn om snel inzicht te hebben in beschikbare plaatsen.		E
F.11.02.04	Het is mogelijk om afspraken handmatig in te plannen en te herplannen.		E
F.11.02.05	Het is mogelijk om een afspraak te voorzien van een 'reminder' of waarschuwing voor de behandelaar.		W
F.11.02.06	Roosters zijn eenvoudig inzichtelijk te maken voor therapeuten middels desktops en hand-held applicaties (bijvoorbeeld telefoon of tablet).		E
F.11.02.07	Cliëntenagenda's kunnen samengesteld worden tot overzichten op persoons en afdelingsniveau, bijvoorbeeld een overzicht met roosters van alle revalidanten van het verpleegcentrum, of juist van de poliklinische revalidanten (huidige "sleeplijsten").		E
F.11.02.08	Het is mogelijk om vanuit de agenda aan- en afmeldingen te registreren. Zodat inzichtelijk is welke revalidanten verwacht kunnen worden.		E
F.11.02.09	Het is mogelijk opmerkingen in vrije tekst aan afspraken toe te voegen, die juist wel of juist niet te lezen zijn voor de revalidant en therapeut.		E
F.11.02.10	Het is mogelijk om agenda's/roosters van collega-therapeuten in te zien, rekening houdend met wet- en regelgeving AVG.		E
F.11.02.11	Er kunnen kenmerken worden opgenomen bij de te plannen medewerkers m.b.t. plankaders/ werkafspraken.		E

4.11.3 Resourceplanning

Resourceplanning			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.03.01	Dienstroosters en werktijden van medewerkers zijn inzichtelijk en in te stellen.		E
F.11.03.02	Per medewerker kan een vast 'structuurrooster' worden ingesteld waarin aanwezigheid en vaste afspraken als blauwdruk voor de		E

	weekplanning zijn vastgelegd, hierbij kunnen ook periodiek terugkerende afspraken worden vastgelegd.		
F.11.03.03	Goedgekeurde verlofaanvragen in het personeelssysteem van Defensie kunnen middels een koppeling automatisch worden overgenomen in het systeem.		W
F.11.03.04	Vakantie/verlof/vrije dagen/cursus: Afwezigheid van medewerkers is ruim voortijdig in te stellen.		E
F.11.03.05	Rapportage: Het systeem biedt leidinggevenden inzicht in de komende capaciteit/aanwezigheid instelbaar per periode, cluster en vakgroep.		E
F.11.03.06	Rapportage: De tekorten (aangevraagde therapie waarvoor geen ruimte is) en overschotten (teveel geplande therapie) per discipline of revalidant per periode (structuur en datum) dienen snel en overzichtelijk inzichtelijk zijn.		E
F.11.03.07	Rapportage: Het systeem ondersteunt bij het definiëren van de wenselijke formatie in een instelbare periode op basis van de (gewenste) productie en de beschikbaarheid van resources.		W
F.11.03.08	Rapportage: het systeem waarschuwt indien er onderbezetting dreigt bij een specifieke discipline.		W
F.11.03.09	Leverancier conformeert zich aan de eventuele realisatie van één of meerdere koppelingen tussen het EPD en deelsystemen waarin de (dienstrooster)planning en aan-/afwezigheid van medewerkers wordt geregistreerd. Dit ten behoeve van de overerving van deze informatie richting het EPD. Hoewel deze koppelingen geen onderdeel zijn van de initiële scope van het project, kan Defensie besluiten dit in de nabije toekomst te implementeren. Leverancier verleent tijdige medewerking aan deze realisatie en sluit voor deze koppelingen aan op de architectuurprincipes en eisen zoals deze in dit Programma van Eisen zijn verwoord voor het gehele EPD (met name het gebruik van standaard protocollen en veilige uitwisseling).		E
F.11.03.10	Eenvoudig aanwezigheidsregistratie van de cliënt: patiënten informatie, kamer en telefoon nummer, inclusief aan- en afwezigheid.		E
F.11.03.11	Op basis van door gebruikers ingevoerde informatie kan een rittenlijst worden gegenereerd ten behoeve van Human Logistics, met daarop een overzicht van welke revalidant op welk moment van waar naar waar moet worden vervoerd.		E

4.11.4 Voorschriften- en zorgpadenplanning

Voorschriften- en zorgpadenplanning			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.04.01	In het systeem kunnen standaard voorschriften/behandelprogramma's/zorgpaden worden ingericht, waaruit de voorschrijvend arts kan kiezen.		E
F.11.04.02	Het is mogelijk om automatisch te plannen vanuit een vooraf ingericht voorschrift/behandelprogramma/zorgpad of vanuit een door de arts handmatig gekozen set therapieën.		E
F.11.04.03	Er kunnen notities voor de planner gemaakt worden bij de te plannen behandelprogramma's m.b.t. werkafspraken.		E
F.11.04.04	Klinische paden/standaard behandelprogramma's die zijn opgenomen in de planningsmodule zijn eenvoudig te wijzigen voor een planner/super user.		E

F.11.04.05	Het systeem is in staat de afspraken uit het voorschrift te koppelen aan de reeds geplande/gereserveerde (groeps)afspraken (gecombineerde groepen is mogelijk of bv duo-planning).		E
F.11.04.06	Bij het verwijderen van afspraken worden deze weer zichtbaar als nog te plannen orders. Het is mogelijk om in te stellen voor welke afspraken dit van toepassing is (tekorten overzicht).		E
F.11.04.07	Bij afwijkingen van het standaardprogramma van een behandelvoorschrift, kan dit vanuit het systeem worden gecommuniceerd richting de planningsafdeling.		E
F.11.04.08	De planning moet per revalidant een zorgpad programma en aanvullende supplementen/activiteiten kunnen 'stapelen' (revalidatieprogramma op maat maken).		E
F.11.04.09	Wijzigingen in zorgpaden of bv verwijderen/toevoegen nieuwe zorgpaden worden aangebracht vanuit de bron waardoor het systeem de wijzigingen overal toepast.		E
F.11.04.10	Per revalidant is duidelijk inzichtelijk wat diens voorschrift/behandelprogramma is en wat daarvan de inhoud is (activiteit, frequentie, periodiek of wekelijks).		E
F.11.04.11	Rapportage: inzichtelijk gemaakt kan worden hoeveel revalidanten er zijn ingepland per voorschriften/behandelprogramma's.		W
F.11.04.12	Het systeem kan rapportages leveren o.b.v. van verschillende variabelen (bijvoorbeeld beschikbaarheid therapeuten en middelen).		W
F.11.04.13	Het is mogelijk een duidelijk overzicht te vervaardigen van nog te plannen activiteiten per dossier/per cluster (verschil gevraagd, gepland).		E

4.11.5 Spreekuren- blokkenplanning

Spreekuren- blokkenplanning			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.05.01	Het systeem ondersteunt het aanmaken van terugkerende en verschillende spreekuren en afspraken (directe/indirecte en voorwaardescheppende tijd) (ritmes, ook met even/oneven weken).		E
F.11.05.02	Het systeem biedt de mogelijkheid om behandelaars te plannen op verschillende locaties/clusters, waarbij de verschillende locaties duidelijk herkenbaar zijn.		W
F.11.05.03	Het systeem biedt de mogelijkheid tot het plannen van meerdere interne en externe specialisten op één spreekuur (Multidisciplinair overleg).		W
F.11.05.04	Het systeem biedt de mogelijkheid tot het plannen van meerdere behandelaren op één behandelstijdstip (voor 1 cliënt) (combinatiebehandeling/interdisciplinair werken).		E
F.11.05.05	Het systeem biedt de mogelijkheid om een blokkenplanning toe te passen, waarbinnen, indien gewenst, behandelaren zelfstandig een detailplanning kunnen maken (planning multidisciplinair overleg).		W
F.11.05.06	Het systeem biedt de mogelijkheid tot het maken van groepsafspraken.		E
F.11.05.07	Groepen kunnen als groep opgeslagen en teruggevonden worden in het systeem. Deze kunnen worden herkend door het systeem en de planner en kunnen opnieuw gebruikt worden.		E
F.11.05.08	Het systeem kan o.b.v. een gepland spreekuur een agenda/overzicht genereren van de te bespreken revalidanten (overzichtslijst genereren).		W

F.11.05.09	Aan afspraken kunnen documenten worden toegevoegd, zoals in MS Outlook.		W
------------	---	--	---

4.11.6 Perspectieven en doorsneden

Perspectieven en doorsneden			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.06.01	Een agenda/de planning is te raadplegen vanuit verschillende perspectieven * Per cluster (ON/ OT/ AR) * Per afdeling * Per RAPA * Per periode (dag/week/ maand) * Per cliënt * Per diagnose * Per discipline * Per behandelaar * Per groep medewerkers * Per therapiemiddel of Locatie		E
F.11.06.02	Op basis van verschillende perspectieven (naast elkaar getoond) kan een overzicht getoond worden van de afspraken op basis van verschillende selectiecriteria.		E
F.11.06.03	De planning kan met verschillende tijdschalen worden gepresenteerd, waaronder minimaal een overzicht per 2 weken, per week en per dag.		W

4.11.7 Orders / Acties ten behoeve van planning

Orders / Acties ten behoeve van planning			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.07.01	Te plannen orders zijn chronologisch te tonen in een overzicht en in te stellen per medewerker, discipline en per activiteit. Dit overzicht bevat eveneens een zoekfunctie op trefwoord/datum enz.		W
F.11.07.02	Per order kan duidelijk worden aangegeven wat de status is en welke medewerker aan de order werkt of heeft gewerkt		E
F.11.07.03	Het overzicht met te plannen orders wordt automatisch geactualiseerd na het afhandelen.		E
F.11.07.04	Artsen kunnen spoedaanvragen in planafspraken (orders) van elkaar inzien.		W
F.11.07.05	Het systeem faciliteert het werken in de planmodule vanuit meerdere afdelingen/ organisatie-eenheden (vb Planningsafdeling en front-backoffice). Bij het plannen van activiteiten worden aangemaakte afspraken en wijzigingen daarop gelogd zodat duidelijk wie welke wijziging heeft gemaakt.		E

4.11.8 Correspondentie met betrekking tot planning

Correspondentie met betrekking tot planning			
Nummer	Details	Ja/Nee/Anders	E/W
F.11.08.01	Het systeem is in staat verschillende wacht- en doorlooptijden voor en van de revalidant te laten zien, vanaf inschrijving tot einde behandeling.		W
F.11.08.02	Het systeem kan na een gemaakte afspraak middels een muisklik direct door naar sjablonen voor aan te maken brieven, om te maken en te printen.		W

F.11.08.03	Het systeem genereert brieven voor verplaatste afspraken met vermelding van de oude én de nieuwe consult afspraak.		W
F.11.08.04	Het systeem biedt de mogelijkheid om voor geplande revalidanten een brief met de startdatum voor behandeling of geplande datum voor een consult te genereren.		E
F.11.08.05	Het systeem ondersteunt bij het printen van combinatiesets documenten, zoals bijvoorbeeld het afsprakenrooster/begeleidende brief/vragenlijsten, vanuit één scherm.		W
F.11.08.06	(Aangepaste) Roosters kunnen met een druk op de knop gedeeld worden met de revalidant (d.w.z. er hoeven niet eerst PDF's te worden gegenereerd, elders te worden opgeslagen om daarna te worden gedeeld als bijlage bij een email). Hiervoor biedt de applicatie een snelle en gebruikersvriendelijke toepassing.		E

4.12 Zorg Administratie

Zorgadministratie			
Nummer	Details	Ja/Nee/Anders	E/W
F.12.01.01	Automatische run voor overzicht Onder Handen Werk positie met peildatum voor aanlevering aan zorgverzekeraars via Vektis/Zorgprisma.		E
F.12.01.02	Mogelijkheid om volledige data uit het systeem te halen (direct of met behulp van BI tool) die naar de grouper moet om product definitief te maken en het tarief te bepalen.		E
F.12.01.03	In het systeem zit een geïntegreerd Tijdregistratiesysteem (TRS)		W
F.12.01.04	Lijst met niet gefiatteerd TRS uren (openstaande afspraken).		W
F.12.01.05	Koppeling vanuit dossier naar TRS om bij schrijven verslag automatisch indirecte tijd te berekenen per cliënt.		W
F.12.01.06	Er zijn mogelijkheden voor de verplichte aanleveringen voor DIS en DCM.		E
F.12.01.07	Mogelijkheid om bij facturatie zorgverzekeraars uit te sluiten (declareren op revalidantenniveau).		W
F.12.01.08	Mogelijkheid om voor een facturatie een test run te draaien.		W
F.12.01.09	Facturatie- en retourinformatie systeem met geïntegreerde koppeling naar Vecozo (facturatie en retouremeldingen)		E
F.12.01.10	Factureren buiten Vecozo om (bijvoorbeeld facturen aan de politie).		E
F.12.01.11	Mogelijkheid om retouremeldingen te crediteren en om te herfactureren.		W
F.12.01.12	Kunnen registreren van eigen ontwikkelde producten, anders dan de standaard zorgproducten (DBC/DOT).		E
F.12.01.13	Automatisch kunnen inlezen van Uzovi codes van de verzekeraar vanuit Vecozo.		E
F.12.01.14	Automatisch kunnen inlezen van de tarieven.		E
F.12.01.15	Verplichte Cov- en BSN check (koppeling met landelijke basis administratie).		E
F.12.01.16	Nachtverwerking Cov- en BSN check controle.		W
F.12.01.17	Controle lijsten (Cov- en BSN check) die volledigheid en juistheid van ingevoerde patiëntgegevens weergeven en waaruit direct gecorrigeerd kan worden.		W
F.12.01.18	Koppeling met landelijke artsentabel (exclusief MGD artsen) en instanties.		W
F.12.01.19	Alle controle- en rappellijsten in 1 menu/tegel/functierol		W
F.12.01.20	Inzicht in declaraties per patiënt (ingediend /afgehandeld/retour).		E

F.12.01.21	Alle aanpassingen in de dienst a.g.v. veranderingen in de Wet- en Regelgeving moeten centraal door de leverancier verwerkt worden (en niet door het MRC zelf).		E
F.12.01.22	Mogelijkheid tot het registreren van paralleliteit.		E
F.12.01.23	Het systeem moet in staat zijn een zelf geconfigureerde journaalpost te kunnen genereren.		E
F.12.01.24	Autorisatie op verwijderen van externe factuur nummers.		W
F.12.01.25	Mogelijkheid tot het raadplegen van de verzekeringshistorie van de patiënt.		W

4.13 Teamcommunicatie

4.13.1 Plannen Multidisciplinair overleg (MDO)

Plannen Multidisciplinair overleg (MDO)			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.01.01	Plannen met tijdsslots is mogelijk (specifiek de teamsamenstelling bij bespreking één cliënt).		E
F.13.01.02	Automatische uitnodiging naar patiënt en systeem (portaal).		W
F.13.01.03	Bij het plannen van een revalidant wordt door het systeem voorgesteld welke teamleden bij het MDO ingeroosterd moeten worden (koppeling aan behandelteam).		E

4.13.2 Voorbereiden MDO

Voorbereiden MDO			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.02.01	Het werken met een interdisciplinair revalidatieplan is mogelijk (overerving van informatie uit bv rapportages).		E
F.13.02.02	Interpretatie van de uitkomsten van klinimetrie wordt gefaciliteerd.		E
F.13.02.03	Inzichtelijk waar de revalidant in het behandeltraject en het DBC traject staat (vanuit BI tool).		E
F.13.02.04	Procesondersteunend door een signaalfunctie op verplichte velden.		E

4.13.3 Bespreken en besluitvorming MDO

Bespreken en besluitvorming MDO			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.03.01	Verslaglegging vanuit revalidatieplan d.m.v. overerving (te selecteren) gegevens.		E
F.13.03.02	Vanuit MDO verslaglegging direct communicatie met planbureau indien mutaties van invloed zijn op roosterwijzigingen.		E

4.13.4 Verslaglegging MDO

Verslaglegging MDO			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.04.01	Verslaglegging is gebaseerd op de ICF methodiek.		E
F.13.04.02	Vanuit revalidatieplan/verslaglegging is een brief met samenvatting te genereren voor de cliënt.		E
F.13.04.03	In het verpleegplan moet naar de doelen toe kunnen worden gewerkt (methodische verslaglegging).		E

4.13.5 Interdisciplinair

Interdisciplinair overleg			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.05.01	Interdisciplinaire digitale communicatie is mogelijk over revalidant gebonden handelingen.		E
F.13.05.02	Formulier is ondersteunend/ sturend t.a.v. de besprekpunten in MDO.		E

4.13.6 Behandelcommunicatie

Behandelcommunicatie			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.06.01	Inzichtelijk wanneer er nieuwe werkafspraken bij zijn gekomen of wijzigingen hebben plaatsgevonden.		E
F.13.06.02	Actiemodule interne mail/chatfunctie binnen systeem met logging en mogelijkheid tot toevoeging aan een revalidanten dossier.		E
F.13.06.03	Werkafspraken inclusief benaderingsafspraken/ risico's zijn inzichtelijk en gecentreerd op één locatie in het dossier		E
F.13.06.04	Doelen van de revalidant zijn inzichtelijk (prominent aanwezig in de views) en er kan melding van de status worden gemaakt		E
F.13.06.05	Teamleden dienen elkaars decursus te kunnen benaderen/ hebben inzage recht.		E
F.13.06.06	Video- en chatfunctie voor communicatie met revalidanten is beschikbaar (toekomst binnen patiënten portaal)		E
F.13.06.07	Templates voor standaard zinnen, brieven, mutaties, verzoeken, doelen (sjablonen raadplegen)		E

4.13.7 Informatieverstrekking

Informatieverstrekking			
Nummer	Details	Ja/Nee/Anders	E/W
F.13.07.01	Het is mogelijk om het verstrekken van informatie aan een patiënt te definiëren als een activiteit die door een zorgverlener (verpleegkundige, doktersassistente) moet worden uitgevoerd.		E
F.13.07.02	Het verstrekken van informatie kan worden opgenomen in werklijsten en zorgpaden, of deel uitmaken van een workflow.		E
F.13.07.03	Net als met andere taken is het mogelijk om af te vinken dat de informatie is verstrekt.		E
F.13.07.04	Informatiefolders MRC zijn vanuit systeem te verzenden.		E

4.14 Ordermanagement

Ordermanagement			
Nummer	Details	Ja/Nee/Anders	E/W
F.14.01.01	Een order kan verzonden worden wanneer het tijdstip van deze order nog niet vast staat		W
F.14.01.02	Het is mogelijk om een order een prioriteit mee te geven.		E
F.14.01.03	Het is mogelijk een uitgezette order te herroepen.		E
F.14.01.04	Het is mogelijk een uitgezette order te wijzigen.		E
F.14.01.05	Het systeem bevat specialisme specifieke ordersets voor veel voorkomende indicaties, orders en verzoeken.		E
F.14.01.06	Ordersets zijn door de gebruiker aan te passen.		E

F.14.01.07	Het is mogelijk om uitgevoerde orders automatisch aan verrichtingen te koppelen.		E
F.14.01.08	Het systeem maakt gebruik van digitale acties, taken en/of werklijsten om te zorgen dat ieder in het proces op het juiste moment zijn actie uit kan voeren en weer naar een ander overdraagt.		E
F.14.01.09	Het EPD kent een werklijstfunctionaliteit die door de functioneel beheerder flexibel is in te richten naar soort taaklijsten en bevoegde gebruikers.		E
F.14.01.10	De werklijsten kunnen worden ingedeeld naar: - persoonlijke lijsten; - beperkt gedeelde lijsten; - algemene lijsten; - automatische systeemlijsten (bv voor het kijken naar uitslagen uit deelsystemen per patiënt).		E
F.14.01.11	De werklijsten zijn minimaal te gebruiken voor de volgende processen (maar niet uitsluitend): - Aanmaken/autoriseren/verzenden van brieven; - Inplannen afspraken - Registreren, afhandelen, corrigeren DBC's - Patiënten klaarzetten voor multidisciplinaire bespreking bij de daarbij betrokken disciplines - Dagelijkse taken als patiënten terugbellen etc.		E
F.14.01.12	Vanuit de werklijst is het mogelijk om direct een activiteit te starten en de daarbij behorende relevante patiënten informatie te raadplegen.		E

4.15 Patiënten portaal

Patiënten portaal			
Nummer	Details	Ja/Nee/Anders	E/W
F.15.01.01	De revalidant kan zijn informatie (zoals wettelijk vastgesteld) via het portaal opvragen.		E
F.15.01.02	De behandelaar kan bepalen welke documenten (eigen formulieren MRC) inzichtelijk zijn voor de cliënt.		E
F.15.01.03	Cliënt kan zijn/haar eigen behandelplan digitaal accorderen (WGBO).		E
F.15.01.04	Eenvoudige en veilige inlogprocedure (bv. DigiD).		E
F.15.01.05	De revalidant (met of zonder tussenkomst behandelaar) kan derden autoriseren om mee te kijken in onderdelen van zijn of haar online dossier.		E
F.15.01.06	Cliëntportaal is responsive en te gebruiken op verschillende soorten apparaten (PC/laptop, tablet, telefoon) en met de gangbare besturingssystemen.		E
F.15.01.07	De leesbaarheid van de tekst op het cliëntportaal is flexibel aan te passen. Het portaal bevat een voorleesfunctie (o.a. voor alt text).		E
F.15.01.08	Een eenvoudige menustructuur die intuïtief is voor revalidanten. Duidelijke knoppen met zo min mogelijk tekst.		E
F.15.01.09	Cliënt of cliëntsysteem kan zelf bepaalde gegevens wijzigingen, zoals contactgegevens (o.a. telefoonnummer, e-mail), exclusief GBA gegevens.		W
F.15.01.10	Er is een download- en printfunctie aanwezig, zodat revalidant zijn eigen behandelplan, dossier en/of overzicht van afspraken kan printen en downloaden in een gangbaar bestandsformaat (bv. PDF).		E

F.15.01.11	Cliënt kan de medicatie die vanuit het EVS is voorgeschreven inzien en kan thuismedicatie als informatie gecontroleerd laten toevoegen.		E
F.15.01.12	Cliënt kan thuismedicatie als informatie gecontroleerd laten toevoegen.		W
F.15.01.13	Beheren van afspraken (aanvragen/annuleren/wijzigen) via portaal door cliënt.		W
F.15.01.14	De revalidant heeft recht om informatie toe te voegen aan het dossier, dus het portaal moet online deze mogelijkheid bieden. Hierbij moet er een optie zijn om deze mogelijkheid voor een individuele revalidant uit te zetten (bijvoorbeeld bij onbegrensd gebruik).		W
F.15.01.15	De revalidant kan middels een zoekfunctie zijn/haar gegevens doorzoeken in het dossier.		E
F.15.01.16	Alerts over afspraken, taken, medicatie, etc. naar keuze: sms/app/mail. Voorkeuren aanpasbaar door revalidant in portaal.		W
F.15.01.17	Het systeem moet de mogelijkheid bieden om informatie over diagnose, behandelmethodiek, praktische informatie, behandelteam, etc. via het portaal afgestemd op de behandeling van de revalidant te delen.		E
F.15.01.18	De mogelijkheid om geparametriseerd te bepalen wanneer er automatisch een account voor het revalidantenportaal / eHealth omgeving aangemaakt moet worden.		E
F.15.01.19	Het systeem voldoet aan de MedMij informatiestandaarden t.b.v. communicatie met de patiënt.		E
F.15.01.20	Alle mutaties en opvragen die door de revalidant zijn doorgevoerd moeten worden gelogd met initialen en datum/tijdstip.		E
F.15.01.21	Het portaal biedt mogelijkheden voor tele-consult (mag m.i.v. 2020 ook als normaal consult gebruikt worden).		E

4.16 Management rapportage

Managementrapportage			
Nummer	Details	Ja/Nee/Anders	E/W
F.16.01.01	De rapportages moeten overzicht bieden op het gebied van: • Personeelsgegevens (beschikbaarheid / productiviteit) • Agenda (Afspraken (op datum)) • Zorgverzekering (Betalende instanties) • Geregistreerde verpleegdagen • Zorgtraject (Inschrijving) • Subtrajecten (DBC) • Diagnose (dbc, ICD9/10) • Verwijzer (geen vaste koppeling tussen AGB persoon en instelling) • Hoofdbehandelaar • Zorgproductcode • Wachtlijst		E
F.16.01.02	Uitval-verrichtingen tonen: niet-gefiatiseerd, niet-gekoppeld, foutieve en onjuist geregistreerde verpleegdagen.		E
F.16.01.03	Financiële rapportages tonen o.a. omzet, aantallen, dbc's, zorgverzekeraar, etc.		E
F.16.01.04	Journalposten genereren t.b.v. het financieel pakket.		E
F.16.01.05	Het systeem biedt verschillende analytische toepassingen zoals forecasting, trendlijnen en andere statistische analyses.		E

F.16.01.06	Het behandelteam ondersteunen in het visueel maken van de informatiebehoefte (zoals uitputting van een DBC). Deze moet per functie/rol in te richten zijn.		E
F.16.01.07	Er dienen signaleringslijsten gedraaid te kunnen worden om de bedrijfsprocessen te kunnen borgen. Deze data moet toe te passen zijn in diverse rapportages.		E
F.16.01.08	Mogelijkheid om zelfstandig analyses uit te kunnen voeren om gerichte data te kunnen extraheren.		E
F.16.01.09	Geautomatiseerd anonieme data kunnen delen ten behoeve van KPI's, enzovoorts.		E
F.16.01.10	Het is met de juiste autorisatie mogelijk om voor specifieke doelgroepen rapportages te definiëren en uit te draaien in het kader van overdracht of informatievoorziening.		E
F.16.01.11	Overzicht bieden op het gebied van: • Inzet en percentage ongeplande zorg per periode per cliënt/cluster/ instelling • Capaciteitsproblemen: welke delen van een voorgeschreven zorgpad zijn niet ingepland of uitgevoerd • Uitputting DBC's • Gemiddelde verblijfsduur revalidanten (klinisch/ poliklinisch/ per diagnosegroep/ behandelprogramma etc) • Scores cliënttevredenheidsonderzoek		E
F.16.01.12	Het moet mogelijk zijn de gehele dataset of een sub-set te kunnen exporteren naar de BI omgeving van het MRC.		E
F.16.01.13	Het is mogelijk een overzicht van verwijzers te generen uit het systeem (aantal verwijzingen per verwijzer, per diagnose, etc).		E
F.16.01.14	De extractie van de basisset prestatie-indicatoren Revalidatiecentra is mogelijk		E
F.16.01.15	Het systeem heeft de mogelijkheid om de resultaten van een bepaalde groep te monitoren.		E
F.16.01.16	Er moet de mogelijkheid zijn om in te zoomen op of uit te zoomen van gegevens (van organisatieniveau tot patiënt niveau).		E

4.17 Generieke Services

4.17.1 Document Management

Document Management			
Nummer	Details	Ja/Nee/Anders	E/W
F.17.01.01	Het is mogelijk bijlagen digitaal vast te leggen.		E
F.17.01.02	Het is mogelijk documenten te koppelen aan een dossier.		E
F.17.01.03	Het is mogelijk vanuit het patiëntendossier gekoppelde documenten te raadplegen.		E
F.17.01.04	De dienst beschikt over een zoekfunctie om documenten op te zoeken.		E
F.17.01.05	Het is mogelijk van en naar het ZIS / R-EPD te scannen middels de scanstraat (JIM I-Fourc).		E
F.17.01.06	Het is mogelijk analoge dossiers van patiënten te digitaliseren.		E

4.17.2 Workflow Management

Workflow Management			
Nummer	Details	Ja/Nee/Anders	E/W
F.17.02.01	De dienst biedt mogelijkheden om de Workflow bij te stellen van minimaal:		W

	- Consult; - Voorschrift; - Recept verwerking.		
F.17.02.02	De dienst beschikt over een Workflow Engine die grafisch in te richten is.		W
F.17.02.03	De dienst beschikt over een Workflow Engine die toestaat custom workflows in te stellen.		W

4.17.3 Standaard Teksten

Standaard Teksten			
Nummer	Details	Ja/Nee/Anders	E/W
F.17.03.01	Het is mogelijk om teksten vast te leggen als Standaard Tekst.		E
F.17.03.02	Het is mogelijk om standaard teksten in te passen in tekstblokken.		E
F.17.03.03	Geef aan in hoeverre reeds bestaande Word-templates kunnen worden hergebruikt in het nieuwe systeem.		E
F.17.03.04	De dienst biedt spellingscontrole binnen vrije tekstvelden		E

4.18 Integraties & Add-ons

4.18.1 Integraties

Integraties			
Nummer	Details	Ja/Nee/Anders	E/W
F.18.01.01	De dienst is een volledig geïntegreerd systeem.		E
F.18.01.02	De dienst voldoet daar waar van toepassing aan de ZIB- en Medmij standaarden en leverancier realiseert toekomstige ontwikkelingen op dit gebied in het systeem		E
F.18.01.03	Integratie met LSP wordt ondersteund voor zowel het ophalen van het AMO, het versturen van het recept én alle toekomstige ontwikkelingen.		E
F.18.01.04	Integratie met VECOZO.		E
F.18.01.05	Integratie met Zorgmail (zowel ontvangen als verzenden).		E
F.18.01.06	Het ZIS ondersteunt gegevensuitwisseling door middel van secure e-mail functionaliteit.		E
F.18.01.07	Integratie met ZorgDomein.		E
F.18.01.08	Integratie met andere Zorgproducten van de Leverancier.		W
F.18.01.09	Integratie met DIS (NZA Data).		W
F.18.01.10	Integratie met Qlikview.		W
F.18.01.11	Integratie met Prismant (DBC Informatie Revalidatie).		W
F.18.01.12	Integratie met Grouper (DBC codes).		W
F.18.01.13	Integratie met KIS (IProva).		W
F.18.01.14	Integratie met Boekhoudpakketten.		W
F.18.01.15	Integratie met SBV-Z.		E
F.18.01.16	Integratie met MFB.		E
F.18.01.17	Integratie met spraakondersteuning bijvoorbeeld Dragon Naturally Speaking.		W
F.18.01.18	Koppeling I Document vanuit revalidanten dossier voor raadplegen protocollen.		W
F.18.01.19	Integratie met JIM I-Fourc.		E

F.18.01.20	Gangbare medische apparaten voor de uitgifte van medicatie, RR, spirometrie en ecg's kunnen worden gekoppeld aan het systeem. <i>Indien hierop uitzonderingen zijn (bijvoorbeeld merken of types die niet ondersteund worden) dan graag specificeren welke niet gekoppeld kunnen worden.</i>		W
F.18.01.21	Gangbare handscanners, desktopscanners en etiketprinters kunnen worden gekoppeld aan het systeem. <i>Indien hierop uitzonderingen zijn (bijvoorbeeld merken of types die niet ondersteund worden) dan graag specificeren welke niet gekoppeld kunnen worden.</i>		W

4.19 Gebruiksvriendelijkheid

4.19.1 Gebruiksvriendelijkheid

Gebruiksvriendelijkheid			
Nummer	Details	Ja/Nee/Anders	E/W
F.19.01.01	De dienst beschikt over een eenduidige opbouw, lay-out en gebruikswijze.		E
F.19.01.02	Het is mogelijk om Defensie huisstijlelementen zoals kleuren, logo's en lettertypen te configureren, voor zowel schermen als voor alle afdrukken.		W
F.19.01.03	Het is mogelijk om attributen van objecten en/of personen automatisch op te nemen in formulieren, velden en vensters.		W
F.19.01.04	Het is mogelijk om digitale informatie te uploaden.		E
F.19.01.05	Het is mogelijk om een verwijsbrief te genereren waarbij de aanhef van de patiënt en tekst(delen) uit SOAP kunnen worden hergebruikt.		E
F.19.01.06	Het is mogelijk om gegevens of combinaties van gegevens op te zoeken binnen dossiers.		E
F.19.01.07	Het is mogelijk om gegevens over lab resultaten, bloeddruk, ECG's en Röntgen te raadplegen.		E
F.19.01.08	Het is mogelijk om multimedia te raadplegen indien meegeleverd bij resultaten. Bijvoorbeeld foto's, grafieken en films.		W
F.19.01.09	Het is mogelijk om ingevoerde gegevens in een tabel en grafiek weer te geven.		W
F.19.01.10	Het is mogelijk om inkomende post te registreren.		E
F.19.01.11	Het is mogelijk om signaleringen te configureren waarmee zorgprofessionals automatisch worden geïnformeerd over het overschrijden van bepaalde drempelwaarden. Bijvoorbeeld het naderen en passeren van een verloopdatum van bepaalde documenten of certificaten.		E
F.19.01.12	Het is mogelijk om te navigeren vanuit overzicht naar details met behulp van hyperlinks, buttons, context-menu's, of submenu's.		E
F.19.01.13	Het is mogelijk om vanuit een agenda item een patiëntendossier te openen.		E
F.19.01.14	Het is mogelijk om vanuit tekst brieven en uitslagen te openen.		E
F.19.01.15	Het is mogelijk de dienst te bedienen via touchscreen.		W

F.19.01.16	De dienst biedt een intuïtieve en prettige ervaring bij het vastleggen van gegevens in verschillende velden en/of vensters en het overschakelen van velden en/of vensters.		E
F.19.01.17	De dienst biedt een intuïtieve en prettige ervaring gedurende het beheren van de episodelijst.		E
F.19.01.18	Het is mogelijk gegevens éénmalig vast te leggen en te hergebruiken.		E
F.19.01.19	De dienst biedt gebruikerservaring vanuit één scherm i.p.v. het veelvuldig moeten schakelen tussen vensters.		E
F.19.01.20	Het is mogelijk om een digitale Nederlandstalige helpfunctie te raadplegen.		E
F.19.01.21	De verschillende functionaliteiten van de dienst zijn eenduidig qua opbouw, lay-out en gebruik.		E
F.19.01.22	De dienst en documentatie zijn volledig Nederlandstalig.		E
F.19.01.23	De Leverancier ondersteunt het opleiden van zorgprofessionals in het gebruik van de dienst.		E
F.19.01.24	De Leverancier beschikt over een Plan van Aanpak waarin de methode en de manier(en) van opleiden is (zijn) beschreven. Denk hierbij aan de methode van opleiden (bijvoorbeeld train-de-trainer), de wijze van opleiden (bijvoorbeeld E-learning of contactonderwijs) en de locatie van opleiden. <i>Indien met Ja is beantwoord, dient de Leverancier dit aantoonbaar te maken door het aanleveren van een beschrijving van de door haar voorgestelde aanpak, waarin tenminste de leermethode(n), de opleidingsduur per (type) gebruiker en de doorlooptijd van het opleidingstraject zijn toegelicht en onderbouwd.</i>		E

4.20 Wet & Regelgeving & Standaarden

4.20.1 Wetgeving

De volgende wet- en regelgeving is van toepassing op de dienst. De Leverancier moet compliant zijn aan deze wet- en regelgeving en blijven.

Wetgeving			
Nummer	Details	Ja/Nee/Anders	E/W
F.20.01.01	Wet Cliëntenrechten bij elektronische verwerking van gegevens Waaronder digitaal inzage recht patiënten 4-10-2016 (implementatie voor 4-10-2019).		E
F.20.01.02	Wet Medezeggenschap Cliënten Zorginstellingen.		E
F.20.01.03	Militaire ambtenarenwet (MAW).		E
F.20.01.04	Algemeen Militair Ambtenarenreglement (AMAR).		E
F.20.01.05	Grondslagen, Hoofdlijnen en Systeemeisen voor de Militaire Gezondheidszorg (zoals bijv afwijkende bewaartermijnen)		E
F.20.01.06	Gezondheidswet.		E
F.20.01.07	Burgerlijk Wetboek (BW), artikel 7:454, lid 1.		E
F.20.01.08	Geneesmiddelenwet (2007).		E
F.20.01.09	Zorgverzekeringswet (2006).		E
F.20.01.10	Wet Algemene Bepalingen Burgerservicenummer (WABB) (21-07- 2007).		E
F.20.01.11	Wet gebruik Burgerservicenummer in de zorg (Wbsn-z).		E
F.20.01.12	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (10-04-2008/1 juli 2018).		E

F.20.01.13	Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz) 07-10-2015.		E
F.20.01.14	Wet op Bijzondere Medische Verrichtingen (24-10-1997).		E
F.20.01.15	Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) Aanpassing op Burgerlijk Wetboek (17 november 1994). Dit beschrijft verantwoordelijkheden en plichten van zorgverleners en zorginstellingen. De behandelaar sluit een behandelovereenkomst met de patiënt en heeft daarbij de plicht een dossier te voeren, de bewaartermijn in acht te nemen en geheimhoudingsplicht toe te passen (beroepsgeheim).		E
F.20.01.16	Algemene verordening gegevensbescherming (AVG) (25-05-2018).		E
F.20.01.17	Wet op de Beroepen in de Individuele Gezondheidszorg (BIG) (11-11-1993).		E
F.20.01.18	Wet op de Medische Hulpmiddelen (15-01-1970).		E
F.20.01.19	Opiumwet (12-05-1928) en aanverwante besluiten. Gelet op recept/voorschrijfverplichtingen rondom OW middelen, zoals het volledig uitschrijven van aantallen, 1 regel per recept, etc.		E
F.20.01.20	Wet marktordening gezondheidszorg (07-07-2006).		E
F.20.01.21	Wet toelating zorginstellingen (WTZI) (20-10-2005).		E
F.20.01.22	Noodwet Geneeskundigen.		E
F.20.01.23	Het systeem voldoet aan wettelijke eisen t.a.v. registratie. Zo volgt het ook de noodzakelijke/ verplichte registraties vanuit de branchevereniging. (bv KPI's)		E

4.20.2 Normen & Regelgeving

Normen & Regelgeving			
Nummer	Details	Ja/Nee/Anders	E/W
F.20.02.01	De dienst voldoet aan de wet en regelgeving voor Elektronisch Voorschrijven		E
F.20.02.02	De dienst voldoet aan Telemedicine norm NEN-8028 en de STANAG 2517 AMedP-5.3 Ed. A Ver. 1 DEVELOPMENT AND IMPLEMENTATION OF TELEMEDICINE SYSTEMS.		W
F.20.02.03	De dienst voldoet aan Richtlijn Overdracht Medicatiegegevens (basis voor G-Standaard).		W
F.20.02.04	De dienst voldoet aan management BSN conform SBV-Z.		W
F.20.02.05	De dienst voldoet aan WID controle.		
F.20.02.06	De dienst voldoet aan berichtenstandaard EDIFACT.		W
F.20.02.07	De dienst voldoet aan berichtenstandaard HL7 CDA v2-v3.		W
F.20.02.08	De dienst voldoet aan berichtenstandaard XDS.		W
F.20.02.09	De dienst voldoet aan de Militair Specifieke Richtlijn omtrent het uitwisselen van gegevens met NATO partners op basis van ICD-10/SNOMED-CT/HL7 CDA (STANAG 2543 AMedP-5.2 Ed. A Ver. 1 STANDARDS FOR DATA INTERCHANGE BETWEEN HEALTH INFORMATION SYSTEMS)		W
F.20.02.10	Leverancier committeert zich aan het realiseren van de benodigde functionaliteit (binnen de bijbehorende tijdslijnen) ten behoeve van het VIPP5 programma		E

5 Architectuur eisen en wensen

In de bijlage is de Project Start Architectuur (PSA) toegevoegd (zie Project Start Architectuur SBA MRC ZIS-R-EPD). De ZIS/R-EPD dienst moet aansluiten op de bijgevoegde PSA. De hieronder geformuleerde eisen en wensen zijn gebaseerd op de PSA. Zoals in de bijlage is aangegeven wordt de PSA SOLL architectuur verder uitgewerkt in de Fase I Opstarten (zie paragraaf 7.1) omdat deze afhankelijk is van de gekozen oplossing als gevolg van dit PvEW. Als in onderstaande teksten gesproken wordt over 'ondersteunen' dan wordt bedoeld dat de dienst het gestelde moet kunnen realiseren.

Als er gesproken wordt over 'dienst' is ook bedoeld het geautomatiseerde gedeelte van het informatiesysteem (de applicatie) of de technisch installeerbare programmatuur (de software).

5.1 Algemeen

De gevraagde dienst wordt voor de zorgprofessional en patiënt beschikbaar gesteld via de IT-infrastructuur van Defensie. De end-to-end dienstverlening bestaat uit meerdere, samenhangende diensten en meerdere leveranciers (waaronder Defensie zelf).

De IT-infrastructuur van Defensie is onder andere in verband met rubricering (specifieke defensie beveiligingseisen) afgeschermd. Het internet is ontsloten via een information exchange gateway. Uitwisseling van gegevens tussen de IT-infrastructuur van Defensie en het internet verloopt via een generiek koppelvlak.

5.2 MRC locatie

De gebouwen van het MRC te Doorn zijn uitgerust met werkstations, mobiele- en randapparatuur. De netwerkinfrastructuur bestaat uit bedrade en draadloze lokale netwerken en een WAN-infrastructuur gebaseerd op het Defensie NTN netwerk aangevuld met provider diensten (ethernet verbindingen, IP-VPN's, Internet). De WAN-infrastructuur biedt breedbandige verbindingen met een hoge beschikbaarheid en wordt momenteel uitgebreid met extra capaciteit.

5.3 Architectuur van de dienst

5.3.1 Dienst

Dienst			
Nummer	Details	Ja/Nee	E/W
A.03.01.01	De dienst moet zich conformeren aan de architectuur zoals beschreven in de bijlage PSA SBA MRC ZIS R-EPD. <i>Indien de vraag met Nee is beantwoord, beschrijf de afwijkingen en de eventuele alternatieve oplossingen.</i>		W
A.03.01.02	De gebruikersinterface (GUI) van de dienst is via een webbrowser te benaderen (webbased).		E
A.03.01.03	Indien de dienst is gebaseerd op client/server technologie moet de client gevirtualiseerd worden aangeboden op basis van Citrix technologie (Citrix receiver).		E
A.03.01.04	De dienst werkt correct in de meest recente versie van de Microsoft webbrowsers (Edge en Internet Explorer).		E
A.03.01.05	De dienst werkt correct in de meest recente versie van de Google webbrowser (Chrome).		W
A.03.01.06	De dienst werkt correct in de meest recente versie van de Firefox webbrowser.		W

5.3.2 Interfaces

Interfaces			
Nummer	Details	Ja/Nee	E/W
A.03.02.01	De dienst ondersteunt (near)realtime berichten uitwisseling via marktconforme berichten structuren (XML/SOAP of JSON/REST) met als transport mechanisme HTTPS (HTTP over TLS).		E
A.03.02.02	De dienst ondersteunt batch gebaseerde (bulk) informatie uitwisseling via marktconforme bestandsstructuren (XML, CSV) en met als transport mechanisme sFTP (FTP over SSH) of FTPs (FTP over SSL)..		E
A.03.02.03	De dienst maakt gebruik van open standaarden zoals vermeld op het forum voor standaardisatie (https://www.forumstandaardisatie.nl/).		W

5.3.3 Datacontrols

Datacontrols			
Nummer	Details	Ja/Nee	E/W
A.03.03.01	De dienst beschikt over een rollback mechanisme, waarmee wijzigingen in de database (een transactie) weer in de oorspronkelijke toestand teruggebracht worden.		E
A.03.03.02	De dienst ondersteunt transactiebewaking en dataherstel in geval van een verstoring (transactionele integriteit).		W
A.03.03.03	De dienst ondersteunt data-integriteit zoals bijvoorbeeld wordt afgedwongen via referentiële integriteit.		W
A.03.03.04	De dienst ondersteunt controle op de kwaliteit van de data-invoer op invoervelden.		W

5.4 Technische architectuur

5.4.1 Devices & Werkplek

Devices & Werkplek			
Nummer	Details	Ja/Nee	E/W
A.04.01.01	De dienst ondersteunt alle functies op mobiele devices (tablet, smartphone) van de platformen iOS & Android en is 'responsive' (schaalt naar de schermgrootte). <i>Indien de vraag met Nee is beantwoord, beschrijf per device type welke functies wel beschikbaar kunnen worden gesteld.</i>		W
A.04.01.02	De Leverancier beschrijft de technische requirements (systeemeisen) om gebruik te maken van ZIS/R-EPD en voegt deze toe aan de Offerte. De beschrijving bevat de technische requirements voor: • Werkplek voor zorgprofessionals; • Patiënten portaal. De Leverancier geeft aan, indien van toepassing, voor welke gewenste functionaliteit van de business er aanvullende en/of afwijkende requirements zijn.		E
A.04.01.03	De Leverancier is bereid technische issues, geconstateerd tijdens het verificatiegesprek en/of transitie opdracht 'beproeven', op te lossen vóór de transitie opdracht 'operationaliseren' (zie hoofdstuk 8 Transitie voor een uitleg).		E
A.04.01.04	De dienst voldoet aan de aansluitvoorwaarden zoals terug te vinden in bijlage D Technische requirements MRC.		W
A.04.01.05	<i>Indien vraag A.04.01.04 met Nee is beantwoord, geldt:</i> De Leverancier is bereid om non-conformities op te lossen vóór de transitie opdracht 'operationaliseren' (zie hoofdstuk 8 Transitie voor een uitleg hierover).		E

5.4.2 Randapparatuur

Randapparatuur			
Nummer	Details	Ja/Nee	E/W
A.04.02.01	De dienst ondersteunt het aansturen van een etikettenprinter.		E
A.04.02.02	De dienst ondersteunt het aansturen van een multifunctional/printer.		E
A.04.02.03	De dienst ondersteunt het koppelen met medische randapparatuur op basis van transport protocollen USB en netwerk/IP		E
A.04.02.04	De dienst ondersteunt het aansturen van een apotheek handscanner.		E

6 Transitie eisen en wensen

6.1 Inleiding

Het is de bedoeling dat op 30 september 2021 het nieuwe ZIS/R-EPD, ter vervanging van het systeem, volledig operationeel zal moeten zijn. Gezien deze planning vormt de transitie een kritisch onderdeel voor het welslagen van het project. Om die reden wil Defensie inzicht krijgen in de aanpak van de beoogd Leverancier voor de transitie.

6.1.1 Transitieonderdelen

Defensie heeft de transitie van dit project ingedeeld in de volgende onderdelen: configureren, koppelen, beproeven, migreren, operationaliseren en beheren.

Configureren:

Het samenstellen en inrichten van de gevraagde dienst ZIS/R-EPD en eventuele andere zaken die onderdeel uitmaken van de aangeboden dienst van de Leverancier.

Koppelen:

Het koppelen van de onderdelen welke deel uitmaken van de aangeboden dienst van de Leverancier met het koppelvlak van Defensie.

Beproeven:

Het grondig en zorgvuldig testen van de geconfigureerde en gekoppelde onderdelen van de door de Leverancier aangeboden ZIS/R-EPD-dienst.

Migreren:

Het migreren van data uit het huidige R-EPD en EVS naar het nieuwe ZIS/R-EPD. Op basis van een data-analyse zal worden vastgesteld welke data wel en niet mag worden gemigreerd naar het ZIS/R-EPD in het civiele domein.

Operationaliseren:

Het in gebruik nemen van het ZIS/R-EPD en het uitvoeren van de werkzaamheden die daarbij horen. Bijvoorbeeld het inrichten en toekennen van autorisaties en het opleiden van de gebruikers.

Beheren:

Het inrichten van het beheer van het ZIS/R-EPD en de andere onderdelen die deel uitmaken van de door de aanbieder aangeboden oplossing. Bijvoorbeeld het inrichten van de ITIL-processen tussen de Leverancier en Defensie maar ook het afronden van de SLA, DAP en DFA.

6.1.2 Beknopte omschrijving huidige ZIS/R-EPD

Het huidige ZIS systeem is een registratie systeem voor tweedelijns Revalidatie zorg. Doel van het systeem is het vastleggen van de verleende zorg aan zowel militairen als burgers.

Het systeem bestaat uit een aantal losse zelfstandige componenten die met elkaar op communiceren via een MIRTH communicatie server. Het betreft hierbij een ZIS, een R-EPD, een Tijdsregistratiesysteem en een Voorschrijfsysteem (EVS). Alle applicatie draaien lokaal en zijn dubbel uitgevoerd over twee gescheiden serverruimtes.

Ecaris

Het basis ZIS systeem, is de primaire gegevens bron en wordt aan de cliënt aangeboden als web applicatie

- Functies: Facturatie, planning
- Os: Oracle Linux Server release 7.6
- Data base: Oracle 12

REPD

Systeem waarin formulieren zijn gedefinieerd voor verslaglegging van het revalidatie proces.

- Systeem: Vital Health
- Os: Server 2012R2
- Database: Microsoft SQL 2014

TRS (Tijdsregistratie)

Systeem voor tijdsregistratie van de behandelaren

Voorschrijfsysteem

Systeem voor het voorschrijven van medicatie

6.2 Plan van Aanpak Transitie

Defensie ontvangt graag een Plan van Aanpak van de Leverancier waarin de onderstaande details staan beschreven.

Plan van Aanpak Transitie			
Nummer	Details	Ja/Nee	E/W
T.02.01.01	Beschrijf op basis van de transitieonderdelen configureren, koppelen, beproeven, migreren, operationaliseren en beheren een Plan van Aanpak (max 10 A4'tjes) waarin de volgende punten worden benoemd: • hoe de transitie per onderdeel wordt uitgevoerd; • de doorlooptijd in weken per onderdeel en de totale doorlooptijd van de transitie waarbij op 30 september 2021 het ZIS/R-EPD volledig operationeel moeten zijn; • de randvoorwaarden die Leverancier per onderdeel en de volledige transitie stelt waarbij rekening wordt gehouden met het PvEW; • indien van toepassing, welke gangbare standaarden per transitieonderdeel worden toegepast. Migreren: • welke migratiemethode zal worden toegepast en licht dat kort toe: dynamische migratie methode met knock-out, andere tool, handmatige migraties of anders.		W

6.3 Projectmanagement

Projectmanagement			
Nummer	Details	Ja/Nee	E/W
T.03.01.01	Leverancier werkt voor de transitie met een gestandaardiseerde projectmanagement methode die aansluit bij breed gehanteerde standaarden in de markt, zoals bijvoorbeeld Prince2.		W

7 Afkortingen

Afkorting	Uitleg
ABDO	Algemene Beveiligingseisen voor Defensie Opdrachten
AIS	Apotheek Informatie Systeem
AMA	Algemeen Militair Arts
AMAR	Algemeen Militair Ambtenarenreglement
AMV	Algemeen Militair Verpleegkundigen
AR	Arbeids Revalidatie
AVG	Algemene Verordening Gegevensbescherming
BA	Bedrijfsarts
BGZ	Bedrijfsgezondheidszorg
BI	Business Intelligence
BIG	Wet op de Beroepen in de Individuele Gezondheidszorg
BMB	Bijzondere Medische Beoordelingen
BN	Betrouwbaarheidsniveau
BSN	Burger Service Nummer
BW	Burgerlijk Wetboek
CAS	Classificaties voor Arbo en Sociale verzekering
CAT	Configuration Assessment Tool
CEAG	Coördinatiecentrum Expertise Arbeidsomstandigheden en Gezondheid
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CMH	Centraal Militair Hospitaal
COPD	Chronisch Obstructive Pulmonary Disease
COV	Controle op Verzekeringsnummer
DA	Doktersassistent(en)
DAP	Dossier Afspraken en Procedures
DBB	Defensie Beveiligingsbeleid
DBMS	Database Management Systeem
DFA	Dossier Financiële Afspraken
DGO	Defensie Gezondheidszorg Organisatie
DGOTC	Defensie Gezondheidszorg Opleidings- en Trainingscentrum
DIS	DBC Informatiesysteem
DMS	Document Management Systeem
DTD	Defensie Tandheelkundige Dienst
E	Eis
EASP	Europese Aanbesteding voor Standaard Programmatuur
ECG	Electrocardiogram
EGB	Eerstelijns Gezondheidszorgbedrijf
EGIZ	Elektronische Gegevensuitwisseling in de Zorg
EPD	Elektronisch Patiënten Dossier
EVS	Elektronisch Voorschrift Systeem
GC	Gezondheidscentrum
GIDS	Geneeskundig Informatiesysteem DefenSie
GUI	Gebruikersinterface
HA	Huisarts
HASP	Richtlijn Informatie-uitwisseling tussen Huisarts en Specialist
HGI	Hoog Gerubriceerde Informatiesystemen
HKZ	Harmonisatie Kwaliteitsbeoordeling in de Zorgsector
HRMS	Human Resource Management Systeem
ICD	International Statistical Classification of Disease and Related Health Problems
ICPC	International Classification of Primary Care
IDP	Identity Provider

IDR	Instituut samenwerking Defensie & Relatieziekenhuizen
KIS	Keten Informatiemanagement Systeem
KNMP	Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie
KNMG	Koninklijke Nederlandse Maatschappij tot bevordering der Geneeskunst
KPI	Kritische of Key Prestatie Indicator
LAB	Laboratorium
LOINC	Logical Observation Identifiers Names and Codes
LSP	Landelijk Schakelpunt
MAW	Militaire Ambtenarenwet
METC	Medisch Ethische Toetsingscommissie
MFB	Medisch Farmaceutische Beslisregels
MGGZ	Militaire Geestelijke Gezondheidszorg
MGLC	Militair Geneeskundig Logistiek Centrum
MRC	Militair Revalidatie Centrum
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NAVO	Noord-Atlantische Verdragsorganisatie
NAW	Naam, adres, woonplaats
NCvB	Nederlands Centrum voor Beroepsziekten
NCSC	Nationaal Cyber Security Centrum
NHG	Nederlands Huisartsen Genootschap
NIP	Nederlands Instituut van Psychologen
NSAID	Non-Steroidal Anti-Inflammatory Drugs
NTS	Nederlandse Triage Standaard
ON	Orthopedie Neurologie
OT	Orthopedie Trauma
OTAP	Ontwikkeling, Test, Acceptatie en Productie
OWASP	Open Web Application Security Project
PGO	Persoonlijke Gezondheidsomgevingen
PKB	Patient Knows Best
PKI-O	Public Key Infrastructure voor de Overheid
POH	Praktijkondersteuner Huisarts
POH GGZ	Praktijkondersteuner Huisarts Geestelijke Gezondheidszorg
POH S	Praktijkondersteuner Huisarts Somatiek
PREM	Patient Reported Experience Measure
PROM	Patient Reported Outcome Measure
PSA	Project Start Architectuur
PU	Productgerichte Uitvraag
PvEW	Programma van Eisen en Wensen
RAPA	Revalidatie Arts / Physician assistant
RBAC	Role Based Access Control
R-EPD	Revalidatie – elektronisch patiënten dossier
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLM	Service Level Management
SOC2	Service Organization Control 2
SOEP	Subjectief, Objectief, Evaluatie, Plan
STANAG	STANDARDization Agreement
TBB	Te Beschermen Belang
TRS	Tijd Registratie Systeem
UI	Uitgifte Informatie
UZI	Unieke Zorgverlener Identificatie
VDI	Virtual Desktop Infrastructure

VIR	Voorschrift Informatiebeveiliging Rijksoverheid
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
W	Wens
WABB	Wet Algemene Bepalingen Burgerservicenummer
Wbsn-z	Wet gebruik Burgerservicenummer in de zorg
WGBO	Wet op de Geneeskundige Behandelingsovereenkomst
Wkkgz	Wet kwaliteit, klachten en geschillen in de zorg
WTZI	Wet toelating zorginstellingen
ZIS	Ziekenhuisinformatiesysteem
ZRS	Zorgregistratiesysteem

8 Begrippenlijst

Begrip	Uitleg
Cluster	De zorg binnen het MRC is verdeeld in 3 clusters: AR (arbeidsrevalidatie), ON (Orthopedie Neuro) en OT (Orthopedie Trauma)
Cluster AR	Als werknemers te maken krijgen met fysieke of mentale belemmeringen die kunnen leiden tot uitval op het werk, ondersteunt de afdeling Arbeidsrevalidatie de verwijzer en werknemer. Wij staan bekend om onze unieke en gespecialiseerde begeleiding van militairen, maar onze diagnostiek, training en re-integratiebegeleiding is toegankelijk voor alle werknemers van zowel binnen als buiten Defensie.
Cluster ON	Ortho-neuro staat voor orthopedie-neurologie. Het wordt ook wel afgekort naar het cluster ON. Dit cluster houdt zich bezig met revalidanten die komen revalideren voor een aandoening die neurologisch is (een aandoening die te maken heeft met de hersenen, de zenuwen of het ruggemerg). Het MRC behandelt in principe alleen revalidanten waarbij de neurologische aandoening niet aangeboren is. Binnen het cluster ortho-neuro werken verschillende vakgroepen. Een vakgroep is namelijk niet gebonden aan één specifiek cluster, maar een therapeut kan wel gebonden zijn aan een cluster. Zo heb je fysiotherapeuten die onder het cluster ortho-neuro werken en fysiotherapeuten die onder het cluster ortho-trauma werken. Hetzelfde geldt voor ergotherapeuten, sporttherapeuten, et cetera.
Cluster OT	Ortho-trauma staat voor orthopedie-traumatologie. Het wordt ook wel afgekort naar het cluster OT. Dit cluster houdt zich bezig met revalidanten die komen revalideren voor een aandoening die door een trauma is ontstaan (een aandoening als gevolg van geweld of een ongeluk). Het verschil met ortho-neuro is dus dat de aandoening niet (direct) te maken heeft met de hersenen, het ruggemerg of de zenuwen. Binnen het cluster ortho-trauma werken verschillende vakgroepen. Een vakgroep is namelijk niet gebonden aan één specifiek cluster, maar een therapeut kan wel gebonden zijn aan een cluster. Zo heb je fysiotherapeuten die onder het cluster ortho-trauma werken en fysiotherapeuten die onder het cluster ortho-neuro werken. Hetzelfde geldt voor ergotherapeuten, sporttherapeuten, et cetera.
Dienst	De beoogde oplossing voor Defensie waarvoor in dit PvEW de eisen en wensen zijn geformuleerd (ZIS/R-EPD).
ZIS/R-EPD	De dienst wordt in dit document ZIS/R-EPD genoemd en wordt gebruikt onder reguliere omstandigheden.
In werkelijke dienst	Actief dienende militair
Krijgsmachtdelen	Onder de krijgsmachtdelen worden de Koninklijke Landmacht, de Koninklijke Luchtmacht, de Koninklijke Marine en de Koninklijke Marechaussee verstaan
Leverancier	De partij, onderaannemer, met wie de Opdrachtnemer mogelijk een contract gaat sluiten ten bate van de ZIS/R-EPD-dienst voor Defensie.
leverancier	Onderaannemer van de Leverancier.
Opdrachtnemer	De partij met wie, door het Ministerie van J en V, mede namens Opdrachtgever FU, een Raamovereenkomst is afgesloten in het kader van Standaard Programmatuur (EASP2017).
STANAG	In de NAVO (Noord-Atlantische definieert een standaardisatie-overeenkomst (STANAG) processen, procedures, voorwaarden en voorwaarden voor gemeenschappelijke militaire of technische procedures of apparatuur voor samenwerking tussen de lidstaten van de alliantie.

Bijlage A Verificatiegesprekken

A.1 Algemeen

A.1.1 Inleiding

De beoogd Leverancier wordt uitgenodigd voor een verificatiegesprek. Het doel van deze verificatiegesprekken is een verduidelijking te krijgen op een aantal specifieke onderwerpen uit dit PvEW en de onderdelen uit de Offerte zoals deze door de Leverancier(s) is aangeboden.

Het betreffen hierbij onderwerpen die volgens Defensie aanvullende en specifieke aandacht vragen omdat zij het welslagen van de samenwerking, de uitvoering en het toekomstig gebruik kunnen verstoren. Op grond van de verificatiegesprekken vindt geen beoordeling plaats, hooguit een toetsing van de resultaten van de beoordeling van de Offerte.

In totaal worden maximaal 7 onderwerpen besproken voor maximaal 2 uur

- financiële aspecten van de Offerte/verstrekke kostenmodel;
- juridische voorwaarden/contractuele aspecten;
- functionaliteiten van de aangeboden dienst op basis van dit PvEW;
- technische aspecten van de aangeboden dienst op basis van dit PvEW;
- informatiebeveiliging- en privacyaspecten van de aangeboden dienst op basis van dit PvEW;
- service- en contractmanagement aspecten van de aangeboden dienst op basis van dit PvEW;
- transitie aspecten van de aangeboden dienst op basis van dit PvEW.

A.2 Verificatiegesprekken

A.2.1 Planning

Zie Productgerichte Uitvraag

Bijlage B Proof of Concept

B.1 Algemeen

B.1.1 Inleiding

Deze bijlage omvat de benodigde informatie over de Proof of Concept (hierna te noemen als 'PoC'), in het kader van de aanbesteding van een Ziekenhuis Informatiesysteem (ZIS) in combinatie met een Elektronisch patiëntendossier (EPD) en Elektronisch Voorschrijf systeem (EVS) door het Militair Revalidatiecentrum van de MGZ van Defensie. In deze bijlage worden de geldende procedures nader toegelicht en wordt de noodzakelijke informatie verstrekt om u als Leverancier in staat te stellen de PoC gedegen voor te bereiden.

B.1.2 Doelstelling

De PoC is erop gericht om aan de hand van de praktijkcasuïstiek te verifiëren in hoeverre de aangeboden dienst daadwerkelijk in overeenstemming is met de gevraagde minimale functionaliteit zoals uitgewerkt in dit PvEW.

B.2 Procedure

B.2.1 Proces PoC

Defensie zal de Leverancier uitnodigen om op basis van deze bijlage de PoC voor te bereiden. Defensie zal de definitieve set van use cases voor de start van de PoC beschikbaar stellen aan de Leverancier. Voor de start van de PoC zal er tevens een kick-off meeting plaatsvinden met het testteam van Defensie en de betrokken medewerkers van de Leverancier.

B.2.2 Planning

Zie Productgerichte Uitvraag

B.2.3 Faciliteiten

De Leverancier stelt de onderstaande faciliteiten beschikbaar aan Defensie gedurende de uitvoering van de PoC:

- een afgescheiden ruimte met 10 tot 15 werkplekken voor het testteam van Defensie dat de PoC zal gaan uitvoeren;
- toegang tot internet;
- whiteboard en presentatiemogelijkheden;
- supportteam van de Leverancier om het testteam van Defensie te ondersteunen bij vragen en het oplossen van issues gedurende de gehele PoC.

B.3 Beschrijving Proof of Concept

B.3.1 Inleiding

Het doel dat Defensie met de PoC nastreeft, is het verifiëren in hoeverre de aangeboden dienst daadwerkelijk in overeenstemming is met de gevraagde functionaliteiten zoals uitgewerkt in dit PvEW. Om dit mogelijk te maken stelt de beoogd Leverancier een ZIS/R-EPD-omgeving beschikbaar gedurende de uitvoering van de PoC door Defensie.

B.3.2 Doorlopen casuïstiek

Voor de start van de PoC zal Defensie de definitieve set van use casussen aan de Leverancier beschikbaar stellen. Dat geldt ook voor het beoordelingsproces en de totstandkoming van de eindbeoordeling van de PoC.

Bijlage C Performance Indicatoren

ZIS/R-EPD		Kant leverancier	Productie	Acceptatie	Leeromgeving	Samengestelde dienst met Defensie	Voorbeelden
Technisch	Beschikbaarheid	Openstelling	7*24	5*11	5*11		
		Openstelling tussen uren maandag-vrijdag	-	07:00-18:00	07:00-18:00		
		Beschikbaarheid	98.0%	97.0%	97.0%		
		Maximaal aantal uur op basis van beschikbaarheid	717	253	253		
		Maximale cumulatieve duur downtime per maand	15	8	8		
		Cumulatieve downtime PROD veroorzaakt door incidenten mag niet meer zijn dan (uur)	12	6	6		
		Cumulatieve downtime PROD veroorzaakt door changes mag niet meer zijn dan (uur)	3	2	2		
					0		
		Recovery Time Objective (downtime bij calamiteit (bijvoorbeeld brand stroomstoring waterschade et cetera))	1 dag	5 dagen	5 dagen		
	Backup & Restore systemen	Maximale dataverlies (RPO)	15 min	1 dag	-		Backup strategie procedure bijvoorbeeld: Full per 6 uur incremental per uur LOG bestanden per kwartier.
		Bewaartermijn backup	1 jaar	30 dagen	-		Backup strategie procedure bijvoorbeeld: incremental daily full backup weekly full backup montly full backup yearly.
		Testen restore procedure backup	elke 4 weken	elke 4 weken	-		
		Transactie logging en transactie herstel	<1 sec	<1 sec	<1 sec		
	Performance	Performance (responsstijd schermen)	<1 sec	<1 sec	<1 sec	JA	
		Concurrent users als percentage van het totaal aantal gebruikers	60%	5%	5%		60% concurrent users leverancier moet in staat zijn op te schalen (versneld) op verzoek van Defensie
Functioneel		Wijzigingen Wet- en Regelgeving doorvoeren in <i>Tijd benodigd om software fouten (bugs) te verhelpen ontwikkelingproces</i>	< 21 dagen 1 maand	< 14 dagen 1 maand	- 1 maand		
Regulier onderhoud/beveiliging aan bouwstenen	Onderliggende operating systems	Kritieke security patches op operating systems geïmplementeerd na uitkomen bij leverancier	-	< 48 uur	< 48 uur		
		<i>Tijd na uitkomen bij leverancier en na uitvoering kritieke security patches op Acceptatie)</i>	<96 uur	-	-		Testen van invloed security patches op stabiliteit van het systeem alvorens door te voeren in productie.
		Patches operating systems in acceptatie geïmplementeerd na uitkomen bij leverancier	-	< 7 dagen	<14 dagen		
		<i>Tijd na uitkomen bij leverancier en na uitvoering kritieke security patches op Acceptatie)</i>	<21 dagen	-	-		Testen van invloed security patches op stabiliteit van het systeem alvorens door te voeren in productie.
		Percentage bouwstenen van de dienst welke niet compliant zijn met de afgesproken Patch policy	5%	5%	5%		5% is niet compliant aan patchlevel zoals deze is beschreven in de Patch policy
		Uitvoeren new releases operating systems	releaseplan	releaseplan	releaseplan		
	ZIS/R-EPD software systeem	Kritieke security patches ZIS/R-EPD acceptatie geïmplementeerd	-	< 48 uur	< 48 uur		
		<i>Tijd na uitkomen bij leverancier en na uitvoering kritieke security patches op Acceptatie)</i>	< 96 uur	-	-		Testen van invloed security patches op stabiliteit van het systeem alvorens door te voeren in productie.
		Uitvoeren new releases ZIS/R-EPD	releaseplan	releaseplan	releaseplan		
		Percentage overtijd van geplande releases (vanuit releaseplan OS en ZIS/R-EPD)	10%	10%	10%		
Monitoring / capaciteit		Percentage van configuratie Items dat wordt gemonitord op performance	100%	00%	85%		Servers storage netwerkcomponenten et cetera
		Percentage capaciteit reserves bij normaal gebruik	>30%	>30%	> 0%		Processor capaciteit geheugen diskruimte etc.
		Percentage minimale reserve bouwstenen dienst	20%	20%	20%		Processor capaciteit geheugen diskruimte etc.

Commercieel vertrouwelijk

Definitief – Programma van Eisen en Wensen – Project Vervanging ZIS & R-EPD MRC – 26-08-2020

Koppelingen		Productie	Acceptatie	Leeromgeving		
Leveren koppelingen met Defensie systemen		Beschikbaarheid koppeling tussen Leverancier en Opdrachtgever	98 0%	97%	97%	
	Openstellingstijd koppelingen tussen Leverancier en Opdrachtgever	7*24	5*11	5*11	JA	Dit betreft de technische verbinding tussen Leverancier en Opdrachtgever.
	Maximale downtime van koppeling tussen Leverancier en Opdrachtgever	< 2u	< 1 dag		JA	
	Maximale downtime van koppeling tussen ZIS-R-EPD en			-	JA	
	i. Landel jk Schakelpunt	< 2u	< 1 dag			
	ii. Zorgdomein	< 1 dag	< 1 dag			
	iii. Zorgmail	< 4u	< 1 dag			
	iv. VECOZO	< 4u	< 1 dag			
	v. SBV-Z	< 4u	< 1 dag			
Expertise & Support		Productie	Acceptatie	Leeromgeving		
Service desk Leverancier		Openstellingstijd servicedesk	7*24	5*11	5*11	JA
	Bevestiging met referentie nummer	15 min	15 min	15 min		
	Herstellen incidenten Prioriteit 1 (definitie incident)	< 2 uur	-	-	JA	Tijd loopt na melding SDD defensie bij servicedesk Leverancier
	Rootcause analyse Report Prioriteit 1	< 48 uur	-	-		
	Incidenten prioriteit 1 hersteld binnen herstellenvenster	90%	-	-		
	Herstellen incidenten Prioriteit 2	< 4 uur	< 4 uur	< 4 uur	JA	Tijd loopt na melding SDD defensie bij servicedesk Leverancier
	Incidenten prioriteit 2 hersteld binnen herstellenvenster	85%	85%	75%		
	Herstellen incidenten Prioriteit 3	< 1 dag	< 1 dag	< 1 dag	JA	Tijd loopt na melding SDD defensie bij servicedesk Leverancier
	Incidenten prioriteit 3 hersteld binnen herstellenvenster	80%	80%	70%		
	Melden beveiligingsincidenten na constatering	< 1 uur	< 1 uur	< 1 uur		
	Leveren rapportages ten behoeve van monitoring toegang na verzoek	< 4uur	< 8 uur	-		
	Loggegevens over een (vermoed) incident blijven bewaard	5 jaar	5 jaar	5 jaar		
Performance						
	Percentage van PI SLA niet gehaald	5%	10%	20%		
	Percentage incidentafhandeling op tijd	90%	85%	85%		
	Percentage change requests openstaand	10%	15%	20%		
	Percentage succesvolle software upgrades	99%	95%	85%		
	Percentage wijzigingen "first time right"	99%	95%	85%		
	Percentage wijzigingen met vertraging door afhankelijkheid Opdrachtgever	1%	1%	1%		
	Percentage wijzigingen met vertraging door derden (bijvoorbeeld ISP)	1%	1%	1%		
	Percentage standaard wijzigingen versus niet standaard wijzigingen	80%	80%	80%		
	Percentage capaciteit resources bij normaal gebruik	85%	90%	95%		
	Percentage meldingen minimale reserve resources worden overschreden.	1%	10%	20%		

Bijlage D Technische eisen MRC

D.1 Technische eisen ZIS/R-EPD

Technische eisen van de werkplek voor zorgprofessionals die gebruik maken van ZIS/R-EPD voldoet minimaal aan;

- De dienst is webbased en heeft geen installatie van extra componenten nodig;
- De dienst dient onafhankelijk van de werkplek te functioneren. Dongels of werkplek gebonden licenties zijn niet toegestaan;
- De webapplicatie functioneert volledig in de browser, ofwel geen gebruik van ActiveX of vergelijkbare componenten;
- De dienst dient geschikt te zijn voor de volgende platformen en versies daarvan;
 - Windows 10 (Enterprise) (64-bits)
 - Internet Explorer 11 (64-bits)
 - Microsoft Edge 44 (64-bits)
 - Mozilla Firefox 45 (64-bits)
 - JRE 8 (1.8) (64-bits)
 - Microsoft Office 2010 of hoger (Outlook; Word; PowerPoint en Excel)
- Protocollen voor datakoppelingen met de dienst (buiten het Defensielandschap):
 - HTTPS
 - sFTP (FTP over SSH)
 - FTPs (FTP over SSL)
 - FTP
- Protocollen en standaarden voor Servicebased koppelingen met de dienst (buiten het Defensielandschap)
 - WSDL en XSD
 - SOAP 1.1 en 1.2
 - REST
 - HTTP 1.1
 - WS-Addressing
 - WS-Security
 - MTOM/XOP

Bijlage E Project Start Architectuur

Zie separaat document: Project Start Architectuur (PSA) ZIS-R-EPD MRC SBA, v0.7 dd 25-6-2020