Ministerie van Buitenlandse Zaken

Algemene Beveiligingseisen Buitenlandse Zaken Opdrachten (ABBO)

Datum November 2018

Colofon

Den Haag

DBV/IV
Informatievoorziening (DBV/IV) | Directiebedrijfsvoering
T- 070-3486379.

Inhoudsopgave

Voorwoord

Het Ministerie van Buitenlandse Zaken (BZ) werkt in binnen- en buitenland voor de belangen van Nederland en Nederlanders. BZ doet dit door het onderhouden van de juiste verbindingen tussen mensen,

informatie, overheden en organisaties.[1] ICT speelt een kritieke rol in het functioneren van BZ als een flexibele netwerkorganisatie. BZ verzorgt haar ICT-dienstverlening niet alleen, BZ heeft de strategische keuze gemaakt om haar IT in hoge mate resultaat gebaseerd uit te besteden. Een leverancier heeft daarom zicht op een of meerdere operationele processen van BZ. Vanuit IT–technisch en –sturingsperspectief is een leverancier in staat om invloed uit te oefenen op de kwaliteit van het proces, waaronder informatiebeveiliging. Uitbesteding met resultaatverplichting verhoogt het risico dat het voldoen aan informatiebeveiligingseisen onvoldoende wordt aangetoond. Daarom verwacht BZ een coöperatieve en pro-actieve IB-houding van de leveranciers. Concreet verlangt BZ van haar leveranciers om periodiek aan te (laten) tonen dat wordt voldaan aan de overeengekomen informatiebeveiligingseisen. In dit document staat het pakket van wensen en eisen m.b.t. informatiebeveiliging waaraan de ICT leveranciers moeten voldoen.

Dit pakket van informatiebeveiligingseisen is van belang omdat bij sommige opdrachten die BZ uitbesteedt krijgen deze bedrijven te maken met de zorg voor gerubriceerde informatie. Bedrijven beseffen soms niet de economische en strategische waarde van de informatie. In deze situatie is het nog essentiëler dat goede afspraken worden vastgesteld over het delen en beschikbaar stellen van gerubriceerde informatie. Deze informatie is kwetsbaar voor spionage en de nationale veiligheid kan in het geding komen. Een opdracht wordt alleen uitbesteed als er voldoende zekerheid is dat een bedrijf voldoet aan een adequate informatiebeveiliging op basis van BZ voorschriften en beveiligingseisen.

De Algemene Beveiligingseisen Buitenlandse Zaken Opdrachten (ABBO) is gebaseerd op het concept Algemene Beveiligingseisen Defensie Opdrachten (ABDO) van het Ministerie van Defensie. BZ specifieke karakter en wensen vragen bepaalde maatregelingen en aanpassingen aan de ABDO. Bijvoorbeeld door het internationale karakter van BZ heeft het ministerie veel te maken met internationale bedrijven of bedrijven met internationale investeerders. Het is niet altijd wenselijk om volledig Nederlandse partners te vinden voor aanbestedingen. Verder ligt de noodzaak voor vertrouwen vooral bij ICT-leveranciers die de ICT-dienstverlening van BZ uitvoert. Dit project beperkt zich in eerste instantie tot ICT-leveranciers. Aanpassingen zullen vooral plaats vinden op het gebied van IT-beveiliging en het internationale aspect voordat BZ een Te Beschermen Belangen (TBB) aan ICT-leveranciers toe vertrouwt.

[1] BZ introductiedossier

Inleiding

De huidige IT-infrastructuur van BZ past niet meer bij de huidige manier van werken. In de komende 3 jaar lopen contracten voor onze wereldwijde netwerken (WWAN) en de applicatie beheer en hosting af. In 2017 t/m 2019 gaat BZ meerdere aanbestedingen doen op het gebied van ICT om de next generation voor de IT-infrastructuur te ontwikkelen. De I-strategie van BZ 2016-2019 benoemt "aansluiten op de wereld van morgen" als strategisch doel voor BZ. Het ministerie streeft er na door samen met ICT-leveranciers de IT-infrastructuur van BZ te verbeteren zodat deze aansluit op de huidige manier van werken. BZ heeft draagvlak vanuit de door het SG/DG-beraad gekozen voor een koers naar een meer open informatievoorziening onder het motto Open, tenzij vastgesteld in 2012. Eind 2016 is er nieuw leven in het programma "Open Tenzij" geblazen om onder dit motto de IT-infrastructuur te vernieuwen. Daarnaast met de hedendaagse dreiging van statelijke actoren is het voor BZ van belang om haar informatiebeveiliging op orde te hebben. Het ministerie van Buitenlandse Zaken heeft de strategisch keuze gemaakt om grote delen van de uitvoering van haar ICT-dienstverlening uit te besteden aan bedrijven. Om een nieuwe veilige IT-infrastructuur te ontwikkelen/bouwen is samenwerking met ICT-leveranciers essentieel. Bij sommige opdrachten die BZ uitbesteedt krijgen deze bedrijven te maken met de zorg voor gerubriceerde informatie. In deze situatie is vertrouwen nodig, de ABBO-status dient als grondbeginsel voor een partnerschap. Het ABBO document is verdeelt in vier delen: Bestuur en Organisatie, Personeel, Fysiek, en Digitaal. Ten aanzien van de

verschillende rubriceringsniveaus zullen bij dat niveau passende beveiligingseisen gesteld worden. De tabel geeft aan welke eis tot welke rubriceringsniveau behoort.

Samenvattend, voor beveiliging van informatie, materieel, goederen en objecten die door BZ aan orderbedrijven zijn toevertrouwd of aldaar worden geproduceerd, wordt door de BZ de Algemene Beveiligingseisen Buitenlandse Zaken Opdrachten opgelegd om ongewenste kennisname of beïnvloeding door derden te voorkomen. De ABBO vormt de basis-set van maatregelen die het risico moet reduceren tot een voor BZ aanvaardbaar restrisico.

De ABBO 2018 verplicht het bedrijf contractueel tot implementatie van adequate beveiligingsmaatregelen en de eisen die worden gesteld dienen middels verwijzing in contracten en overeenkomsten naar het ABBO 2018, van toepassing te worden verklaard.

Hoofdstuk 1: Toepassing ABBO

1.1 Inleiding

Bij overeenkomsten tussen het ministerie van Buitenlandse Zaken en de private sector wordt een TBB aan een bedrijf toevertrouwd of aldaar gegenereerd.

Daarbij wordt er van uitgegaan, al dan niet contractueel vastgelegd, dat beide partijen deze TBB zorgvuldig en vertrouwelijk zullen behandelen en beveiligen. Beveiligen brengt meestal extra werkzaamheden en daardoor extra kosten met zich mee. Ook kan het leiden tot inbreuken op de persoonlijke levenssfeer omdat een veiligheidsonderzoek verricht moet worden ter beoordeling van de vraag of een persoon in aanmerking kan komen voor de vervulling van een Vertrouwensfunctie. Daarom worden bij het beveiligen altijd twee uitgangspunten gehanteerd, hetgeen wil zeggen dat er pas beveiligings-maatregelen worden getroffen indien:

- er risico's aanwezig zijn die dat rechtvaardigen;
- het samenhangend pakket van beveiligingsmaatregelen zodanig is ingericht dat zo min mogelijk inbreuk hoeft te worden gemaakt op de privacy.

1.2 Risicomanagement ABBO

Het doel van risicomanagement is het identificeren van dreigingen jegens de TBB-en, 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 functioneren van het ministerie. Kortweg: risico = kans x effect.

Bij de opzet van de beveiligingseisen in de ABBO 2018 is uitgegegaan van het restrisico dat de opdrachtgever, zijnde het ministerie, aanvaardt.

Voor de vaststelling van het restrisico heeft het ministerie alle informatie, materieel, goederen en objecten op basis van een risicoanalyse ingedeeld in vier categorieën Te Beschermen Belang (TBB 1 t/m TBB 4, waarbij TBB 1 de zwaarst te beveiligen categorie is). Deze indeling is gebaseerd op de schade voor veiligheid en andere gewichtige belangen van de Staat en haar bondgenoten en op de aantasting van de bedrijfsvoering van BZ en haar bondgenoten. Op basis van de door het ministerie gestelde betrouwbaarheidseisen, de ingeschatte dreiging en een kosten/baten afweging is in de ABBO 2018 per TBB-categorie een set beveiligingsmaatregelen opgenomen die moet voorkomen dat bedrijfsprocessen van het ministerie (en de daaronder ressorterende uitvoeringsorganisaties) stagneren en dat de Staat of haar bondgenoten onaanvaarbare schade lijden.

Risicomanagement houdt ook in dat medewerkers, betrokken bij de industrie, die in aanraking komen met een TBB door middel van voorlichting en training bewustzijn en medeverantwoordelijkheid ontwikkelen en onderhouden betreffende de noodzaak tot beveiligen van TBB-en.

Omdat omstandigheden en dreigingen voortdurend aan wijzigingen onderhevig zijn is risicomanagement een cyclisch proces dat door de toezichthoudende instantie en vertegenwoordigers van de industrie periodiek moet worden uitgevoerd. Dergelijke wijzigingen kunnen derhalve aanleiding zijn het beveiligingsniveau bij te stellen. Het voorschrift ABBO 2018 beschrijft de minimale beveiligingseisen en -maatregelen die het onderkende risico reduceren tot een voor de BZ aanvaardbaar restrisico.

De opdrachtnemer kijkt in overleg met BZ per situatie welke normen van toepassing zijn en welke maatregelen dienen te worden genomen. Omdat de omstandigheden altijd aan verandering onderhevig zijn, moet dit proces regelmatig worden herhaald.

1.3 Bijzondere Informatie

Bedrijven die opdrachten uitvoeren voor krijgen daartoe vanuit BZ informatie verstrekt. Informatie die is voorzien van een rubricering wordt Bijzondere Informatie (BI) genoemd. BI wordt onderscheiden in Staatsgeheime en niet-Staatsgeheime BI. Er is sprake van een

Staatsgeheim als het belang van de Staat of zijn bondgenoten in het geding is en indien kennisname door niet-gerechtigden kan leiden tot schade aan deze belangen. Er is sprake van niet-Staatsgeheime BI indien kennisname door niet-gerechtigden kan leiden tot nadeel aan het belang van één of meer ministeries of bondgenoten.

1.4 Rubriceringen en merkingen

In de tabel hiernavolgend zijn de vier mogelijke rubriceringen opgenomen met de overeenkomstige TBB-categorie.

NL *Rubricering*	*TBB* categorie	Betekenis
Stg.ZEER GEHEIM	*TBB* 1	Kennisname door niet-gerechtigden kan zeer ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.
Stg. GEHEIM	*TBB* 2	Kennisname door niet-gerechtigden kan ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.
Stg. CONFIDENTIEEL	*TBB* 3	Kennisname door niet-gerechtigden kan schade toebrengen aan het belang van de Staat of zijn bondgenoten.
DEPARTEMENTAAL VERTROUWELIJK	*TBB* 4	Kennisname door niet-gerechtigden kan nadeel toebrengen aan het belang van één of meer ministeries.
Geen-rubricering	*Open*	Kennisname door niet gerechtigden kan geen nadeel toebrengen aan het belang van één of meer ministeries. (Open, van open, Tenzij)

Tabel: Beveiligingsniveau's

Naast gerubriceerde informatie bestaat tevens gemerkte informatie. Een merking heeft als doel de kring van tot kennisname gerechtigden te beperken tot een specifieke groep of kan een specifieke behandeling en beveiliging tot doel hebben. In **bijlage 1** is een tabel met de meest voorkomende merkingen, alsmede hun betekenis, opgenomen. Ongerubriceerde informatie van het Ministerie die wel voorzien is van een merking dient als TBB 1 te worden beveiligd. Als de merking betrekking heeft op een specifieke wijze van behandeling of beveiliging, dan dienen deze aanwijzingen te worden gevolgd.

Indien het gaat om grote hoeveelheden informatie voorzien van een rubricering en/of merking (bijvoorbeeld de medische informatie van personeel) kan door de toezichthoudende instantie worden besloten hieraan als verzameling een (hogere) rubricering toe te kennen en dus hiervoor een hoger niveau van beveiliging te eisen dan voor de individuele gegevens. De schade die bij compromittatie van een grote hoeveelheid informatie ontstaat is immers groter dan bij compromittatie van een enkelvoudig gegeven.

1.5 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 TBB1-niveau beveiligd. Personeel dat toegang moet hebben (Need-to-be), dient te beschikken over een Veiligheidsmachtigingsniveau dat overeenkomt met de hoogst aanwezige Rubricering.

1.6 Buitenlandse rubriceringen

In de tabel in **bijlage 1** zijn de met de nationale rubricering overeenkomstige NAVO- en EU-rubriceringen opgenomen. De vergelijkingstabel met de meest voorkomende buitenlandse nationale beveiligingsniveau's is in **bijlage 1** opgenomen.

In het kader van een buitenlandse 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), kunnen separaat beveiligingseisen worden gesteld. Dergelijke informatie, materieel en/of goederen vallen doorgaans in de categorie Controlled Unclassified Information of Item (CUI). Veelal worden hier door het betrokken bedrijf rechtstreeks afspraken gemaakt met BZ in bijvoorbeeld een Technical Assistance Agreement. De ABBO 2018 kan hierop een handvat bieden voor het beoogde beveiligingsregime.

1.7 Internationale aspecten

1.7.1 Inschakeling buitenlands bedrijf

Ook voor de inschakeling van een buitenlandse opdrachtnemer is toestemming van het ministerie van Buitenlandse Zaken vereist. Wanneer het voornemen bestaat om een buitenlands bedrijf in te schakelen voor een bijzondere opdracht, of als subcontractor van een reeds bestaand ABBO bedrijf, dient een autorisatieverzoek bij BZ te worden ingediend. In het buitenland is het niet mogelijk om bij een bijzondere opdracht het ABBO contractueel te bedingen in verband met nationale wetgeving. BZ neemt contact op met de bevoegde autoriteit op het gebied van Industrieveiligheid in het desbetreffende land. Deze autoriteit verstrekt op verzoek van de toezichthoudende instantie een "Facility Security Clearance" (FSC) van het betreffende bedrijf op basis van de in dat land vigerende stelsel van beveiligingseisen. Op basis van deze FSC verstrekt de toezichthoudende instantie de autorisatie aan de aanvrager.

1.7.2 Bi-laterale beveiligingsafspraken

Voorwaarde voor de wederzijdse internationale inschakeling van bedrijven is wel dat er tussen Nederland en het betreffende buitenland een beveiligingsverdrag, overeenkomst of MoU bestaat, waarin uitwisseling van BI en wederzijds de beveiliging van die uitgewisselde BI is gegarandeerd. De overheid heeft met een groot aantal landen in multi-lateraal verband (MISWG) en met een beperkt aantal landen op bi-laterale basis afspraken om de wederzijdse inschakeling op efficiënte wijze te faciliteren.

1.8 Autorisatie

Het bedrijf is pas geautoriseerd om aan het in vooruitzicht gestelde contract gerelateerde Bijzondere Informatie, materieel of goederen op te slaan en te verwerken, wanneer een goedgekeurde autorisatie is afgegeven door BZ. Deze autorisatie is geen algemeen certificaat, maar wordt, op enkele uitzonderingen na, per contract verleend. Definitieve gunning en ondertekening van het contract kunnen pas plaatsvinden wanneer er een (voorlopige) autorisatie is verleend. Indien niet (meer) voldaan kan worden.

1.9 Octrooien op vindingen die betrekking hebben op gerubriceerde gegevens

Indien uit een gerubriceerde opdracht van het Ministerie een vinding voortvloeit waarop naar mening van de Opdrachtnemer octrooi moet worden aangevraagd, zal hij of zij alvorens daartoe over te gaan, BZ hiervan in kennis stellen. Mogelijk wordt aan de octrooiaanvraag, gezien het karakter, een rubricering toegekend van de Rijksoctrooiwet 1995. Alle aan de octrooiaanvraag gerelateerde informatie, indien gerubriceerd, valt onder de ABBO 2018. Ook het octrooigemachtigde bureau waar de gerubriceerde octrooiaanvraag wordt ingediend dient aan de ABBO 2018 te voldoen.

1.10 Escrow

Om de continuïteit van een bedrijfsproces van BZ ook bij bijvoorbeeld een faillissement van een software leverancier of distributeur te waarborgen wordt tussen Opdrachtgever en Opdrachtnemer een zogenaamde Escrow-overeenkomst afgesloten. Deze overeenkomst houdt in dat de leverancier de broncode van een softwareproduct ten behoeve van de gebruiker deponeert bij een gespecialiseerde door BZ aangewezen Escrow Agent. Dit wordt ook wel Broncode Escrow genoemd. Doorgaans betreft het informatie (variërend van vercijfersleutels tot softwarebroncode) waarvan de Opdrachtnemer het intellectueel eigendom bezit. De broncode wordt aan BZ overgedragen op het moment dat aan bepaalde voorwaarden

wordt voldaan of dat Opdrachtnemer zijn verplichtingen niet kan nakomen.

In die gevallen waar de in bewaring gegeven informatie als een TBB kan worden beschouwd dient ook de Escrow Agent aan de ABBO 2018 te voldoen.

1.11 Advies en controle

In het kader van een bijzondere opdracht wordt de Opdrachtnemer op meerdere momenten bezocht. Het doel van deze bezoeken varieert:

- advies: het bedrijf wordt bezocht in het kader van advies over de maatregelen die getroffen moeten worden om te voldoen aan de beveiligingseisen zoals beschreven in deze ABBO 2018;

- controle: het bedrijf wordt, al dan niet vooraf aangekondigd, bezocht voor een tussentijdse beoordeling van de implementatie van de beveiligingseisen. De resultaten worden aan het bedrijf bekend gesteld teneinde, waar nodig, de beveiligingsmaatregelen te verbeteren;

- audit: het bedrijf wordt, vooraf aangekondigd, bezocht voor een formele, integrale beveiligingsaudit op de implementatie en toereikendheid van de beveiligingseisen. De resultaten worden vastgelegd in een auditrapport dat wordt vastgesteld door BZ of een onafhankelijke derde partij en aangeboden aan de directie van het bedrijf en aan de Beveiligingsautoriteit van het ministerie;

- onderzoek: het bedrijf wordt bezocht na melding van een (mogelijk) beveiligingsincident. Er wordt nader onderzoek verricht naar mogelijke compromittatie van een TBB en de gevolgen daarvan met als doel de schade voor de Staat en zijn bondgenoten te beperken en herhaling te voorkomen.

1.12 Uitgangspunten bij dit voorschrift

De normen in deze ABBO 2018 zijn bedoeld om de kring van personen en bedrijven die in aanraking komen met of toegang hebben tot BI, materieel, goederen of objecten zo beperkt mogelijk te houden. Het ministerie is verantwoordelijk voor de vaststelling van de rubricering, ook van de informatie die in het kader van een in opdracht van het ministrie uitgevoerde opdracht extern wordt geproduceerd, verwerkt of bewerkt. In het contract of standaardvoorwaarden worden hierover afspraken gemaakt. De ABBO 2018 gaat ervan uit dat een risicoanalyse met betrekking tot de BI reeds heeft plaatsgevonden. Deze analyse is afgerond met een indeling in TBB en/of rubricering en een nadere specificatie in een RAL.

Dit voorschrift ABBO 2018 houdt rekening met voorwaarden op basis van nationale en internationale wetgeving, zoals de voorschriften van de NAVO en de EU voor de beveiliging van gerubriceerde informatie, de Wet op de inlichtingen- en veiligheidsdiensten 2002, de Wet veiligheidsonderzoeken en de Archiefwet 1995.

1.13 Sancties

De ABBO 2018 vormt een integraal onderdeel van het contract tussen BZ en de opdrachtnemer. Het niet naleven van de in de ABBO 2018 gestelde beveiligingseisen wordt derhalve als contractbreuk beschouwd. Dit kan leiden tot opschorting of intrekking van de verleende autorisatie tot verwerken en opslaan van TBB-en. Dit op zijn beurt kan beeindiging van het contract tot gevolg hebben. Indien het niet naleven is terug te voeren op een bepaald persoon kan intrekken van diens VGB het gevolg zijn. Bij beëindiging van het contract dient het TBB te worden ingeleverd of vernietigd. Het moedwillig achterhouden, vertrekken aan of ter beschikkingstellen van een TBB aan een niet-gerechtigde, danwel nalatigheid in de omgang met een TBB, is een strafbaar feit conform het gestelde in het Wetboek van strafrecht (artikel 98, 98a, 98b, 98c, 272 en 273).

1.14 Uitvoeringsbepalingen, instructies en aanvullende regelingen

In deze beveiligingseisen zijn uitvoeringsbepalingen, instructies en aanvullende regelingen opgenomen. Deze bepalingen en regelingen kunnen worden gewijzigd of aangevuld indien de nationale of internationale omstandigheden dit vereisen.

Hoofdstuk 2: Beveiligingseisen en maatregelen

BZ vertrouwt als opdrachtgever in het kader van bijzondere opdrachten TBB-en toe aan opdrachtnemers. Dit kan bijvoorbeeld plaatsvinden door

het verstrekken van documenten of materieel, de overdracht van een object, of bij het voeren van gesprekken. Een TBB kan ook digitaal worden uitgewisseld.

Indien een TBB aan bedrijven wordt verstrekt dan wel bij bedrijven wordt gegenereerd, is het noodzakelijk beveiligingsmaatregelen op basis van de ABBO 2018 te treffen. In deze ABBO 2018 is de algemene basisset van beveiligingseisen beschreven met betrekking tot een drietal deelgebieden:

- bestuurlijke en organisatorische beveiliging;
- personele beveiliging;
- fysieke en digitale beveiliging.

Afhankelijk van de aard van de bijzondere opdracht dient het bedrijf te voldoen aan de eisen die in deze ABBO 2018 ten aanzien van één of meerdere deelgebieden zijn gesteld. Het is derhalve mogelijk dat niet alle deelgebieden (volledig) van toepassing zijn. Een door de BZ opgestelde Rubriceringsaanduidingslijst (RAL) geeft aan welk TBB-niveau van toepassing is op de specifieke onderwerpen van de bijzondere opdracht. de toezichthoudende instantie stelt vervolgens vast welke deelgebieden van toepassing zijn en per deelgebied het juiste beveiligingseisenpakket.

In de hoofdstukken drie tot en met vijf zijn de deelgebieden nader uitgewerkt en de beveiligingseisen voor het desbetreffende deelgebied beschreven.

Deze *ABBO* 2018 bevat de eisen voor de beveiliging van *TBB* waaraan minimaal moet zijn voldaan. Per opdracht of project kunnen additionele eisen worden gesteld, die in de overeenkomst nader zijn vastgelegd.

De eisen hebben betrekking op vier deelgebieden: bestuur en organisatie, personeel, fysiek en digitaal. In de volgende hoofdstukken zijn de eisen per deelgebied in een tabel verwoord.

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 *BZ* te worden bepaald of, respectievelijk in welke mate, aan de eis moet worden voldaan. Een half open en gesloten bolletje (◐) houdt in dat de voorkeur gaat naar de gestelde eis maar dat er in een specifieke situatie mogelijk een uitzondering gemaakt kan worden, dit allen in overleg met BZ.

Hoofdstuk 3: Bestuurlijke en organisatorische beveiliging

3.1 Inleiding

Een organisatiebreed, structureel gehandhaafd en breed gedragen beveiligingsbeleid is noodzakelijk om TBB-en afdoende te beschermen. Het implementeren van adequate beveiligingsmaatregelen waaraan men zich ook daadwerkelijk dient te conformeren, zijn bepalende factoren voor het succes van elk beveiligingsbeleid. 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 de *TBB*, kan een bedrijfscultuur ontstaan waarin de *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 *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.

ABBO 2018 eisen								
HOOFDSTUK 3: BESTUUR EN ORGANISATIE			**BEVEILIGINGSREGIME**					
3.1	**Inrichten van de beveiligingsorganisatie**	***Specificatie***	***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***
1	*Opdrachtnemer* beschikt over een organisatiebreed, structureel gehandhaafd en breed gedragen beveiligingsbeleid, bekrachtigd door het hoogste bestuursorgaan.	Beveiligingsplan	●	●	●	●	●	ISO
2	*BZ* heeft toegang tot het beveiligingsplan, opgesteld door de *beveiligingsfunctionaris* (*BF*) van de *opdrachtnemer*, waarin de beveiligingseisen uit de *ABBO 2018* zijn uitgewerkt in duidelijke, hanteerbare maatregelen en procedures.	Beveiligingsplan	●	●	●	●	●	ISO
3	*Opdrachtnemer* heeft de in het beveiligingsplan beschreven maatregelen en procedures eenduidig geïmplementeerd in de organisatie.	Beveiligingsplan	●	●	●	●	●	ISO
4	*Opdrachtnemer* heeft, met voorafgaande schriftelijke instemming van *BZ*, een *BF* benoemd. BZ heeft 3 maanden om toestemming te vergeven.	Beveiligingsfunctionaris	●	●	●	●	●	ISO
5	De *BF* beschikt bij voorkeur over: de Nederlandse nationaliteit en is in dienst van het desbetreffende bedrijf. Indien een Nederlandse nationaliteit niet mogelijk is er een uitzondering mogelijk, mits er een veiligheidsonderzoek kan worden uitgevoerd door een buitenlandse inlichtingendienst waarmee Nederland een overeenkomst heeft. De *BF* beschikt ten minste over: voldoende autonomie, bevoegdheden, slagkracht en senioriteit; een *Verklaring Omtrent Gedrag* (*VOG*) of een *Verklaring van Geen Bezwaar (VGB)* op het hoogst geldende rubriceringsniveau van de *Bijzondere opdracht (BO)*; rechtstreekse en onafhankelijke toegang tot alle bestuursorganen.	Beveiligingsfunctionaris	●	●	●	●	●	
3.2	**De *Beveiligingsfunctionaris***		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***

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. BZ heeft toegang tot deze resultaten en rapporten.	Beveiligingsfunctionaris	●	●	●	●	●	
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 BZ, gerapporteerd. Zonodig wordt het beveiligingsplan geactualiseerd.	Beveiligingsaudits	●	●	●	●	●	
3	Beleidswijzigingen die impact hebben op het security beleid van het bedrijf zijn aan *BZ* ter beoordeling verstrekt en zijn verwerkt in het beveiligingsplan.	Beveiligingsplan	●	●	●	▯	▯	
4	Noodzakelijke wijzigingen n.a.v. een verhoogd dreigingsbeeld of een incident, zijn geïmplementeerd in het beveiligingsplan binnen de door *BZ* gestelde termijn.	Beveiligingsplan	**direct**	**1 maand**	**1 maand**	▯	▯	
5	De BF draagt zorg voor volledige medewerking bij controles, audits en onderzoeken bij *Opdrachtnemer* door *BZ*.	Procedure ABBO	●	●	●	●	●	
6	De BF stelt zich door middel van het onderhouden van contacten met de gemeente, omliggende bedrijven en de wijkagent op de hoogte van zaken die de lokale veiligheid aangaan.	Beveiligingsplan	●	●	●	●	▯	
3.3	***Zeggenschap* en bedrijfsstructuur**		***TBB* 1/ZG**	***TBB* 2/G**	***TBB* 3/C**	***TBB* 4/DV**	***Open***	***Norm***
1	*Opdrachtnemer* heeft ten behoeve van de autorisatie een Verklaring van Eigendom, *Zeggenschap* en bedrijfsstructuur opgesteld en ter beschikking gesteld aan *BZ*.	Wijzigingen in zeggenschap, structuur, aandeelhouderschap	●	●	●	●	●	Arbit (artikel 7 en 8)
2	*Opdrachtnemer* meldt voorgenomen wijzigingen in eigendom/aandeelhouderschap waarbij meer dan 10 % van (de aandelen van) het bedrijf in bezit komt van één natuurlijke of rechtspersoon, of van één of meerdere buitenlandse natuurlijke of rechtspersonen, terstond	Wijzigingen in zeggenschap, structuur, aandeelhouderschap	●	●	●	●	▯	

	schriftelijk aan de Directeur *BZ/ DBV-IV*. Dit geldt eveneens voor elke verdere toename.							
3	*Opdrachtnemer* meldt voorgenomen wijzigingen in *Zeggenschap* (anders dan bedoeld onder 1.3.2) waarbij deze grotendeels in handen komt van één natuurlijke of rechtspersoon, of van één of meerdere buitenlandse natuurlijke of rechtspersonen, terstond schriftelijk aan de Directeur *BZ/ DBV-IV*.	Wijzigingen in zeggenschap, structuur, aandeelhouderschap	●	●	●	●	☐	
4	*Opdrachtnemer* meldt voorgenomen benoemingen van bestuurders die niet beschikken over de Nederlandse nationaliteit, terstond schriftelijk aan de Directeur *BZ/ DBV-IV*.	Wijzigingen in zeggenschap, structuur, aandeelhouderschap	●	●	●	◐	◐	Arbit (artikel 22)
5	*Opdrachtnemer* meldt voorgenomen samenwerking met buitenlandse bedrijven of overheden, terstond schriftelijk aan de Directeur *BZ/ DBV-IV*.	Wijzigingen in zeggenschap, structuur, aandeelhouderschap	●	●	●	●	☐	
6	*Opdrachtnemer* meldt dreigende bedrijfsbeëindiging, surseance van betaling of faillissement terstond schriftelijk aan de Directeur *BZ/ DBV-IV*.	Fusies, bedrijfsbeëindiging, surseance van betaling of faillissement	●	●	●	●	☐	Arbit (artikel 30)
7	*Opdrachtnemer* meldt voorgenomen wijziging van bedrijfsactiviteiten, locaties, sourcing, splitsing, fusies of gedeeltelijke dan wel volledige overname terstond schriftelijk aan de Directeur *BZ/ DBV-IV*.	Wijziging van bedrijfsactiviteiten, sourcing en overname	●	●	●	●	●	
8	*Opdrachtnemer* verschaft duidelijkheid bij welk (onderdeel van het) bedrijf en op welke locatie de *Bijzondere Opdracht* wordt belegd en streeft maximaal naar onderbrenging van alle *Bijzondere Opdracht* bij één duidelijk herkenbaar en juridisch en organisatorisch af te schermen (onderdeel van het) bedrijf.	overzicht	●	●	●	●		

9	*Opdrachtnemer* is een Nederlands Rechtspersoon in geval van een *Bijzondere Opdracht* waarbij een grote hoeveelheid (te bepalen door *BZ*) *Bijzondere Informatie (BI)* is overgedragen.	Nederlands Rechtspersoon	●	●	●	○		
10	*Opdrachtnemer* garandeert dat een grotere hoeveelheid *Bijzondere Informatie* (te bepalen door *BZ*) slechts op Nederlands grondgebied wordt gegenereerd, bewerkt en opgeslagen.	locatie	●	●	●	●		
11	*Opdrachtnemer* plaatst slechts medewerkers met de Nederlandse nationaliteit op *Vertrouwensfuncties* waarbij toegang tot een grotere hoeveelheid *Bijzondere Informatie* (te bepalen door *BZ*) is vereist	*Vertrouwensfuncties*	●	●	●	◐		
12	*Opdrachtnemer* legt waar mogelijk vast in statuten dat bij mogelijke vervreemding van zijn bedrijf of onderdelen of locaties de *Rijksoverheid* het eerste recht van koop heeft.	statuten	○	○	○			
3.4	**Beveiligingsbewustzijn**		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***
1	*Opdrachtnemer* voert een programma uit ter bevordering van het beveiligingsbewustzijn waarbij deelname verplicht en meetbaar is.	Beveiligingsbewustzijn	●	●	●	●	●	Arbit (artikel 19) + Iso
2	De *BF* geeft voorlichting aan vertrouwensfunctionarissen aangaande *ABBO* 2018 procedures en de bijbehorende verantwoordelijkheden, bij aanstelling op een *Vertrouwensfunctie*, bij de start van een nieuwe *Bijzondere Opdracht* en vervolgens periodiek, doch tenminste eenmaal per jaar.	Voorlichting	●	●	●	●	●	Iso
3	De *BF* geeft individueel instructie en begeleiding aan medewerkers, die werken aan *Bijzondere Opdrachten*, in dien sprake van: buitenlandse contacten hebben of op reis gaan naar risicolanden. (Zie Bijlage 2 voor lijst met risicolanden)	Voorlichting	●	●	●	●	●	Iso
3.5	***Rubriceren en lijsten***		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***

1	Een door BZ ingevulde RAL, waarin de onderdelen benoemd zijn die op een bepaald niveau beveiligd dient te worden, is per bijzondere opdracht aanwezig.	RAL	●	●	●	●		Iso
2	Bij meerjarig bijzondere opdrachten en/of wanneer meerdere partijen betrokken zijn, dient er een Project Security Instruction (PSI) te worden opgemaakt. Dit gebeurt in overleg met de toezichthoudende instantie.	PSI	●	●	●	●		
3	Bij internationaal een bijzondere opdrachten dient er een Security Aspect Letter (SAL) te worden opgemaakt. Dit gebeurt in overleg met de toezichthoudende instantie.	SAL	●	●	●	●		
3.6	**Logistieke keten**		***TBB* 1/ZG**	***TBB* 2/G**	***TBB* 3/C**	***TBB* 4/DV**	***Open***	***Norm***
1	*Opdrachtnemer* meldt voorgenomen uitbesteding van werkzaamheden in het kader van een *Bijzondere Opdracht* aan *Subcontractors* vooraf aan *BZ* voor toestemming.	Subcontracting	●	●	●	●		Arbit (artikel 23)
2	Na toestemming van *BZ* tot uitbesteding heeft *Opdrachtnemer* in het contract met *Subcontractors* die in aanraking komen met een *TBB*, de *ABBO* 2018 bedongen. Een ingevulde *Rubriceringsaanduidingslijst* is hierbij verstrekt aan *BZ.*	Subcontracting	●	●	●	●		
3	Op (toe)leveranties van systeemonderdelen die op grond van hun kritische / vitale functie een zekere mate van bescherming verdienen, heeft *Opdrachtnemer* in overleg met *BZ* de *ABBO* 2018 bedongen.	Subcontracting	□	□	□	□		
4	Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan een *Bijzondere Opdracht* zijn de werkzaamheden aan een *TBB* zoveel mogelijk gecentraliseerd. (***Opdrachtnemer* draagt de verantwoordelijkheid voor de bedrijven die hij als *Subcontractor* onder zijn hoede neemt**).	Subcontracting	●	●	●	●	●	

5	*Opdrachtnemer* meldt het voornemen een buitenlandse Subcontractor in te schakelen voor een *Bijzondere Opdracht* vooraf aan *BZ* voor toestemming. Voor inschakeling van een buitenlands bedrijf is toestemming en autorisatie van *BZ* vereist.	Subcontracting	●	●	●	●		
3.7	**Pers, internet, sociale media, publicatie, fotografische opnamen, etc.**		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB4/DV***	***Open***	***Norm***
1	*Opdrachtnemer* en zijn medewerkers maken zonder uitdrukkelijke voorafgaande toestemming van *BZ* op geen enkele wijze publiekelijk bekend welke *Bijzondere Opdracht* zij voor de Nederlandse overheid, buitenlandse overheid en/of *NAVO* / *EU* uitvoeren.	Publieke uitlatingen	●	●	●	◐		Arbit (artikel 21)
2	Het maken van opnamen van een *TBB*, anders dan noodzakelijk voor de uitvoering van de *Bijzondere Opdracht*, is ongeacht het middel, niet toegestaan zonder voorafgaande schriftelijke goedkeuring van *BZ*.	Afspraken	●	●	●	◐		Arbit (artikel 21)
3	*Opdrachtnemer* en zijn medewerkers maken contactgegevens en afspraken met de *BZ* op geen enkele wijze publiekelijk bekend.	Publieke uitlatingen	●	●	●	◐		Arbit (artikel 17)
3.8	**beveiligingsincidenten**		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***
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*.	Beveiligingsincidenten	●	●	●	●	◐	
2	veiligheidsincidenten dienen binnen de normstelling genoemd in tabel “Classificatie” met behulp van de *IRP* aan *BZ* te zijn bekend gesteld.	Beveiligingsincidenten	●	●	●	●		
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 incidenten mogelijk te maken.	Beveiligingsincidenten	**6 maanden**	**6 maanden**	**3 maanden**	**3 Maanden**	**3 Maanden**	

4	*Informatie* aangaande vastgestelde incidenten wordt gedurende de aangegeven periode door de *BF* bewaard.	Beveiligingsincidenten	3 jaar	3 jaar	3 jaar	2 jaar	2 jaar	
5	Werknemers dienen zwakke plekken in de beveiliging binnen de aangegeven termijn aan de *BF* te rapporteren.	rapportage	direct	werkdag	week	week	week	
6	Er is een evaluatiemechanisme gedefinieerd bij de opdrachtnemer waarmee men specifieke lessen (lessons learned) identificeert en deze verwerkt in het beveiligingsbeleid.	Lessons learned	●	●	●	●	●	
7	Er zijn disciplinaire maatregelen mogelijk tegen veroorzakers van veiligheidsincidenten.	Sancties	●	●	●	●	●	Iso
8	Informatie m.b.t. tot beveiligingsincidenten alleen beschikbaar directe medewerkers opdrachtnemer en BZ. De informatie wordt niet breed in de organisatie van de opdrachtnemer verspreid.	Publieke en interne uitlatingen	●	●	●	●	●	

3.9	Buitenlandse Bedrijven	Specificatie	*TBB* 1/ZG	*TBB* 2/G	*TBB* 3/C	*TBB* 4/DV	*Open*	*Norm*
1	Het Bedrijf moet bereid zijn om zich te registreren bij de KvK zodat het bedrijf onder Nederlandse wetgeving valt (Nederlandse BV).	Buitelandse bedrijven	●	●	●	●	●	
2	Indien mogelijk alleen medewerkers met een Nederlandse nationaliteit op vertrouwensfuncties plaatsen.	Buitelandse bedrijven	●	●	●	●	●	
3	Als het bedrijf zich niet in Nederland bevindt (en om te voorkomen dat eerdere MoU's in gevaar komen) worden voor audits en andere controles een derde onafhankelijke partij gebruikt .	Buitelandse bedrijven	●	●	●	●	●	
4	De BF moet op de hoogte zijn welke medewerkers zich in het buitenland bevinden voor hun werk of privé, er is geen toestemming nodig van de BF voor buitenlandse reizen.	Buitelandse bedrijven	●	●	●	●	●	

5	De BF moet op de hoogte zijn welk apparatuur/werkstations zich in het buitenland bevinden en gebruikt worden.	Buitelandse bedrijven	●	●	●	●	●	

Hoofdstuk 4: Personele beveiliging

4.1 Inleiding

Personele veiligheid is, in de context van BZ, een complex van maatregelen dat de bedrijfsvoering van BZ zo goed als mogelijk beschermt tegen negatieve personeelsinvloeden door betrouwbaarheidseisen te stellen aan het burgerpersoneel van de BZ, alsmede het personeel in dienst van bedrijven in opdracht van BZ opdrachten uitvoeren.

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

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

Daarnaast is het zaak aandacht te besteden aan het veiligheidsbewustzijn bij medewerkers, zodat deze zich bij voortduring bewust zijn van de risico's en zich nut en noodzaak realiseren van gedegen veiligheidsmaatregelen. Dit speelt ook een belangrijke rol bij reizen naar het buitenland.

ABBO 2018 eisen								
HOOFDSTUK 4: PERSONELE BEVEILIGING			**BEVEILIGINGSREGIME**					
4.1	**Het *Veiligheidsonderzoek* en de *VGB***	**Specificatie**	***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***
1	Er is een formele *Lijst van Vertrouwensfuncties* (*LvV)* vastgesteld en gedeeld met *BZ*.	Vaststelling LvV	●	●	●	□		
2	*Veiligheidsonderzoeken* worden aangevraagd op basis van een formeel vastgestelde *LvV*.	Aanvraag veiligheidsonderzoek	●	●	●	□		
3	Een geldige *VGB* voor het vervullen van een *Vertrouwensfunctie* op A-niveau is aanwezig voor alle betrokken medewerkers. In overleg met BZ is bij uitzondering een vergelijkbaar VGB niveau van een geaccepteerde buitenlandse dienst ook toegestaan.	VGB op A-niveau	●					Arbit (artikel 19) + ISO
4	Een geldige *VGB* voor het vervullen van een *Vertrouwensfunctie* op B-niveau is aanwezig voor alle betrokken medewerkers. In overleg met BZ is bij uitzondering een vergelijkbaar VGB niveau van een geaccepteerde buitenlandse dienst ook toegestaan.	VGB op B-niveau		●	□			Arbit (artikel 19) + ISO
5	Een geldige *VGB* voor het vervullen van een *Vertrouwensfunctie* op C-niveau is aanwezig voor alle betrokken medewerkers. In overleg met BZ is bij uitzondering een vergelijkbaar VGB niveau van een geaccepteerde buitenlandse dienst ook toegestaan.	VGB op C-niveau			●			Arbit (artikel 19) + ISO
6	Een geldige *VOG* voor vervullen van een functie op *DV*-niveau is aanwezig voor alle betrokken medewerkers. In overleg met BZ is bij uitzondering een vergelijkbaar VOG niveau van een geaccepteerde buitenlandse dienst ook toegestaan.	VOG op DV-niveau				●	●	Arbit (artikel 19) + ISO
7	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een *VGB* op A-niveau. In overleg met BZ is bij uitzondering een vergelijkbaar VGB niveau van een geaccepteerde buitenlandse dienst ook toegestaan.	VGB op A-niveau	●					Arbit (artikel 19) + ISO

8	Beheerders, in het bijzonder beheerders van de digitale omgeving, zijn in het bezit van een *VGB* op minimaal B-niveau. In overleg met BZ is bij uitzondering een vergelijkbaar VGB niveau van een geaccepteerde buitenlandse dienst ook toegestaan.	VGB op B-niveau		●	●	●		Arbit (artikel 19) + ISO
9	De *BF* van de *Opdrachtnemer* vraagt tenminste drie maanden voor het verstrijken van de geldigheidsduur van de jongste *VGB* een hernieuwd Veiligheidsonderzoek aan.	Hernieuwd veiligheidsonderzoek	●	●	●	□		Arbit (artikel 19) + ISO
10	Bij tussentijdse aanleiding, bijvoorbeeld bij wijziging persoonlijke omstandigheden, vraagt de *BF* een hernieuwd *Veiligheidsonderzoek* aan.	Wijziging persoonlijke omstandigheden	●	●	●	●		
11	*Opdrachtnemer* plaatst slechts medewerkers met de Nederlandse nationaliteit op *Vertrouwensfuncties* waarbij toegang tot een grotere hoeveelheid *Bijzondere Informatie* (te bepalen door *BZ*) is vereist.	niet-Nederlander op een vertrouwensfunctie	●	●	●	◐		
12	Plaatsing op een *Vertrouwensfunctie* van een medewerker die niet beschikt over de Nederlandse nationaliteit, is voorafgaande aan de aanvraag van het *Veiligheidsonderzoek* goedgekeurd door *BZ*.	Goedkeuring BZ	●	●	●	◐		
13	Een overzicht van alle *VGB*'n, *VOG'n* en verklaringen van bekendheid met de geheimhoudingsplicht is bij de *BF* aanwezig.	Overzicht BF	●	●	●	●	●	
4.2	***Geheimhoudingsverklaring***		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***
1	De *BF* heeft de *medewerker* gewezen op de verplichtingen die voortvloeien uit het bekleden van een *functie*.	Verplichtingen geheimhoudings verklaring	●	●	●	●	●	
2	Een door een f*unctionaris* getekende 'Verklaring van bekendheid met de geheimhoudingsplicht voor medewerkers' is aanwezig en dit onderwerp wordt 1x per jaar meegenomen in een awareness sessie.	Getekende geheimhoudings verklaring	●	●	●	●	●	Arbit (artikel 17)

3	Een door een *Vertrouwensfunctionaris*, die kennis moet nemen van crypto, crypto-security of CCI-gemerkte informatie of materiaal, getekende 'Verklaring van bekendheid met de geheimhoudingsplicht voor *Vertrouwensfunctionarissen* in het kader van een *CRYPTO functie*' is aanwezig en dit onderwerp wordt 1x per jaar meegenomen in een awareness sessie.	Getekende geheimhoudings verklaring	●	●	●	●		
4	De BF organiseert 1x per jaar awareness sessie voor alle medewerkers m.b.t. informatiebeveiliging.	Bewustwording	●	●	●	●		
4.3	**Ontheffing uit een *Vertrouwensfunctie***		***TBB* 1/ZG**	***TBB* 2/G**	***TBB* 3/C**	***TBB* 4/*DV***	***Open***	***Norm***
1	De *BF* meldt ontheffing uit een *Vertrouwensfunctie* aan *BZ* bij: - functiewijziging van een *Vertrouwensfunctionaris* (*VF*); - ontslag van een *VF*; - overtreding van beveiligingsregels door een *VF*.	Functiewijziging, ontslag en overtreding	●	●	●	□		
2	Een door de medewerker getekende ontheffingsverklaring bij ontheffing uit een *Vertrouwensfunctie* respectievelijk *Cryptofunctie* is aanwezig.	Ontheffingsverklaring	●	●	●	□		
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.	Toelichting op ontheffingsverklaring	●	●	●	□		
4	Indien de *Vertrouwensfunctionaris* de beveiligingsregels van de *Opdrachtnemer* bewust of onbewust negeert of overtreedt, dient de *BF* passende maatregelen te nemen en *BZ* hierover te informeren.	Overtredingen	●	●	●	□		

	Grove nalatigheid of bewuste *Compromittatie* van *Staatsgeheime* of *Vitale Informatie* of *Materieel* kan aanleiding zijn tot strafrechtelijke vervolging.							
4.4	**Reizen naar het buitenland**		***TBB 1/ZG***	***TBB 2/G***	***TBB 3/C***	***TBB 4/DV***	***Open***	***Norm***
1	Een *Vertrouwensfunctionaris* heeft een voorgenomen zakelijke reis naar het buitenland onverwijld gemeld aan de *BF*.	Melden aan de BF	●	●	●	☐		
2	De leverancier heeft een zakelijk en privé reis beleid/procedure ingericht m.b.t. risicolanden. Zie Bijlage 2 voor lijst met risicolanden)	Reizen naar risicolanden	●	●	●	☐		
3	De BF brieft (instructie) en debrieft vertrouwensfunctionarissen/medewerkers over buitenlandse reizen.	Instructie reizen	●	●	●	☐		

Hoofdstuk 5: Fysieke en digitale beveiliging

1. Inleiding

In het verleden lag de focus voornamelijk op het detecteren en voorkomen van compromittatie van BI, en derhalve op het toepassen van preventieve en detectieve maatregelen. De ontwikkelingen op het gebied van dreiging en technologie, vooral IT, stellen echter steeds hogere eisen aan de beveiliging waarbij de aandacht niet langer beperkt blijft tot BI maar zich uitstrekt over alle categorieën TBB-en. Door het achterblijven van adequate IT-beveiliging bij eerder genoemde ontwikkelingen is een situatie ontstaan waarbij zwakheden in de IT-beveiliging op grotere schaal kunnen worden misbruikt door kwaadwillenden.

Door statelijke actoren worden dergelijke acties vaak jaren lang voorbereid. Hierdoor wordt slechts het toepassen van een verzameling preventieve en detectieve beveiligingsmaatregelen niet langer afdoende geacht om de exclusiviteit van een TBB te garanderen. De huidige ABBO 2018 beschrijft derhalve naast de preventieve beveiligingsmaatregelen ook responsieve maatregelen zowel in het fysieke als in het digitale deelgebied.

Als er op eigen locatie van het bedrijf sprake is van opslag, verwerking of het transport van TBB-en of dat een bepaalde fysieke ruimte gebruikt wordt ten behoeve van vitale dienstverlening zal het TBB fysiek en/of digitaal beveiligd moeten worden. In dit hoofdstuk wordt beschreven op welke manier tot een afgewogen set van beveiligingsmaatregelen gekomen wordt en welke minimale eisen daarbij gelden. Het doel is de schade tot een aanvaardbaar minimum te beperken of in zijn geheel te voorkomen.

Wanneer een bedrijf een bijzondere opdracht gaat uitvoeren en hierbij op eigen locatie gaat werken dan is er sprake van opslag, verwerking en transport van een TBB. Er zal op locatie een compartiment moeten worden ingericht waarbij de ABBO 2018- normen van toepassing zijn. Naast de algemeen fysieke eisen die aan het compartiment en de locatie worden gesteld, zijn er ook specifieke eisen voor de fysieke TBB en de digitale TBB.

Fysieke beveiligingsmaatregelen worden onderscheiden in maatregelen van Organisatorische (O), Bouwkundige (B), Elektronische (E) en Reactieve (R) aard. Met een afgewogen selectie uit deze OBER-maatregelen wordt bewerkstelligd dat, binnen de met deze maatregelen bereikte uitsteltijd, interventie plaats vindt om compromittatie van het TBB te voorkomen. Uitsteltijd wordt gerealiseerd met bouwkundige maatregelen zoals stevige wanden, vloeren en plafonds en geschikte deuren, ramen en dergelijke. Interventie vindt plaats door de gebruiker, een beveiligingsbedrijf, de politie of BZ personeel. Interventie kan pas plaatsvinden na detectie en verificatie van ongewenste toegang.

ABBO 2018 eisen								
Hoofdstuk 5: Fysiek			**BEVEILIGINGSREGIME**					
5.1	**Organisatorische maatregelen**	***Specificatie***	***TBB 1 / ZG***	***TBB 2 / G***	***TBB 3 / C***	***TBB 4 / DV***	***Open***	***Norm***
1	De fysieke beveiligingsmaatregelen zijn volgens een schillenstructuur opgebouwd met toepassing van het "*Need-to-Be*" principe. Met controleerbare geautoriseerde overgang tussen de schillen.	Toegangscontrole	●	●	●	●	●	
2	Bij het samenstellen van de (fysieke) maatregelen worden de "*Need-to-Be*" en "*Need-to-Know*" principes toegepast. Regulering van de autorisaties vindt plaats door de BF. Personen binnen de schillen dienen altijd bekend en herkenbaar te zijn (Zichtbaar dragen Pas).	Toegangscontrole	●	●	●	●	●	
3	*TBB*'n worden opgeborgen in een af te sluiten opbergmiddel. Conform het VIRbi	Toegangscontrole	●	●	●	●		
4	Toegang tot het *TBB* of compartiment is alleen door middel van tweefactor *Authenticatie* verleend.	Toegangscontrole	●	●	●			
5	Periodiek, doch minimaal 1x per jaar, wordt het betrokken personeel en bewakingspersoneel getraind in het uitvoeren van beveiligingsmaatregelen.	Toegangscontrole	●	●	●	●		
6	Toegang van personen zonder *Autorisatie* (zoals bezoekers) is vooraf gemeld en afgestemd met de *BF*.	Toegangscontrole	●	●	●	○		Arbit (artikel 19)
7	In alle ruimten met een *TBB* wordt personeel zonder *Autorisatie*(zoals bezoekers) begeleid door personeel met een *Autorisatie*. Van personen zonder *Autorisatie* is vooraf de identiteit vastgesteld en geregistreerd. Op de pas staat voor een ieder goed zichtbaar "bezoeker" vermeld. Tevens dient het bekend te zijn dat er bezoekers aanwezig zijn binnen de schillen. De registratie hiervan wordt minimaal een jaar bewaard en op aanvraag aan *BZ* verstrekt.	Toegangscontrole	●	●	●	●		
8	Toegang tot een ruimte met een *TBB* door bezoekers zonder *Autorisatie* die niet beschikken over de Nederlandse nationaliteit is minimaal vijf werkdagen voor het bezoek gemeld via de *BF* aan	Toegangscontrole	●	●	●	●		

	BZ. Zonder toestemming van *BZ* kan het bezoek niet plaatsvinden.							
9	In een ruimte met een *TBB* zijn geen camera's, smartphones, microfoons of andere opnameapparatuur aanwezig.	Toegangscontrole	●	●	●			
10	Aan de buitenzijde van het compartiment met een *TBB* zijn algemene beveiligingsinstructies bekend gesteld. In het beveiligingsplan is een overzicht van deze instructies opgenomen.	Toegangscontrole	●	●	●			
11	De uitgifte van sleutels voor toegang tot ruimten en opbergmiddelen met een *TBB* is geregistreerd. Bij de uitgifte door de BF van sleutels is gecontroleerd of men over een *Autorisatie* beschikt. Sleutels zijn voor zo min mogelijk personen toegankelijk. De registratie hiervan wordt minimaal een jaar bewaard.	Toegangscontrole	●	●	●	●		
12	Er zijn uitsluitend gecertificeerde sleutels gebruikt.	Toegangscontrole	●	●	●			
13	De *BF* beheert certificaten, cijfercombinaties en reservesleutels van opbergmiddelen. Deze zijn gescheiden opgeborgen in een ander opbergmiddel met tweefactor *Authenticatie*. Daarbij wordt het beveiligingsniveau gehanteerd van het *TBB*.	Toegangscontrole	●	●	●	●		
14	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 of weggaat; - indien wordt vermoed of vaststaat dat *Compromittatie* heeft plaatsgevonden; uiterlijk zes maanden na de laatste wijziging van de combinatie.	Toegangscontrole	●	●	●			

15	Alvorens een *TBB* buiten het reguliere, in het beveiligingsplan beschreven, proces te plaatsen, is hier toestemming voor verkregen van *BZ*. De beveiliging van het *TBB* wordt hierbij op minimaal hetzelfde niveau gehouden.	Toegangscontrole	●	●	●	●		
16	Het "clear desk principe" en “clear screen principe” is toegepast in alle ruimten waar zich een *TBB* bevindt of kan bevinden. Een *TBB* dient niet onbeheerd achter gelaten te worden.	Clear Desk	●	●	●	●	●	Iso
17	Beheer- en instandhoudingsmaatregelen zijn getroffen om beveiligingsmaatregelen blijvend goed te laten functioneren.	Beveiligingsplan	●	●	●	●		
18	Het verlies van een authenticatiemiddel, zoals (elektronische) sleutel, dient behandeld te worden als een beveiligingsincident.	Beveiligingsplan	●	●	●	○		
19	Meerdere *TBB’n* worden zoveel mogelijk samengebracht en gecompartimenteerd.	Compartimentering	●	●	●	●		
20	Het aantal compartimenten wordt tot een minimum beperkt. Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan een opdracht worden de compartimenten zoveel mogelijk gecentraliseerd.	Compartimentering	●	●	●	●		Iso
21	Het compartiment bevindt zich in een zone die met toegangscontrole is afgeschermd van de openbare ruimte of van ruimten die niet onder controle staan.	Compartimentering	●	●	●			
22	Beveiligingspersoneel heeft de beschikking over anti-overvalmaatregelen, waaronder een alarmknop.	Incidenten	●	●	●	○		
23	Bij het verlaten van een ruimte met een *TBB* is een sluitronde gemaakt, waarbij de deur van het opbergmiddel, de ruimte en zo mogelijk het gebouw is afgesloten. Ramen en deuren zijn afgesloten en het *Indringer Detectie- en Signaleringssysteem*	controle	●	●	●	○		

	(IDSS) is geactiveerd. Tevens is een controle op insluiping en de verzegeling van nooddeuren uitgevoerd.							
24	Beveiligingspersoneel oefent bij afwezigheid van *Geautoriseerd* personeel permanente controle uit ten aanzien van het compartiment.	Oefeningen	●	●				
25	Beveiligingspersoneel loopt controlerondes bij afwezigheid van toezicht van *Geautoriseerd* personeel op het *TBB*.	Oefeningen			●	○		
5.2	**Bouwkundige maatregelen**		***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	***Norm***
1	Ruimten met een *TBB* zijn afsluitbaar.	Sluit- en sleutelplan	●	●	●	●		
2	In het beveiligingsplan is een sluit- en sleutelplan opgenomen. Ramen, deuren en opbergmiddelen zijn afgesloten bij afwezigheid van *Geautoriseerd* personeel. Sleutels en plan worden op hetzelfde niveau beveiligd als het *TBB* waar de sleutel toegang toe geeft.	Sluit- en sleutelplan	●	●	●	●		
3	Een ruimte waarin een *TBB* 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.	Sluit- en sleutelplan	●	●	●	●		
4	Nooddeuren die toegang geven tot het compartiment zijn alleen van binnenuit te openen en te verzegelen.	Sluit- en sleutelplan	●	●	●	●		
5	Het gebouw waarin zich een *TBB* bevindt, is tegen opklimmen beveiligd. Opklimmogelijkheden zijn verwijderd (ook losse, zoals (afval) containers en ladders). Hemelwaterafvoeren, lage muren e.d. zijn van opklimbeveiliging conform NEN1887 voorzien.	Braakwering	●	●	●	●		
6	Gevelopeningen groter dan 15 cm, Kelderramen en dergelijke zijn afgeschermd met traliewerk of strekmetaal, Lichtkoepels, indien niet slagvast, zijn voorzien van traliewerk of strekmetaal	Braakwering	●	●	●	○		

	moeten zijn beveiligd conform de NEN-norm die geldt voor het compartiment.							
7	De ruimte met een *TBB* of een opbergmiddel met een *TBB*, zijn in alle vlakken van inbraakwerende maatregelen voorzien.	Braakwering	●	●	●	○		
8	Wanneer de ruimte 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 braakwerendheid van de buitengevel de eisen van het niveau *TBB* 4.	Braakwering	●	●	●	●		
9	Ramen en gevelopeningen die open kunnen, zijn voorzien van braak- werend gaas.	Braakwering	●	●	●	○		
10	Opbergmiddelen zijn chemisch verankerd en Opbergmiddelen voldoen aan normering conform NEN-EN-1143-1. Deze opbergmiddelen moeten voldoen aan de ECB-S certificering en gekeurd zijn door een onder het ECB-S vallende certificeringinstelling. De sloten van deze opbergmiddelen voldoen aan EN-1300 en dat braak achteraf kan worden vastgesteld.	Braakwering	●	●	●	○		
11	Bevestigingspunten die van buitenaf bereikbaar zijn, zijn voorzien van beveiligde schroeven, bouten of moeren.	Braakwering	●	●	●	●		
12	Opbergmiddelen zijn voorzien van tweefactor *Authenticatie*.	Opbergmiddelen	●	●	●			
13	Rondom het gebouw of terrein met een *TBB* staat een terreinafscheiding met toegangscontrole en een inspecteerbare goed verlichte zone van 2 meter. Het zich ongeautoriseerd toegang verschaffen via de terreinafscheiding wordt gedetecteerd.	Terrein	●	●	●			
14	Indien aan de eisen genoemd in 3.2.17 t/m 3.2.19 niet kan worden voldaan, is opslag en verwerking van *TBB* niet toegestaan.	Terrein	●	●	○	○		

15	Bij de aanleg van cultuurtechnische infrastructuur is rekening gehouden met inbraakpreventie door middel van het creëren van een overzichtelijk geheel, dat wil zeggen de begroeiing laag te laten, zodat de indringer niet ongezien te werk kan gaan en door de toegankelijkheid te beperken door bijvoorbeeld doornachtige beplanting aan te brengen of waterpartijen aan te leggen.	Terrein	●	●	●			
16	De ramen en glazen wanden in een ruimte met een *TBB* zijn voorzien van inkijk beperkende maatregelen. De constructie / cq ramen mogen niet meetrillen met geluid.	Inkijkbeperking	●	●	●			
17	Er zijn voorzieningen getroffen om elektronische apparatuur die niet strikt noodzakelijk zijn voor het uitvoeren van bijzondere werkzaamheden buiten de compartimenten te houden.	Compartimentering	●	●	○			
5.3	**Elektronische maatregelen**		***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	***Norm***
1	Het opbergmiddel met een *TBB*, de ruimte waar het opbergmiddel is geplaatst en de aanliggende ruimten zijn voorzien van een *Indringer Detectie- en Signaleringssysteem* (*IDSS*). Welke actief doormeld bij afwezigheid van personen.	IDSS	●	●	●	○		
2	Het activeren en deactiveren van een *IDSS* kan alleen door middel van een tweefactor *Authenticatie*.	IDSS	●	●	●	○		
3	Het *IDSS* functioneert 24 uur per dag en 7 dagen per week. Nooddeuren dienen in een 24-uurs zone te zitten onder constante detectie.	IDSS	●	●	●	○		
4	De ruimte met een *TBB* is binnen het *IDSS* als aparte zone opgenomen. Deze zone is actief wanneer er geen *Geautoriseerd* personeel aanwezig is in de ruimte.	IDSS	●	●	●	○		
5	Er is doormelding van een *IDSS* (Alarmsysteem)	IDSS	●	●	●	○		
6	Een alarm van een *IDSS* leidt tot een alarmopvolging binnen de gestelde *Interventietijd*.	IDSS	●	●	●	○		

7	Het *IDSS* signaleert en registreert uitval van de primaire stroomvoorziening. Tevens kan het IDSS nog minimaal voor 4 uur volledig blijven functioneren bij uitval van de primaire stroomvoorziening.	IDSS	●	●	●	○		
8	Het *IDSS* en de componenten zijn niet onopgemerkt te saboteren c.q. een *Compromittatie wordt gemeld als alarm* en beschikken over anti-maskings maatregelen.	IDSS	●	●	●	○		
9	Detectie vindt onder alle (klimatologische) omstandigheden plaats.	IDSS	●	●	●	○		
10	Alleen elektronische apparatuur die essentieel is voor het uitvoeren van de opdracht is toegestaan binnen de ruimten van het *TBB*. Een lijst van de apparatuur is opgenomen in het beveiligingsplan.	Beperken elektronische apparatuur	●	●	●			
11	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. Door daarvoor gescreende personeelsleden. Rapportage en plannen dienen conform de TBB te zijn beveiligd tijdens alle omstandigheden.	Beheer van systemen	●	●	●			
12	Om een alarm te verifiëren, mogen camera's worden gebruikt.	Camera’s	●	●	●	●		
13	Beveiligingscamera's zijn toe te passen, ook om later onderzoek te kunnen doen naar incidenten betreffende ongewenste toegang. De gehele naderingsroute naar het *TBB* is onder observatie.	Camera’s	●					
14	Beveiligingscamera's zijn toe te passen, ook om later onderzoek te kunnen doen naar incidenten betreffende ongewenste toegang.	Camera’s		●	●			
15	Als gebruik is gemaakt van elektronische sloten, zijn maatregelen getroffen om te detecteren of toegangsverlening buiten de ingestelde bloktijden plaatsvindt.	Dwangdetectie	●	●	●			

17	Er is een *ETS* voor gecontroleerde toegang tot het compartiment geïnstalleerd en in werking.	ETS	●	●	○	○		
16	Een *ETS* is uitgerust met een Anti Pass Back (APB) systeem.	ETS	●	●				
18	Een *ETS* is voorzien van *Logging*, waarbij de logs tenminste een jaar worden bewaard.	ETS	●	●	○	○		
19	Een *ETS* is zodanig uitgevoerd dat, wanneer het systeem uitschakelt of uitvalt, alle toegangen tot het compartiment mechanisch worden afgesloten of elektronisch afgesloten blijven voor de duur van minimaal 4 uur. Er dient controle op de primaire stroomvoorziening te zijn incl. alarmmelding bij uitval. Indien de primaire stroom niet tijdig terug is dient er manbewaking te komen.	ETS	●	●	○	○		
20	Een *ETS* is zodanig uitgevoerd dat een noodknopbediening of mechanische paniek ontgrendeling binnen het object op zodanige wijze is aangebracht dat bij calamiteit het object snel in het kader van veiligheid (safety) kan worden verlaten. De noodknopbediening of mechanische paniek ontgrendeling is van buitenaf niet bereikbaar. Er dient een alarm melding te zijn bij gebruik van de noodknop cq mechanische paniek ontgrendeling. Na gebruik van de noodknopbediening of mechanische paniek ontgrendeling dienen adequate veiligheidsmaatregelen te worden getroffen ter bescherming van het *TBB*.	ETS	●	●	○	○		
21	Wanneer een beveiligingssysteem (*ETS* of *IDSS*) gekoppeld is aan een gebouwbeheersysteem, gelden de beveiligingsmaatregelen van het beveiligingssysteem ook voor het gebouwbeheersysteem.	ETS	●	●	○	○		
5.4	**Reactieve maatregelen**		***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	**TBB 4 / *DV***	***Open***	***Norm***

1	Alle Meldingen uit het *IDSS* en het *ETS* moeten leiden tot tijdige *Interventie*. Onder tijdig verstaat men bij *TBB* 1 en *TBB* 2: een positief beveiligingsrendement en bij *TBB* 3 en *TBB* 4: *Interventie* binnen 2- 4 uur	Interventie	●	●	○	○		
2	Interventie vindt plaats door daartoe aangewezen en opgeleid personeel dat aanwezig is in de directe omgeving van het gebouw met een *TBB*.	Interventie	●	●	●	●		
3	Beveiligingspersoneel informeert bij een alarmmelding op de beveiliging / ETS terstond de *BF*.	Interventie	●	●	●	○		
4	Reactie op (technische) storingen moet leiden tot het herstellen van het gewenste beveiligingsrendement.	Interventie	●	●	●	○		
5	Na een alarm vindt controle van het *TBB* plaats door de *BF* of diens gemandateerde.	Incidentafhandeling	●	●	●	○		
6	Alarmverificatie vindt aan de buitenzijde van het compartiment met een *TBB* plaats. Hierbij zijn alle toegangen, gevelopeningen, daken e.d. gecontroleerd.	Incidentafhandeling	●	●	●	●		
7	Personeel dat alarmverificatie uitvoert, heeft ten tijde van de alarmverificatie niet de beschikking over sleutels of codes die toegang geven tot het *TBB*.	Incidentafhandeling	●	●	●	●		
8	Een Particuliere Alarm Centrale beschikt over een justitiële erkenning en voldoet aan de NEN-EN 50518 norm.	Incidentafhandeling	●	●	●	●		
5.5	**Transport en verzenden**		***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	***Norm***
1	Een *TBB* wordt uitsluitend buiten het compartiment gebracht als dit voor de voortgang van de werkzaamheden absoluut noodzakelijk is.	Transport en Verzending	●	●	●	●		
2	De *BF* stelt voorschriften op voor het transporteren en verzenden van een *TBB* en houdt hier toezicht op.	Transport en Verzending	●	●	●	●		
3	Een *TBB* mag nooit mee naar huis worden genomen.	Transport en Verzending	●	●	●	○		
4	Transport van *TBB* is vooraf gemeld aan *BZ*.	Transport en Verzending	●	●	●	●		

5.5 a	Transport en verzenden binnenland		*TBB* 1 / ZG	*TBB* 2 / G	*TBB* 3 / C	*TBB* 4 / *DV*	*Open*	*Norm*
5	De opdrachtnemer stelt een transport beleid van een TTB op, BZ krijgt inzicht in het transport beleid.	Transport en Verzending	●					
6	Een *TBB* is uitsluitend mee te nemen in een door *BZ* goedgekeurd afsluitbaar transportmiddel.	Transport en Verzending		●	●			
7	Transport van een *TBB* vindt plaats: - handcarried, al dan niet met eigen vervoer, door twee *Geautoriseerde* medewerkers, of - met inschakeling van een door *BZ* goedgekeurd transport- / koeriersbedrijf, of.	Transport en Verzending		●	●			
8	Een *TBB* is uitsluitend mee te nemen in een afsluitbaar transportmiddel.	Transport en Verzending				●		
9	Transport van een *TBB* vindt plaats: - handcarried, al dan niet met eigen vervoer, door een *Geautoriseerde* medewerker, of - met inschakeling van een door BZ goedgekeurd transport-/ koeriersbedrijf, of - met inschakeling van een transport-/koeriersbedrijf, begeleid door een *Geautoriseerde* medewerker.	Transport en Verzending				●		
10	Het transport-/koeriersbedrijf waaraan het *TBB* zonder toezicht of begeleiding wordt toevertrouwd is als *Subcontractor* aangemeld bij *BZ*.	Transport en Verzending		●	●	○		
11	Transport van een *TBB* gaat via de kortst mogelijke weg zonder onderbrekingen. Het *TBB* blijft onder toezicht, voertuigen worden niet onbeheerd gestald.	Transport en Verzending		●	●	●		
12	Verzenden van een *Gerubriceerd* en/of *gemerkt TBB* per post is niet toegestaan.	Transport en Verzending	●	●	○			
13	Verzenden van een *Gerubriceerd* en/of *gemerkt TBB* per post is toegestaan binnen Nederland, met gebruikmaking van aangetekende post, in dubbele verpakking en met onmiddellijke ontvangstbevestiging.	Transport en Verzending			○	●		

5.5 b	Transport en verzenden buitenland		*TBB* 1 / ZG	*TBB* 2 / G	*TBB* 3 / C	*TBB* 4 / *DV*	*Open*	*Norm*
14	Transport van een *TBB* geschiedt uitsluitend door tussenkomst van *BZ*.	Transport en Verzending	●					
15	Een *TBB* mag zonder toestemming van *BZ* niet worden meegenomen naar het buitenland.	Transport en Verzending		●	●	●		
16	Internationaal transport van een *TBB* vindt plaats na goedkeuring van het transportplan door *BZ*.	Transport en Verzending		●	●	●		
17	Voor transport van *Bijzondere Informatie* naar het buitenland kan worden teruggevallen op *BZ* (“Government-to-Government”-procedure).	Transport en Verzending		●	●	●		
18	Verzenden van een *Gerubriceerd* en/of *gemerkt TBB* per post is niet toegestaan.	Transport en Verzending	●	●	○			
19	Verzenden van een *Gerubriceerd* en/of *gemerkt TBB* per post is toegestaan, met gebruikmaking van aangetekende post, in dubbele verpakking en met onmiddellijke ontvangstbevestiging.	Transport en Verzending			○	●		
5.6	**Fysieke opslag, verwerking en ontwikkeling**		*TBB* 1 / ZG	*TBB* 2 / G	*TBB* 3 / C	*TBB* 4 / *DV*	*Open*	*Norm*
1	Geregistreerd is wie een *TBB* onder zijn berusting heeft.	Registratie en Rubricering	●	●	●			
2	Geregistreerd is wie werkzaamheden aan een *TBB* heeft uitgevoerd of *Bijzondere Informatie* heeft ingezien.	Registratie en Rubricering	●	●				
3	*Informatie* waarbij de steller vermoedt dat bij *Compromittatie* voor de Staat schade kan ontstaan, is *Gerubriceerd*. De *Rubricering* is door de *BF* vastgesteld, geregistreerd en aan *BZ* gemeld.	Registratie en Rubricering	●	●	●	●		
4	Een *TBB* is geregistreerd en van een kenmerk (labeling) voorzien.	Labeling	●	●	●			
5	Een *TBB* is geregistreerd en van een uniek exemplaarnummer voorzien.	Labeling	●	●				

6	*Rubriceringen* zijn conform BZ beleid aangebracht.	Labeling	●	●	●	●		
7	De reproductie van *Informatie* geschiedt alleen met toestemming van degene die de *Rubricering* heeft vastgesteld.	Reproductie	●	●	●			
8	Gemaakte reproducties zijn geregistreerd.	Reproductie	●	●	●			
9	Het maken van reproducties is voorbehouden aan daartoe aangewezen geautoriseerd personeel dat ook zorg draagt voor de registratie hiervan.	Reproductie	●	●	●			
10	Reproducties kennen dezelfde *Rubricering* als het origineel, ook als slechts delen van het origineel is gebruikt.	Reproductie	●	●	●	●		
11	Er zijn niet meer reproducties gemaakt dan strikt noodzakelijk is.	Reproductie	●	●	●	●		
12	Reproducties maken, is alleen toegestaan met door *BZ* toegestane middelen.	Reproductie	●	●	●			
13	Reproductiemiddelen worden beschouwd als een informatiesysteem en worden minimaal op hetzelfde niveau beveiligd als de verwerkte informatie.	Reproductie	●	●	●	●		
14	In geval van vernietiging wordt door de *BF* of een aangewezen medewerker met de juiste *Autorisatie* een proces verbaal van vernietiging opgemaakt.	Vernietiging	●	●	●			
15	Vernietigen van *Informatie* geschiedt conform Nederlandse wetgeving.	Vernietiging	●	●	●	●		

5: Digitaal

Periodiek wordt het Nationaal Cyber Security Beeld Nederland (CSBN) tot stand gebracht in nauwe samenwerking tussen publieke en private partijen. Doel is het jaarlijks bieden van inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van “Cyber Security”. Inzicht en expertise in het tot stand komen van het CSBN komen vanuit overheidsdiensten, vitale sectoren en de wetenschap.

Een van de kernbevindingen in het CSBN is dat cybercriminelen en staten de grootste dreiging vormen. De dreiging van digitale spionage door statelijke actoren is onverminderd groot. De tendens is een groeiend aantal digitale spionageaanvallen met toenemende complexiteit en steeds diepere impact. De verwachting is dat deze tendens zich de komende jaren zal voortzetten. Bijna elke buitenlandse inlichtingendienst heeft de afgelopen jaren geïnvesteerd in (offensieve) digitale capaciteiten.

De dreiging van digitale spionage tegen BZ en bondgenootschappelijke netwerken is significant, groeiend en steeds vaker geavanceerd en agressief van aard. Sommige tegenstanders vallen op door de grootschaligheid waarmee zij bedrijfsgegevens of gevoelige overheidsinformatie proberen te stelen terwijl andere bij hun activiteiten veel meer gebruik maken van geavanceerde, technische middelen.

De Nederlandse (rijks)overheid, en bondgenootschappelijke netwerken zijn in dat kader een gewild doelwit van digitale spionage gebleken.

De inlichtingen- en veiligheidsdiensten verrichten daarbij attributie onderzoek en heeft een aantal van deze aanvallen kunnen koppelen aan digitale spionagecampagnes van specifieke statelijke actoren. De meest gebruikte aanvalsmiddelen zijn ”spear phishing” en ”wateringholes”. Dit zijn plaatsen op het internet waar grotere groepen gebruikers bij elkaar komen en daardoor op een effectieve wijze besmet kunnen worden door de aanvaller. De digitale aanvallen op netwerken van zowel overheid als industrie onderstrepen het belang om aandacht te blijven besteden aan de bevordering van het beveiligingsbewustzijn van de medewerkers en de accreditatie van de IT-infrastructuur.

Digitale aanvallen maken vaak gebruik van nieuwe methodieken zoals verborgen communicatiekanalen en nog onbekende kwetsbaarheden in software (“zero-days”). Statelijke actoren zijn actief op zoek naar “zero-days” om deze te misbruiken. Zo’n digitale aanval wordt ook wel aangeduid met “Advanced Persistant Threat” (APT). Een APT kenmerkt zich onder andere door complexiteit, het gebruik van “zero-days” en het bijvoorbeeld ontwijken van detectiesoftware. Social Engineering is hierbij meestal de basis voor succesvolle injectie van “malware” in het netwerk van het doelwit en vormt daarmee de start van een APT.

Preventieve en detectieve beveiligingsmaatregelen zijn veelal niet afdoende voor het ontdekken van een APT. Het ontdekken en mitigeren van een APT is alleen mogelijk door zorgvuldige Incident Handling.

Het waarborgen van de vertrouwelijkheid en integriteit van een TBB is daarom, naast het implementeren van maatregelen in het organisatorische, personele en fysieke domein, steeds meer een zaak van het implementeren van maatregelen in het voorkomen en oplossen van incidenten in het digitale domein (*Cyber Space*).

Dit hoofdstuk beschrijft de basisprincipes van digitale beveiliging (“*Cyber Security”)* genoemd, waarbij permanent bewustzijn van dreiging en noodzaak tot beveiligen essentieel is.

ABBO 2018 eisen								
H6 DIGITAAL		**BEVEILIGINGSREGIME**						
6.1	***Cyber* Beveiligingsorganisatie Specificatie**	**Specificatie**	***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	***Norm***
1	De BF heeft de taak om toezicht te houden op een veilige inrichting van de digitale omgeving binnen het bedrijf.	Beveiligingsfunctionaris	●	●	●	●		
3	De *BF* is verantwoordelijk voor de analyse op beveiligingsrelevante issues van *Loggings* en voor *Monitoring* van activiteiten die een impact op de beveiliging hebben.	Logging en monitoring	●	●	●	●	○	
4	De *BF* laat zich periodiek informeren over de inrichting van integriteit, vertrouwelijkheid en controleerbaarheid van de digitale omgeving binnen het bedrijf.	Digitale omgeving	●	●	●	●	●	
5	De beveiligingsfunctionaris heeft meerdere malen per jaar een geformaliseerd overleg over de interne controle op *Cyber* security .	Beveiligingsplan	●	●	●	●	●	
6	Beveiligingsincidenten in het digitale domein dienen direct bij de *BF te* worden gemeld, en direct doch uiterlijk binnen de normstelling genoemd in tabel “Classificatie” met behulp van de *Incident Response Procedure* (*IRP*) aan *BZ* te zijn bekend gesteld.	Beveiligingsplan	●	●	●	●	●	
7	Het beveiligingsplan beschrijft de beveiligingsmaatregelen die noodzakelijk zijn voor de digitale omgeving waarin zich het *TBB* bevindt. In het *Beveiligingsplan* is tenminste aandacht besteed aan eisen en maatregelen ten aanzien van de *Cyber* beveiligingsorganisatie, *Cloud Computing* en *Virtualisatie*, *BYOD/CYOD*, *Versleuteling*, *communicatie*- en	Beveiligingsplan	●	●	●	●	●	

	netwerkbeveiliging, systeem- en softwareontwikkeling en *TEMPEST*.							
8	De *BF* verstrekt de aan het bedrijf toebehorende externe *IP adressen* aan *BZ*.	raportage	●	●	●	●	●	
9	De *BF* houdt door middel van een registratie nauwgezet toezicht op locatie, uitgifte, inname en herkomst van alle door de organisatie in ontvangst of beheer genomen digitale *TBB.* Dit is van toepassing op zowel de gegevensdragers als *Documenten* die een *TBB* bevatten.	Overzicht	●	●	●	●		
10	De *BF* voert periodiek controle uit op implementatie van de in de *ABBO* 2018 opgenomen beveiligingseisen. De resultaten van deze controles worden vastgelegd en besproken met *BZ*.	Controle	●	●	●	●	●	
11	Minimaal eens per jaar dient door de *Cyber* beveiligingsorganisatie of rechtstreeks in opdracht hiervan een *Penetratietest* te zijn uitgevoerd op de *TBB* omgeving. De resultaten hiervan worden gedeeld met *BZ*.	Controle	○	○	○	○	○	
12	Indien een externe partij betrokken is bij het beheer van een *TBB* omgeving, dient deze partij een door *BZ* goedgekeurde *Subcontractor* te zijn die voldoet aan de *ABBO* 2018.	Controle	●	●	●	●		
13	De *BF* is namens het management bevoegd tot het (laten) nemen van gepaste beveiligingsmaatregelen op het gebied van *Cyber* security.	Beveiligingsorganisatie	●	●	●	●	●	
14	Indien de opdrachtnemer een grote verzameling aan personeelsgevoelige data in ontvangst neemt, opslaat en/of verwerkt, dient de opdrachtnemer de gegevensverzameling minimaal als *TBB* 4 te behandelen.	labeling	○	○	○	●	●	
15	De *BF* heeft ervoor gezorgd dat beveiligingsmaatregelen getroffen zijn die:	Beveiligingsplan	●	●	●	●	●	

	- de integriteit en vertrouwelijkheid van data blijvend garanderen; - de vertrouwelijkheid van data garanderen tijdens of na uitval van het systeem; - het regelmatig testen borgen van de getroffen maatregelen t.b.v. de continuïteit .							
16	De *Opdrachtnemer* draagt zorg voor de ontwikkeling van de benodigde competenties en kennis van de *BF en* het personeel dat betrokken is bij de behandeling van een *TBB* door relevante training, opleiding en mogelijk deelname aan oefeningen.	Beveiligingsorganisatie	●	●	●	●	●	
17	De *BF* beschikt over voldoende kennis om invulling te geven aan zijn verantwoordelijkheden, en dient minimaal te beschikken over een *CISSP of gelijkwaardige* certificering.	Beveiligingsorganisatie	●	●	●	●	●	
18	IT beheerders beschikken over actuele kennis om *Cyber* dreigingen en kwetsbaarheden van het beheerde systeem op waarde te kunnen schatten.	Beveiligingsorganisatie	○	○	○	○	○	
19	Medewerkers doorlopen jaarlijks een *Cyber* security-awareness training met goed gevolg. Hier komen minimaal de volgende onderwerpen aan bod: - *ABBO* 2018; - dreigingen en uitingsvormen in het digitale domein bijvoorbeeld *Social Engineering*; - hoe corporate- en persoonlijke informatie gestolen kan worden via het digitale domein met begrip over de wijze waarop aanvallers misbruik maken van menselijk handelen, zoals de natuurlijke drang behulpzaam te zijn bij de beantwoording van vragen; - welke *Informatie* beschermd wordt en hoe de bescherming in lijn is met het beveiligingsplan;	Beveiligingsplan	●	●	●	●	●	

	- wanneer incidenten te rapporteren aan de *BF*							
6.2	**Data opslag en transport**	**Specificatie**	***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	**Norm**
1	Een netwerk waarop TBB zijn opgeslagen, heeft nooit een verbinding met een ander (inter, extern, publiek) netwerk, tenzij met toestemming van *BZ*..	Compartimentering	●	●	●	○		
2	Voor dataopslag is *Compartimentering* doorgevoerd: - dataopslag vindt plaats op basis van logische samenhang; - het is niet toegestaan *GerubriceerdeInformatie* in hetzelfde compartiment op te slaan als niet-*GerubriceerdeInformatie*; - het is niet toegestaan *Informatie* op te slaan in één en hetzelfde netwerksegment indien deze *Informatie* behoort aan verschillende *Opdrachtgevers* en bij verschillende projecten.	Compartimentering	○	○	○	○	○	
3	Medewerkers bergen *TBB* op de daartoe bestemde plaats op indien men de *Informatie* niet gebruikt (bijv. vanwege afwezigheid of andere werkzaamheden), onbeheerde gebruikersapparatuur is geblokkeerd en tijdens een onderbreking van de werkzaamheden wordt de ruimte afgesloten.	Compartimentering	●	●	●	●		
4	Indien dataopslag van een *TBB* door een derde partij is gefaciliteerd, is deze derde partij als *Subcontractor* aangemerkt.	dataopslag	○	○	○	○		
5	Een TBB dat is opgeslagen op mobiele werkstations/laptops mag niet zonder toestemming van BZ worden meegenomen op dienstreis naar het buitenland.	Datatransport	●	●	●			

6	Mobiele werkstations/laptops waarop een TBB is opgeslagen en die op dienstreis naar het buitenland worden meegenomen dienen: - van door *NBV* goedgekeurde *Vercijfering* te zijn voorzien; - alleen de hoogst noodzakelijke informatie in opslag te hebben; - niet gebruikt te worden in publieke ruimten. Er mag geen koppeling via "publieke" *WLAN* tot stand worden gebracht;	Datatransport				○		
7	Apparatuur waarop zich *TBB* bevinden, is beveiligd conform de eisen behorende bij het hoogst gerubriceerde *TBB*.	Datatransport	●	●	●	●		
8	Uitwisseling van *TBB* is alleen toegestaan indien gebruik is gemaakt van de *Vercijfering* voorgeschreven door het *NBV* en na toestemming van *BZ*.	Datatransport	○	○	○	○		
9	Een *TBB* mag niet per e-mail e.d. worden verstuurd. Ook niet als bijlage.	Datatransport	●	●	●			
10	Een *TBB* in e-mail is versleuteld met een door het *NBV* toegestaan vercijferalgoritme. In de mail is de *Rubricering* aangegeven.	Datatransport				○		
11	Het versturen en ontvangen van e-mail is geregistreerd en gearchiveerd.	Datatransport				○	○	
12	Op transport van informatie op digitale informatiedragers zijn de eisen genoemd onder 3.2 in het hoofdstuk fysieke beveiliging van toepassing	Datatransport	●	●	●	●		
6.3	**Toegang tot data**	**Specificatie**	***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	**Norm**
1	De *BF* controleert verstrekte *Autorisaties* op juistheid.	Accesscontrol/logging	wekelijks	wekelijks	wekelijks	maandelijks	maandelijks	

2	Administrator- of rootrechten zijn slechts aan een beperkte groep beheerders toegekend. Van deze beheerders wordt een register bijgehouden. De beheerders administreren het gebruik van de administrator- of rootaccounts.	Accesscontrol/logging	●	●	●	●	●	
3	Functionele of groepsaccounts zijn niet toegestaan.	Accesscontrol/logging	●	●	●			
4	Functionele of groepsaccounts zijn uitsluitend na toestemming van *BZ t*oegestaan.	Accesscontrol/logging				○	○	
5	Wanneer gebruik is gemaakt van een functioneel- of groepsaccount blijkt uit een administratie welke natuurlijke persoon van dit account gebruikgemaakt heeft.	Accesscontrol/logging				○	○	
6	Gebruikers-*Identificatie* en -*Authenticatie* vindt plaats per natuurlijk persoon.	Accesscontrol/logging	●	●	●	●	●	
7	Het inlogmechanisme is zo geconstrueerd dat *Ongeautoriseerde* gebruikers geen toegang verkrijgen tot het netwerk of applicatie.	Accesscontrol/logging	●	●	●	●	●	
8	De minimale lengte van wachtwoorden is 10 karakters (*Passphrases* worden gebruikt om wachtwoorden te genereren).	Accesscontrol/logging	○	○	○	○	○	Iso
9	Gebruikerswachtwoorden voldoen aan onderstaande eisen: - om de zestig dagen wijzigen; - minimale lengte zoals beschreven; - enige complexiteit (gebruik speciale karakters); - gebruik hoofd- en kleine letters; - niet te gebruiken in automatische aanlogprocessen/batchfiles; - initieel verkregen wachtwoorden per direct wijzigen; - niet herkenbaar & vindbaar voor derden opgeslagen; - verplicht wijzigen na vermoeden *Compromittatie*;	Accesscontrol/logging	○	○	○	○	○	Iso

	- altijd persoonsgebonden.							
10	Gebruik van tokens of biometrie is na toestemming *BZ* toegestaan. Biometrie wordt uitsluitend als een van de twee factoren voor *Authenticatie* toegestaan.	Accesscontrol/logging	○	○	○	○	○	
11	Indien tokens of biometrische toepassingen zijn gebruikt, mag het niet zonder meer mogelijk zijn deze toepassingen buiten werking te stellen om daarna alsnog toegang tot een *TBB* te verkrijgen.	Accesscontrol/logging	○	○	○	○		
12	Het eerste inlogscherm vermeldt de wettelijke voorschriften en strafbaarheid van *Ongeautoriseerde* toegang.	Accesscontrol/logging	●	●	●	●	●	
13	Aanlogprocedures voor werkstations zijn vastgelegd in een procedure en vertaald naar een gebruikersinstructie.	Accesscontrol/logging	●	●	●	●	●	
14	Het aantal foutieve inlogpogingen is beperkt tot drie, waarna blokkade volgt.	Accesscontrol/logging	●	●	●	●	●	
15	Het deblokkeren van een gebruikersaccount gebeurt door tussenkomst van de *BF.*	Accesscontrol/logging	●	●	●	●	●	
16	Er zijn regels opgesteld voor het hebben van een “clear screen” bij het verlaten van de werkplek.	Clear screen	●	●	●	●	●	

17	Bestaande sessies zijn automatisch geblokkeerd na tien minuten inactiviteit en worden na maximaal dertig minuten inactiviteit beëindigd.	Remote werken	●	●	●	○	○	
18	Remote werken is niet toegestaan.	Remote werken	●	●	●			
19	Indien toegang tot een *TBB* via een remote inlogvoorziening mogelijk is, is een procedure hiervoor in het beveiligingsplan opgenomen.	Remote werken				●		
20	De technische inrichting en de procedurele borging van de remote inlogvoorziening is voor ingebruikname ter beoordeling aan *BZ* voorgelegd.	Remote werken		.		●		
21	Voor remote toegang wordt gebruik gemaakt van de door het *NBV* goedgekeurde producten.	Remote werken			.	●	○	
22	Toegang door derden tot (delen van) omgevingen waar een *TBB* op wordt verwerkt, is niet toegestaan. Hieronder wordt ook verstaan aangekondigde en onaangekondigde gewenste toegang tot de omgeving uit hoofde van toezicht, inspectie en of audit. Uitzonderingen hierop zijn in overleg met *BZ* vastgesteld.	Logging & monitoring	●	●	●	●		
23	Er is een eenduidige procedure beschikbaar die inzichtelijk maakt op welke wijze medewerkers toegang hebben tot een digitaal *TBB*.	Logging & monitoring	●	●	●	●		
24	Binnen een *Gerubriceerd* netwerk zijn de door personen opgestarte handelingen altijd terug te voeren op natuurlijke personen.	Logging & monitoring	●	●	●	●		
25	Het systeem geeft aan wie welke autorisatie tot *Gerubriceerde Informatie* heeft.	Logging & monitoring	○	○	○	○		

26	Rechten tot een *TBB* zijn op basis van "*Need-to-Be*", "*Need-to-Know*" en "Least Privilege" verleend.	Logging & monitoring	●	●	●	●		
27	Het systeem voorkomt ongeautoriseerde toegang tot een *TBB.*	Logging & monitoring	●	●	●	●		
6.4	**Logging en Monitoring**	**Specificatie**	***TBB* 1 / ZG**	***TBB* 2 / G**	***TBB* 3 / C**	***TBB* 4 / *DV***	***Open***	**Norm**
1	Gebruikershandelingen en netwerkactiviteiten worden continu gemonitord en gelogd.	Logging & monitoring	●	●	●	●	○	
2	Beveiligingsrelevante activiteiten worden gelogd. (system, event, applicatie en user-*Logging*).	Logging & monitoring	●	●	●	●	●	
3	Configureer netwerk perimeter devices, zoals firewalls, netwerk IPS en ingaande en uitgaande *Proxies*, zodanig dat alle (toegestane en geblokte) metaverkeersgegevens zijn gelogd.	Logging & monitoring	○	○	○	○	○	
4	Er vindt doorlopend controle plaats op ongeautoriseerde verbindingen.	Logging & monitoring	●	●	●	●	●	
5	Er vindt geen (inter)netwerkverkeer plaats. Het normbeeld blijft altijd hetzelfde.	Logging & monitoring	●	●	●			
6	Afwijkingen van het normbeeld (anomalies) met betrekking tot sessies door perimeter devices zijn onderzocht op aanwezige "covert channels". Monitoring op ongebruikelijke creaties en aanwezigheid van processen teneinde infiltratie te onderkennen, vindt continu plaats.	Logging & monitoring				○	○	
7	Alle hosts en geupdate content in het netwerk worden doorlopend gescand op *Malware* waarbij gebruik is gemaakt van "up-to-date" anti-*Malware* software.	Logging & monitoring	●	●	●	●	●	

8	Kwetsbaarheid assessments en security tests worden periodiek uitgevoerd op de online sites en applicaties om zeker te stellen dat de beveiliging "up-to-date" is.	Logging & monitoring	○	○	○	○	○	
9	Er vindt doorlopend onderzoek plaats naar de kwetsbaarheden in de gemonitorde systemen.	Logging & monitoring	●	●	●	●	●	
10	De opslag van loggegevens vindt plaats op een separate log-server en blijft minimaal drie jaar opvraagbaar. Toegang tot de log is slechts voorbehouden aan een beperkte groep, ook toegang tot de logomgeving dient gelogd te worden.	Logging & monitoring	○	○	○	●	●	
11	In '*Demilitarized Zone*' (*DMZ*) zijn monitoring systems ingericht die ten minste *Packet headers* informatie en bij voorkeur full *Packet header* en payload van het data verkeer monitoren. De monitoring richt zich op netwerkoverstijgend verkeer. Security Information Event Management (SIEM) of log analyse systemen zijn ingericht zodat correlatie tussen events kan plaatsvinden.	Logging & monitoring				○		
12	Er is gebruik gemaakt van *Honeypots of honeynets*.	Logging & monitoring				○		
13	De *BF* ontvangt eens per week een overzicht van *ongeautoriseerd* gekoppelde devices en software op de netwerken. Dit overzicht bevat een duidelijke toelichting op geconstateerde afwijkingen en de genomen maatregelen.	Logging & monitoring	○	○	○	○	○	
14	De *BF* controleert wekelijks de log-gegevens op afwijkingen van het normbeeld (anomalies) en zendt een samenvatting naar *BZ* indien anomalies zijn vastgesteld.	Logging & monitoring	●	●	●	●	○	
15	Configureer de operating systems zo, dat de event logs geassocieerd zijn met gebruikers, gericht op het gebruik van resources door gebruikers.	Logging & monitoring	●	●	●	●	●	
16	Binnen het domein is het Network Time Protocol (NTP) geïmplementeerd zodat alle "timestamps" in de logfiles consistent zijn.	Logging & monitoring	●	●	●	●	●	

17	Controleer synchronisatie van systeemklokken eens per zestig dagen.	Logging & monitoring	●	●	●	●	●	
18	Op verzoek van *BZ* wordt, binnen het kader van de *Wiv*, medewerking verleend aan : - het statisch monitoren van netwerken en hosts door gebruik van monitoring boxen; het actief real time monitoren van netwerken en hosts, met het doel informatie te verzamelen over (mogelijke) digitale aanvallen en het *Mitigeren* van deze aanvallen; - actieve *Monitoring* en detectie op een knooppunt binnen het bedrijf of bij de Internet Service Provider (ISP) die het IP-verkeer afhandelt; - indien een CAT 1 incident plaatsvindt, is de *BZ* bevoegd actieve maatregelen te laten treffen op het bedrijfsnetwerk of bij de ISP om de dreiging te *Mitigeren*.	Logging & monitoring	○	○	○	○	○	
6.5	**Beheer, onderhoud, contingency planning**	**Specificatie**	***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3 / C***	***TBB 4 / DV***	***Open***	**Norm**
1	Servers en andere apparatuur waarop zich een concentratie van *TBB* van Geheim en lager bevindt, zijn geplaatst in een ruimte die op ZG niveau is beveiligd.	Beveiligde ruimte	○	●				
2	Servers en andere apparatuur waarop zich een concentratie van *TBB* van Confidentieel en lager bevindt, zijn geplaatst in een ruimte die minimaal op G niveau is beveiligd.	Beveiligde ruimte		○	●			
3	Servers en andere apparatuur waarop zich een concentratie van *TBB* van Departementaal Vertrouwelijk en lager bevindt, zijn geplaatst in een ruimte die op minimaal C niveau is beveiligd.	Beveiligde ruimte			○	●		
4	Servers en andere apparatuur waarop zich een concentratie van ongerubriceerde, gemerkte *TBB* bevindt, zijn geplaatst in een ruimte die op minimaal DV niveau is beveiligd.	Beveiligde ruimte				○		

5	Bij de inrichting van het netwerk is *Compartimentering* toegepast, op basis van het: "*Need-to-Be*", "*Need-to-Know*" en "Least Privilege" principe.	Need to Know	●	●	●	●	○	
6	Systeemcomponenten - zoals firewall, router, switches, servers - zijn ingericht volgens een standaard configuratie. Deze configuratie wordt regelmatig gecheckt op actualiteit.	configuratie	○	○	○	○	○	
7	Onderhoud en beheer vinden op locatie plaats en zijn uitsluitend toegestaan met door *BZ* goedgekeurde procedures.	Onderhoud en beheer	●	●	●			
8	Onderhoud en beheer vinden op locatie plaats en zijn uitsluitend toegestaan met toestemming van *BZ*.	Onderhoud en beheer				○		
9	Indien werkzaamheden door technisch beheer een impact hebben op een *TBB* omgeving worden deze via het wijzigingen-beheerproces en na accordering door de *BF* uitgevoerd.	Onderhoud en beheer	●	●	●	●		
10	Remote werken en beheer is niet toegestaan.	Remote werken	●	●	●			
11	Remote beheer van mobile devices is toegestaan indien gebruik is gemaakt van door *BZ* goedgekeurde middelen.	Remote werken				○		
12	Bedieningsprocedures voor remote werken zijn gedocumenteerd in het beveiligingsplan.	Remote werken				●		
13	De door de fabrikant van de gebruikte apparatuur (server, standalone) minimaal voorgeschreven en aangeraden beveiligingsmaatregelen zijn uitgevoerd.	Remote werken	○	○	○	○		
14	Voor het aanbrengen van wijzigingen in of aan een *TBB* omgeving is een helder wijzigingenbeheer ingericht. Op basis van registraties is duidelijk wie welke activiteiten heeft uitgevoerd, en wie op welk moment specifieke wijzigingen heeft doorgevoerd (bijvoorbeeld: registratie van de installatie van updates van patches).	wijzigingenbeheer	●	●	●	●		

15	Wijzigingen die mogelijkerwijs een impact hebben op de toegang tot *TBB*'n zijn altijd aan de *BF* ter beoordeling en goedkeuring voorgelegd.	wijzigingenbeheer	●	●	●	●		
16	Er is een registratie van digitaal ontvangen en verzonden *TBB,* die: - zowel fysieke, digitale als back-up omgevingen omvat; - op een veilige plaats is gearchiveerd; - ieder *TBB* uniek identificeerbaar en altijd traceerbaar bevat; - gecontroleerd uitgegeven en ingenomen mobiele apparatuur en gegevensdragers bevattende een *TBB* omvat.	Registratie TBB	●	●	●	.		
17	Alle apparatuur en systemen die gebruikt zijn voor het verwerken van een *TBB* worden in een netwerk- of configuratietekening bijgehouden. Hierin zijn duidelijk aangegeven de locatie en de functie van de component.	apparatuur en systemen	○	○	○	○		
18	Alle apparatuur en systemen die gebruikt zijn voor het verwerken van een *TBB* worden bijgehouden in een configuratiedatabase. Tenminste zijn de unieke ID-omschrijving, type en fabrikant, datum indienststelling, locatie, gebruiker, onderhoud en bijzonderheden bijgehouden.	apparatuur en systemen	○	○	○	○		
19	Naast de hiervoor beschreven bepalingen is een eenduidige omschrijving van de configuratie beschikbaar. Hierin dient te zijn opgenomen: - vermelding *Netwerksegmentatie*; - beheersegment / *DMZ* / standaard gebruikersomgeving / gastennetwerk / dataopslag; - gebruikte hardware; - gebruikte software; - externe/interne koppelingen; - vermelding locatie;	configuratie	●	●	●	●		

	- gebruikte *Vercijfering*.							
20	Capaciteitsplanning is zodanig ingericht dat de integriteit van de data niet verloren gaat.	Capaciteitsplanning	○	○	○	○		
21	Reservekopieën (back-ups) worden minimaal drie jaar en maximaal voor de duur van een project opgeslagen. De opslag vindt plaats op een beveiligingsniveau dat in overeenstemming is met de *Rubricering* die is vastgesteld voor de *Informatie* op deze reservekopieën, met inachtneming van eisen 4.5.1 t/m 4.	Reservekopieën (back-ups)	●	●	●	●		Iso
22	De opslag van reservekopieën bevindt zich op een andere fysieke locatie dan de opslag van de gekopieerde omgeving.	Reservekopieën (back-ups)	○	○	○	○	○	
23	Reservekopieën dragen dezelfde *Rubricering* als het origineel.	Reservekopieën (back-ups)	●	●	●	●		
24	Er zijn niet meer reservekopieën dan strikt noodzakelijk.	Reservekopieën (back-ups)	●	●	●	●		
25	De hoogste *Rubricering* en *Merking vanInformatie* dient te worden vermeld: - op verwisselbare gegevensdragers en omslagen; - boven en onderaan afgedrukte *TBB;* - daar waar het vermelden van de *Rubricering* met het oog op het trekken van ongewenste aandacht niet wenselijk is, dient een alternatieve behandeling te worden gekozen, bijvoorbeeld door te werken met een nader met *BZ*te bespreken (kleur)code.	Merking	●	●	●	●		

6.6	*Cloud computing* en *Virtualisatie*	Specificatie	*TBB 1 / ZG*	*TBB 2 /G*	*TBB 3 / C*	*TBB 4 / DV*	*Open*	Norm
1	Het gebruik van *Cloud*-diensten (computing, opslag, transport) is niet toegestaan.	Cloud-diensten	●	●	●			
2	Een *Cloud*-dienst wordt conform *ABBO* 2018 beschouwd als dienst waarbij dataopslag en verwerking door een derde partij wordt aangeboden en gebruik is gemaakt van Internet als medium tussen de gebruiker en aanbieder en is uitsluitend toegestaan in overleg met *BZ*.	Cloud-diensten				○		
3	Wanneer een *Opdrachtnemer* van een *Cloud*-dienst gebruik maakt om een *TBB* te verwerken of op te slaan, is de *Cloud*-dienstaanbieder en mogelijk ook de aanbieder van de verbinding over Internet naar de *Cloud*-dienst als *Subcontractor* door BZ ingeschakeld. Op de *Cloud*-dienstaanbieder, de gebruikte applicatie-omgeving, de gebruikte systemen en de infrastructuur zijn de bepalingen in de *ABBO* 2018 van toepassing.	Cloud-diensten				○		
4	Dataopslag, transport en verwerking in *Cloud*-omgevingen vindt plaats op Nederlands grondgebied. Gebruik van *Cloud*-omgevingen in het buitenland voor (delen van) opslag- of verwerkings- of transportdiensten vindt slechts plaats na goedkeuring door *BZ*.	Cloud-diensten				●	○	
5	Bij *Virtualisatie* gelden de volgende minimale eisen t.a.v. de installatie van de omgeving: - 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; - tijdsynchronisatie tussen hosts en VM's vindt plaats;	Virtualisatie	○	○	○	○		

	- 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 test omgevingen voor VM's zijn gescheiden; - er is een firewall geplaatst en geactiveerd om de host te beschermen; - er zijn slechts de noodzakelijke programma's en services geïnstalleerd op de VM's; - gast OS's dienen regelmatig gepatcht te worden; - het gast OS is beschermd door een firewall op het host OS.						○	
6	De volgende maatregelen moeten in ieder geval getroffen zijn 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 loggen van 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.	Virtualisatie	○	○	○	○	○	
7	Om herleidbaarheid naar individuele gebruikers en systeemfuncties te kunnen realiseren, dient het volgende gerealiseerd te zijn: - geen enkele administrator mag inloggen onder 'administrator' of 'root'. Administrators moeten inloggen onder een persoonlijk toegewezen account;	herleidbaarheid	○	○	○	○		

	- 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 “passwords” voor 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.							
6.7	***BYOD / CYOD***		***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3 / C***	***TBB 4 / DV***	***Open***	**Norm**
1	Mobiele devices in het kader van *BYOD* of *CYOD* zijn niet toegestaan.	byod/Cyod	●	●	●			
2	Mobiele devices in het kader van *BYOD* of *CYOD* zijn slechts na goedkeuring van *BZ* toegestaan .	byod/Cyod				●		ISO
3	Basis principes voor Mobile devices (*BYOD/CYOD*) zijn toegepast: - opslag, verwerking en transport van data vindt plaats op basis van gelijke condities gesteld aan *DV* netwerken; - geen lokale opslag van data, tenzij versleuteling is toegepast; - beheer vallende onder *ABBO 2018* bepalingen.	byod/Cyod				○		ISO
6.8	***Vercijfering***	**Specificatie**	***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3 / C***	***TBB 4 / DV***	***Open***	**Norm**
1	Een *TBB* is *Vercijferd* opgeslagen met door *NBV* of *BZ* toegestane versleuteling.	vercijfering	●	●	●	●		

2	Het sleutelbeheer is vastgelegd en dient te zijn geaccordeerd door *BZ*.	Sleutelbeheer	●	●	●	●		
3	*PKI* is niet toegestaan.	PKI	●	●	●			
4	*PKI* is toegestaan. Voor gebruik is de *PKI* architectuur beoordeeld door *BZ*. *CA/RA* zijn in eigen beheer of ondergebracht bij een door *BZ* goedgekeurde "*Escrow*".	escrow				○		
5	Ontsluiting van *TBB* op een netwerk tussen verschillende bedrijfslocaties (*WAN*) is niet toegestaan.	ontsluiting	●	●				
6	Ontsluiting van *TBB* op een netwerk tussen verschillende bedrijfslocaties (*WAN*) is alleen toegestaan indien de verbinding tussen de locaties van een door *BZ* goedgekeurde *Vercijfering* is voorzien.	vercijfering			○	○		
6.9	**Communicatie en netwerkbeveiliging**	**Specificatie**	***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3 / C***	***TBB 4 / DV***	***Open***	**Norm**
1	Er vindt geen (inter)netwerkverkeer plaats. Het normbeeld blijft altijd hetzelfde.	(inter)netwerkverkeer	●	●	●			
2	Bij het ontwerpen en implementeren van netwerken zijn maatregelen genomen om digitale dreigingen te onderkennen en af te weren.	netwerken	●	●	●	●		
3	Het gebruik van wireless (waaronder Satelite, LTE, 1-5G, GSM, RF) communication is niet toegestaan.	netwerken	●	●	●			
4	Het gebruik van wireless (waaronder Satelite, LTE, 1-5G, GSM, RF) communication is toegestaan na toestemming van BZ	netwerken				○		
5	Het gebruik van wireless toegang tot netwerken wordt voortdurend gemonitord en er zijn maatregelen getroffen die besmetting met *Malware* tegengaan (Firewall / IDS / IPS).	netwerken				●		
6	VLAN is zonder toestemming van BZ niet toegestaan.	VLAN	●	●				

7	VLAN is toegestaan in netwerken met een gelijke *Rubricering.* Er dienen voldoende maatregelen getroffen te zijn om "VLAN hopping" tegen te gaan. Per project kan een VLAN ingericht zijn.	VLAN			●	●		
8	Netwerken mogen niet verbonden zijn met lager *Gerubriceerde* netwerken.	netwerken	●	●	●			
9	Alle "devices" die gebruikt zijn om te koppelen aan een *TBB* vallen onder het beheer van de *Opdrachtnemer*, evenals de configuratie, geïnstalleerde software en aangebrachte patches.	devices				○		
10	Koppelingen met het Buitenlandse Zaken netwerken voldoen aan bepalingen die met *BZ* besproken zijn. De volgende aspecten zijn vastgelegd: - generieke beschrijving van de koppeling (keten, functionaliteiten, wederzijdse partijen, beveiliging); - netwerkdiagram, beschrijving datastromen en koppelvlakken; - eisen waaraan koppeling dient te voldoen, inclusief implementatiewijze en implementatiestatus; - beschrijving overige relevante punten.	netwerken	○	○	○	●		
11	Er zijn geen externe koppelingen naar andere netwerken.	netwerken	●	●	●			
12	De *BF* heeft inzicht in alle externe koppelingen naar andere netwerken: - daar waar externe partijen toegang verkrijgen tot interne of in een *DMZ* omgeving te raadplegen *Informatie*; - externe koppelingen zijn in de configuratieschets meegenomen;	netwerken				●		

	- indien externe partijen remote toegang nodig hebben tot digitale *TBB* is vooraf toestemming gevraagd aan *BZ*.							
13	*Blacklisting* wordt niet toegepast.	Blacklisting	●	●	●			
14	*Blacklisting* is toegepast voor bekende "malicious" IP-adressen.	Blacklisting				○		
15	Er is een netwerk "based" IDS of IPS monitoring toegepast. Waar mogelijk, is gewerkt met een *DMZ* (*DV*) voor systemen die internet koppeling nodig hebben.	Monitoring				○		
16	Netwerk "based" IPS zijn voorzien van bekende "*Signatures*" of gedrag dat complementair is aan geïmplementeerde IDS.	Signatures				○		
17	Ontwerp en implementeer netwerk perimeters zodat uitgaand web-, *File Transfer Protocol* (*FTP*) en *Secure Shell Verkeer* gecontroleerd is door ten minste één proxy in een *DMZ*. De proxy logt individueel TCP sessies, blokt specifieke URL's, domeinnamen en IP adressen conform de *Blacklist*.	FTP				○		
18	Uitgaand HTTP (S) verkeer verloopt via een proxy of er *vindt Network Adress Translation (NAT)* plaats voor IPv4. Als er gebruik gemaakt is van IPv6 verloopt het verkeer via een proxy.	NAT				○		
19	Er is gebruik gemaakt van *Two-factor-authentication* login, ook als gebruik gemaakt is van VPN, dial-up en andere vormen van toegang tot gerubriceerde omgevingen.	Two-factor-authentication				○		
20	Er is geen (inter)netverkeer.	Internetverkeer	●	●	●			
21	Blokkeer al het TOR (The Onion Router)/*Darknet* verkeer.	TOR				●		

22	Het is niet toegestaan om Darknet webbrowsers te gebruiken.	darknet				●		
6.10	**Systeem en software ontwikkeling**	**Specificatie**	***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3/ C***	***TBB 4 / DV***	***Open***	**Norm**
1	Acceptatie van systemen/software vindt pas plaats nadat vastgesteld is dat de *ABBO* 2018 beveiligingsmaatregelen daadwerkelijk zijn geïmplementeerd.	Software acceptatie	●	●	●	●		
2	De software ontwikkelaars zijn getraind op het implementeren van security in de software lifecycle. Er dient gebruik gemaakt te worden van secure software ontwikkeling methodieken (*Security by Design*).	Security by Design	○	○	○	○		
3	Er dient een softwarebibliotheek te worden bijgehouden.	Systeembeheer	○	○	○	○		
4	Beveiliging ten aanzien van systeemdocumentatie is gelijk aan de *Rubricering* van het betreffende systeem.	Operations & Maintenance	○	○	○			
5	Systeemhulpmiddelen zijn niet toegankelijk voor een standaard gebruiker.	Operations & Maintenance	○	○	○			
6	In een ontwikkel-, test- en acceptatieomgeving moet worden voorkomen dat met een *TBB* wordt gewerkt. Indien in een dergelijke omgeving toch een *TBB* wordt verwerkt zonder goedkeuring van *BZ* dan dient dit als een CAT1 security incident gemeld te worden.	Operations & Maintenance	●	●	●	●		
7	Code security review en testen zijn uitgevoerd door hiertoe opgeleid en gescreend personeel. Verificatie door *B Z*van in dit kader uitgevoerde activiteiten dient te kunnen plaatsvinden.	testen	○	○	○	○		
8	Standaard wachtwoorden van apparatuur en componenten - zoals: applicaties, operating systems, routers, firewalls, wireless access points en andere componenten in netwerken - zijn vóór ingebruikname vervangen door wachtwoorden conform de beheerprotocollen.	wachtwoorden	●	●	●	●		

9	Er zijn maatregelen getroffen die het gebruik van geheime communicatiekanalen (*covert channel*) en *Malware* in code tegengaan.	malware	○	○	○	○		
10	Te ontwerpen websites dienen veilig te zijn. Zo dient een secure handling van sessies plaats te vinden en dienen bijv. risico's op SQL-injectie en *Cross-site scripting* te worden voorkomen.	SQL	○	○	○	○		
11	Er vindt secure handling van sessies plaats binnen web applicaties. Dit kan inhouden dat gebruik gemaakt is van online mechanismen zoals: cookies en *Encryptie*. Beschouw hiertoe de Open Web Application Security Project (OWASP) richtlijnen.	OWASP	○	○	○	○		
6.11	**Vernietiging van gegevensdragers**		***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3/ C***	***TBB 4 / DV***	***Open***	**Norm**
1	Als een Buitenlandse Zaken project is beëindigd of niet langer benodigd, worden het project en het gebruikte systeem ontbonden en alle gerelateerde toegangen tot het *TBB* verbroken. Alle *TBB'n* zijn teruggegeven aan BZ	Disposal	○	○	○	○		Arbit (artikel 30) + Iso
2	Afvoer van media vindt plaats door fysieke vernietiging van informatiedrager in eigen beheer of door *BZ*. Een proces-verbaal van vernietiging is opgesteld.	Disposal	●	●	●			
3	Het wissen van *TBB* van media is alleen toegestaan in eigen beheer en indien gebruik is gemaakt van door *BZ* of *NBV* goedgekeurde middelen. Een proces-verbaal van vernietiging is opgesteld.	Disposal				●		
6.12	***Hardening* Systemen & Applicaties**		***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3/ C***	***TBB 4 / DV***	***Open***	**Norm**
1	Op apparatuur die ingezet wordt voor de opslag, verwerking en distributie van een *TBB* is tenminste de door de fabrikant voorgeschreven *Hardening* toegepast.	Hardening Systemen & Applicaties	●	●	●	●		

2	Alleen applicaties die door applicatiebeheer op een systeem geplaatst zijn, mogen gebruikt worden. Alle andere applicaties zijn verwijderd.	Hardening Systemen & Applicaties	●	●	●	●		
3	Dataoverdracht van en naar een *TBB* omgeving mag pas plaatsvinden nadat is zeker gesteld dat over te dragen data geen *Malware* bevat. Inzet van een *Scrubber* is hiertoe noodzakelijk.	Hardening Systemen & Applicaties	○	○	○			
4	In de *Cyber* beveiligingsorganisatie houdt zich minimaal één medewerker bezig met bestaande en de ontwikkeling van nieuwe technische kwetsbaarheden en dreigingen van de gebruikte soft- en hardware. Daar waar relevant adviseert deze medewerker over passende tegenmaatregelen.	Hardening Systemen & Applicaties	○	○	○			
5	Ongebruikte services (Windows), processen (Unix) of applicaties zijn van het systeem verwijderd.	Hardening Systemen & Applicaties	●	●	●			
6	Netwerken zijn gesegmenteerd teneinde de verspreiding van kwaadaardige software te voorkomen.	Hardening Systemen & Applicaties	○	○	○	○		
7	Er is gebruik gemaakt van automatische *Identificatie* van werkstations.	Hardening Systemen & Applicaties	○	○	○	○		
8	Alle fysieke verbindingen van en naar servers en hosts zijn afgesloten. Deze worden slechts bij een beperkt aantal accounts opengesteld (geen USB poorten open, geen CD-/DVD-roms of andere in/of uitvoerapparaten).	Hardening Systemen & Applicaties	●	●	●			
9	Nieuwe “devices” met een vaste of draadloze verbindingsmogelijkheid zijn niet toegestaan zonder toestemming van *BZ*.	Hardening Systemen & Applicaties	●	●	●			
10	Nieuwe “devices” met een vaste of draadloze verbindingsmogelijkheid zijn toegestaan na overleg met *BZ*.	Hardening Systemen & Applicaties				○		

10	Industrial Control Systems (ICS), al dan niet bevattende een *TBB,* mogen niet zonder toestemming van *BZ* gekoppeld worden aan een (andere) *TBB* omgeving. Denk hierbij aan beheerinrichting voor aircosystemen, een brandmeldinstallatie, toegangscontrolesysteem of de aansturing van een fabricageproces.	Hardening Systemen & Applicaties	●	●	●	●		
6.13	***TEMPEST***	**specificatie**	***TBB 1 / ZG***	***TBB 2 /G***	***TBB 3/ C***	***TBB 4 / DV***	***Open***	**Norm**
1	Wanneer een bedrijf in opdracht van Buitenlandse Zaken een dienst of product levert waardoor het in aanraking komt met *Bijzondere Informatie* zijn *TEMPEST* maatregelen van toepassing. Dat betekent dat onder leiding van *BZ* het stappenplan uit de bijlage *TEMPEST* moet worden doorlopen.	Enkel toepasbaar op STG gerubriceerde informatie.	●	●	●			
2	Aan de hand van de 'zone meting' is in overleg met *BZ* een keuze gemaakt uit de set beveiligingsmaatregelen, zodat aan de norm in de bijlage *TEMPEST* is voldaan.	Enkel toepasbaar op STG gerubriceerde informatie.	●	●	●			

Bijlage 1 - Rubriceren

Handleiding rubriceren ministerie van Buitenlandse Zaken

http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/dgobr/organisatie___interdepartementaal_/documenten_70/ibr/Handleiding_rubricering_v28-09-2015.pdf

Bijlage 2 - Risicolanden

U dient alle reizen te vermelden naar:

- landen waar een gewapend conflict bestaat of ten tijde van uw bezoek bestond;

- landen die zijn aangewezen bij Ministerieel Besluit het ministerie van Defensie waarin het verblijf een bijzonder risico voor de nationale veiligheid kan opleveren, te weten: Afghanistan, Irak, Iran, Noord-Korea, Pakistan, Turkmenistan en Wit-Rusland;

- de voormalige GOS-landen: Armenië, Azerbeidzjan, Georgië, Kazachstan, Kirgizië, Moldavië, Oekraïne, Oezbekistan, Rusland en Tadzjikistan

- De Volksrepubliek China

Bijlage 3 – Terminologie van veelgebruikte namen, termen en afkortingen

ABBO
Algemene Beveiligingseisen voor Buitenlandse Zaken opdrachten. 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 Persistant Threat. Een langdurige, complexe en doelgerichte digitale aanval met spionage als doel.

Attributie
Het toeschrijven van een geconstateerd effect (*Compromittatie*) aan een actor.

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.

Beveiligen
Het beschermen van een *TBB*, *BI* in het bijzonder, tegen toegang of kennisname door niet-gerechtigden.

BF
Beveiligingsfunctionaris. De functionaris die is belast met de implementatie en uitvoering van de voorgeschreven beveiligingsmaatregelen.

Beveiligingsverdrag
Een bilateraal verdrag dat de uitwisseling en wederzijdse bescherming van gerubriceerde *informatie* tussen twee landen faciliteert.

BI
Bijzondere Informatie is informatie die voorzien is van een *Rubricering* en op grond daarvan moet worden beveiligd.

BO
Bijzondere Opdracht. Een opdracht vanuit de overheid als *Opdrachtgever* aan een civiele partij als *Opdrachtnemer* waarbij een *TBB* betrokken is.

Blacklisting
Een zwarte lijst met bijvoorbeeld domeinen of *IP adressen* waarmee geen digitale communicatie mag plaatsvinden.

Broncode

Een computerprogramma in leesbare vorm zoals die door de programmeur in een programmeertaal is geschreven.

BYOD/ CYOD
Bring Your Own Device. De mogelijkheid voor een medewerker eigen apparatuur te gebruiken voor zakelijke toepassing.
Choose Your Own Device. De mogelijkheid voor een medewerker te kiezen uit een aantal door het bedrijf aangeboden apparaten.

BZ
Het Ministerie van Buitenlandse Zaken

CA/RA
Certificaat Autoriteit. De CA waarborgt de integriteit en authenticiteit van certificaten en garandeert de identiteit van de certificaatbezitter.
Registratie Autoriteit.De*RA* stelt vast aan wie een certificaat kan worden verstrekt en controleert de uitgifte ervan.

Categoriemanagement
Een overheidsbreed systeem van verwerven waarbij één ministerie t.b.v. de gehele *Rijksoverheid* goederen en diensten inkoopt.

CCTV
Closed Circuit Television. Een gesloten systeem van camera's als hulpmiddel bij het voorkomen en verwerken van incidenten.

CISSP
Certified Information Systems Security Professional. Kennisstandaard voor digitale beveiliging.

Cloud computing
Het via een netwerk op internet, op aanvraag beschikbaar stellen van hardware, software en gegevens.

Code security review
Software die ondersteunt bij het vinden van fouten in de broncode van software.

Command en Control (C2) server
Infrastructuur (servers en andere componenten), als doelwit gebruikt om M*alware* aan te verspreiden en/of deze aan te sturen, in het bijzonder botnets of *APT*'s.

Cookies
Een hoeveelheid data die een server naar de browser stuurt met de bedoeling dat deze opgeslagen wordt en bij een volgend bezoek weer naar de server teruggestuurd wordt. Zo kan de server de browser opnieuw herkennen en bijhouden wat de gebruiker, c.q. de webbrowser, in het verleden heeft gedaan.

Compartimentering
Het aanwijzen en *Beveiligen* van gewoonlijk afgescheiden fysieke dan wel digitale locaties waar een *TBB* mag worden verwerkt of opgeslagen, alsmede het aanwijzen van (groepen van) personen die toegang mogen hebben tot of kennis mogen nemen van een *TBB*.

Compromittatie

De ongeautoriseerde toegang tot of kennisname van een *TBB*, meestal *BI*.

COTS
Commercial of the Shelf. Een term om commerciële goederen en diensten aan te duiden die direct op de markt beschikbaar zijn.

Cross-site scripting
Een fout in de beveiliging van een web applicatie waarbij ontvangen invoer (zoals cookie, url, request parameters) door onjuiste verwerking in de uitvoer terechtkomt. Hierdoor kan een kwaadaardige code (JavaScript, VBScript, ActiveX, HTML, Flash etc.) geïnjecteerd worden.

Cryptofunctie
Een vertrouwensfunctie waarin behandeling van of kennisname van CRYPTO, CRYPTO-SECURITY of CRYPTO CONTROLLED ITEM (CCI)-gemerkt materiaal noodzakelijk is.

CUI
Controlled Unclassified Information / *Item*. Een categorie informatie of goederen die in het kader van de Amerikaanse *ITAR*, hoewel ongerubriceerd, een zekere mate van beveiliging vereist.

Cyber
Een term om het digitale domein in en om het internet aan te duiden. Vaak als voorvoegsel gebruikt voor nadere specificering van begrippen (cybercrime, cybersecurity, cyberdreiging).

Darknet
Deel van het World Wide Web waarvan de inhoud alleen met behulp van specifieke software (browser) en/of configuraties toegankelijk is.

Datacenter
Een instantie die digitale diensten levert op het gebied van supercomputers, netwerken en dataopslag of -verwerking op basis van hoogwaardige virtualisatie van systemen.

BZ BB
Het *BZ Beveiligingsbeleid*

Buitenlandse Zaken opdracht
Een overeenkomst tussen (de Staat der Nederlanden ten behoeve van) het Ministerie van Buitenlandse Zaken enerzijds en een natuurlijke of rechtspersoon anderzijds, waarbij overdracht of behandeling van *Informatie*, *Materieel*, *Goederen* of objecten plaatsvindt.

DMZ
Demilitarised zone. Een fysiek of logisch deel van het netwerk dat de extern, vanuit het Internet te benaderen services van een organisatie bevat, zonder dat de interne services en werkstations rechtstreeks te benaderen zijn (bijvoorbeeld mail- en webservers).

DV
Departementaal Vertrouwelijke Informatie is *Bijzondere Informatie* met de laagst mogelijke rubricering. *DV* wordt niet als Staatsgeheim aangemerkt maar behoeft wel een bepaald niveau van beveiliging.

Detectiesoftware

Software die in staat is *Malware* en/of een aanvaller te detecteren op basis van signaturen, anomalieën of gedrag.

Diagnosepoort
Een fysieke poort op een actieve component (router of switch) die het mogelijk maakt diagnose op een apparaat of netwerkverkeer te verrichten.

Dienstverlener (service provider)
Een bedrijf dat diensten aanbiedt. De term service provider wordt vaak geassocieerd met internet- en telefoniediensten.

Digitale code sign-in voor binaries
Een cryptografische techniek waarmee de integriteit en authenticiteit van programmatuur kan worden gewaarborgd.

Disclosure
De ontsluiting van een *TBB* waardoor dit ter beschikking of ter kennis wordt gesteld aan derden.

DoS/DDoS
Denial of Service. Het onbruikbaar maken van een computer, computernetwerk of dienst door overbelasting van de bandbreedte, geheugen- of verwerkingscapaciteit.
Distributed Denial of Service. De *DoS* aanval wordt vanaf meerdere computers tegelijkertijd uitgevoerd.

Document
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.).

Dual-homed hosts
Een ethernet apparaat dat meer dan één netwerkkaart bevat voor redundante functies, of, in firewall technologie, een firewall architectuur voor preventieve beveiligingsmaatregelen.

Encryptie
Zie *Vercijfering*.

Escrow Agent
Een betrouwbare derde partij waar sleutels of *Broncode* zijn opgeslagen.

ETS
Elektronisch Toegangbeheer Systeem.

EU
Europese Unie.

Executable
De vanuit de *Broncode* gegenereerde code die voor een computer uitvoerbaar is.

FTP
File Transfer Protocol.Een protocol dat uitwisseling van bestanden tussen computers faciliteert.

Forensisch goedgekeurde verwijdering

Het op bit niveau verwijderen van data, zodat alle replicatie van data onmogelijk is.

Geheimhoudingsverklaring
De verklaring waarin men aangeeft bekend te zijn met voorschriften en verplichtingen aangaande het omgaan met een *TBB*, *BI* in het bijzonder.

Goederen
Alle materiële en immateriële zaken (producten en diensten) die kunnen worden gebruikt om in behoeften te voorzien.

Hardening
Het proces van systeembeveiliging door verkleining van de aanvalsmogelijkheden in een systeem. Dit wordt o.a. gerealiseerd door slechts de benodigde functionaliteiten in een systeem te implementeren en de niet benodigde soft- en hardware te verwijderen.

Honeypot of honeynet
Een computersysteem of -netwerk dat zich bewust kwetsbaar opstelt voor (worm)virussen en andere aanvallen, zodat de aanvaller en/of zijn eigenschappen zichtbaar worden.

Hypervisor
Een opstelling (software) die ertoe dient om meerdere besturingssystemen tegelijkertijd op een hostcomputer te laten draaien.

Identificatie
Het kenbaar maken van de identiteit van een subject (een gebruiker of een proces).

IDSS
Indringer Detectie en Signalering Systeem.

Informatie
Kennis die in welke vorm dan ook overdraagbaar is. Hieronder worden zowel *Documenten* verstaan als materieel waarin kennis opgeslagen kan worden c.q. waaruit kennis af te leiden valt.

Informatiebeveiliging
Dat gedeelte van de beveiliging dat betrekking heeft op de verwerking van *Bijzondere Informatie* in ICT-systemen en netwerken.

IP adres
Internet Protocol adres. Een numeriek label aangebracht op een apparaat (bv. computer, printer) dat deel uitmaakt van een netwerk dat het *Internet Protocol* gebruikt voor communicatie.

IRP
Incident Response Procedure. Een procedure waarin is opgenomen welke stappen in onderzoek en afhandeling moeten worden uitgevoerd als een Incident wordt gemeld.

ITAR
International Traffic of Arms Regulations.

Interventietijd
De tijd tussen detectie/verificatie van een poging tot inbraak en het ter plaatse ingrijpen door de bewaking, politie of BZ personeel.

Introspectieve capaciteit

Het vermogen van een *IDS*om de interne activiteiten van een systeem (netwerk) op legitimiteit te beoordelen en zonodig actie te ondernemen.

Invoer- en uitvoervalidatie
Validatie van invoer of uitvoer door gebruikers aan de hand van verwachte waarden teneinde aanvallen die kunnen leiden tot verstoringen en onverwachte resultaten te voorkomen.

Leverancier
Een bedrijf dat goederen of diensten levert in ruil voor geld.

Logging
Het vastleggen van gegevens die betrekking hebben op (pogingen tot) de toegang (zowel fysiek als digitaal) tot een *TBB*.

LvV
Lijst van Vertrouwensfuncties. Het overzicht van aantallen *Vertrouwensfuncties* ingedeeld naar functiecategorie en *Veiligheidsmachtigingsniveau*.

Malware
Software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.

MAN/WAN
*Metropolitan Area Network / 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.

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.

Nationaal Detectie Netwerk
Een samenwerkingsverband vanuit de overheid voor het beter en sneller waarnemen van digitale dreigingen. Door het delen van dreigingsinformatie kunnen deelnemende partijen vanuit de eigen verantwoordelijkheid tijdig gepaste maatregelen nemen om mogelijke schade te beperken of te voorkomen.

NAT

Netwerk Adres Translatie is een verzamelnaam voor technieken die gebruikt worden ter afscherming van private *IP-adressen* voor de buitenstaander voor wie dan alleen het enkele publiek bekende *IP-adres* zichtbaar is.

NAVO
Noord Atlantische Verdrags Organisatie.

NBV
Het *Nationaal Bureau Verbindingsbeveiliging* voorziet de Rijksoverheid van voornamelijk technische middelen (*Cryptografie*) voor de beveiliging van *Bijzondere Informatie*.

Need-to-be
Een *Vertrouwensfunctionaris* heeft slechts fysieke toegang tot ruimten en locaties waar *Vitale* I*nformatie* 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 *VitaleInformatie* kennisnemen als dat nodig is om zijn werk te kunnen doen. Bovendien mag hij deze kennis niet met collega's delen voor wie deze kennis niet noodzakelijk is en/of geen vertrouwensfunctionaris zijn.

Netwerk perimeter devices
Apparaten die op het grensvlak van het vertrouwde netwerk zorgdragen voor beveiliging, toegang, verzending of ontvangst van data.

Netwerksegmentatie
Het opsplitsen van een netwerk in kleine coherente delen teneinde *Compromittatie* van grotere delen van een netwerk in één actie te bemoeilijken.

Objecten
Door de mens geproduceerd of gerealiseerd voorwerp, constructie, bouwwerk of kunstwerk (gebouw/brug/etc.).

Opdrachtnemer
Een natuurlijke persoon of een juridische entiteit (een rechtspersoon als bedoeld in boek 2van 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 *Buitenlande Zaken opdracht* wordt betrokken dan wel een *Buitenlandse Zaken opdracht* heeft ontvangen en aanvaard, alsmede derden nadat zij bij de uitvoering van een dergelijke opdracht zijn betrokken.

e-OPG (SvI)
(elektronische) Opgave Persoonlijke Gegevens (Staat van Inlichtingen) op basis waarvan een *Veiligheidsonderzoek* wordt uitgevoerd.

Packet headers
Data die aan het begin van een digitaal blok is geplaatst, benodigd voor interpretatie van de te transporteren data.

Penetratietest
Een toets op kwetsbaarheden van een of meerdere computersystemen met als doel de systemen beter te Beveiligen.

Phishing
Het trachten *Informatie* te ontfutselen aan mensen door hen te lokken naar een valse website, die een kopie is van een bekende, bestaande website. De aanvaller doet zich hierbij voor als een vertrouwde instantie of persoon, veelal via een e-mail met besmette files.

Proxies
Een computersysteem dat of applicatie die als een intermediair functioneert tussen verzoeken van werkstations en resources van servers.

PKI
PKI (*Public Key Infrastructure*) ondersteunt uitgifte en beheer van digitale certificaten. *PKI* geeft gebruikers extra garanties over via netwerken uitgewisselde *Informatie*. De garanties die een *PKI* verstrekt, zijn een grotere zekerheid betreffende verzender en ontvanger van de uitgewisselde *Informatie*.

PSC(C)
Personnel Security Clearance (Certificate). De verklaring dat een persoon is geautoriseerd tot toegang of kennisname van een *TBB*, *BI* in het bijzonder.

PSI
Project Security Instruction. Een *Document* waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van een buitenlandse opdracht.

Rijksdienst
De ministeries met hun directoraten-generaal, centrale en stafdirecties, buitendiensten en internverzelfstandigde dienstonderdelen.

Rijksoverheid
De Rijksoverheid, als onderdeel van de Nederlandse overheid, is de bestuurslaag op landelijk niveau en wordt gevormd door alle ministeries en de uitvoeringsorganisaties die onder de verantwoordelijkheid van een minister vallen.

Rubricering
Het vaststellen en aangeven dat een *TBBBijzondere Informatie* is of bevat, alsmede het bepalen en aangeven van de mate van beveiliging daarvan.

RAL
Rubriceringsaanduidingslijst. Een lijst die in het kader van een *BO* per onderwerp de rubricering van het daarop betrekking hebbende *TBB* aangeeft.

SAL
Security Aspect Letter. Een *Document* waarin nadere beveiligingseisen zijn vastgelegd, doorgaans in het kader van kleinere buitenlandse projecten.

Screening
Zie *Veiligheidsonderzoek*.

Scrubber
Een standalone systeem dat informatiedragers controleert op de aanwezigheid van *Malware* en deze zonodig onschadelijk maakt.

Secure Shell Verkeer
Een protocol dat het mogelijk maakt vercijferd in te loggen op een andere computer en op afstand commando's op de andere computer uit te voeren.

Security by Design
Een term die aangeeft dat reeds in de ontwerpfase van de software livecycle rekening wordt gehouden met het implementeren van beveiligingseisen en het voorkomen van kwetsbaarheden.

Security MoU
Memorandum of Understanding. Een bilaterale overeenkomst tussen partijen waarin wederzijdse beveiligingsafspraken zijn vastgelegd.

SG
De *Secretaris-generaal* van het betrokken ministerie.

Signatures
Eigenschappen van *Malware* op basis waarvan herkenning kan plaatsvinden.

Social Engineering
Het onder valse voorwendselen verzamelen van informatie uit communicatie waarbij wordt gebruikgemaakt van de intrinsieke motivatie van een ander behulpzaam te zijn, met het oogmerk toegang tot een *TBB*, *BI* in het bijzonder, te verkrijgen.

Staatsgeheim
Bijzondere Informatie waarvan de geheimhouding vanwege het belang van de Staat of zijnbondgenoten is geboden.

Subcontractor
Een bedrijf waaraan de *Opdrachtnemer* bepaalde werkzaamheden aan een *TBB* uitbesteed.

TBB
Te Beschermen Belang. Alle *Informatie*, *Materieel*, *Goederen* en objecten die een zekere mate van bescherming behoeven zijn door het ministerie van Buitenlandse Zaken ingedeeld in een viertal categorieën *Te Beschermen Belang* (TBB 1 tot en met TBB 4, waarbij TBB 1 de zwaarst te Beveiligen categorie is).

Toeleverancier
Een bedrijf dat goederen levert aan een ander bedrijf dat die *Goederen* op zijn beurt verwerkt in een door de eindgebruiker gewenst product.

TEMPEST
Het tegengaan van mogelijk compromitterende emissie van elektronische systemen die kan leiden tot het onbevoegd opvangen, verwerken en reproduceren van data.

Two-factor authentication
Op basis van twee factoren controleren of iemand daadwerkelijk is wie hij claimt te zijn. De factoren bestaan uit iets dat iemand weet, bezit of hem/haar kenmerkt.

Uitsteltijd
De tijd tussen detectie/verificatie van een inbraak en *Compromittatie* van een *TBB*.

Veiligheidsonderzoek

Het proces dat leidt tot afgifte, weigering, verlenging of intrekking van een *VGB*.

Vercijfering
Het door middel van een algoritme zodanig wijzigen van informatie dat deze onleesbaar en onbegrijpelijk is voor niet-gerechtigden.

Versleuteling
Zie *Vercijfering*.

Vertrouwensfunctie
Een functie die in beginsel de mogelijkheid biedt de veiligheid of andere gewichtige belangen van de Staat te schaden.

Veiligheidsbriefing
Een voorlichting met als doel het beveiligingsbewustzijn te vergroten.

VMN
Veiligheidsmachtigingsniveau. Het voor de *Vertrouwensfunctie* vereiste niveau waarop het *Veiligheidsonderzoek* moet worden uitgevoerd (A, B dan wel C).

VGB
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.

Virtualisatie
Het op een virtuele wijze creëren van een computersysteem in plaats van een combinatie van hard- en software. Hierbij werken computers, operating systemen, dataopslag systemen en andere actieve componenten virtueel samen.

VOG
Verklaring Omtrent Gedrag. Een verklaring van de Dienst Justis van het Ministerie van V&J benodigd voor toegang tot of kennisname van informatie op *DV*-niveau.

VPN
Virtual Private Network. Een vercijferde verbinding tussen twee systemen, waarbij de integriteit en de vertrouwelijkheid van de data gewaarborgd blijft.

Wateringholes
Een strategie waarbij een aanvaller een website infecteert met *Malware* na te hebben vastgesteld dat een bepaalde groep gebruikers die website regelmatig bezoekt.

Wet op de inlichtingen- en veiligheidsdiensten (Wiv)
De *Wet op de inlichtingen- en veiligheidsdiensten* zoals gepubliceerd 2002 (zie stb. 2002, 148)of de rechtsopvolger.

Wet veiligheidsonderzoeken (Wvo)
De *Wet veiligheidsonderzoeken* zoals gepubliceerd 1996 (zie stb. 1996, 525) en gewijzigd in 2015 (zie stb. 2015, 208).

Wetboek van strafrecht (Wvs)

Het wetboek van strafrecht waarin ondergebracht de Nederlandse strafwet die toepasselijk is op een ieder die zich in Nederland aan enig strafbaar feit schuldig maakt.

Zeggenschap
Onder “Zeggenschap” wordt verstaan de mogelijkheid op grond van feitelijke of juridische omstandigheden een invloed uit te oefenen op het beleid van een onderneming. Het hebben van relevante invloed op het beleid van een onderneming kan voortvloeien uit financiële,organisatorische en formele banden (benoemingsrechten, stemrechten op aandelen), directe dan wel indirecte banden (dochter- en zusterondernemingen), samenwerking in een groep of informele samenwerkingsverbanden.

Zero-day
Een (onbedoelde) kwetsbaarheid in software die nog onbekend is bij de softwareontwikkelaar en anderen. Een Zero-day-exploit is software die misbruik maakt van een dergelijke kwetsbaarheid in de software.