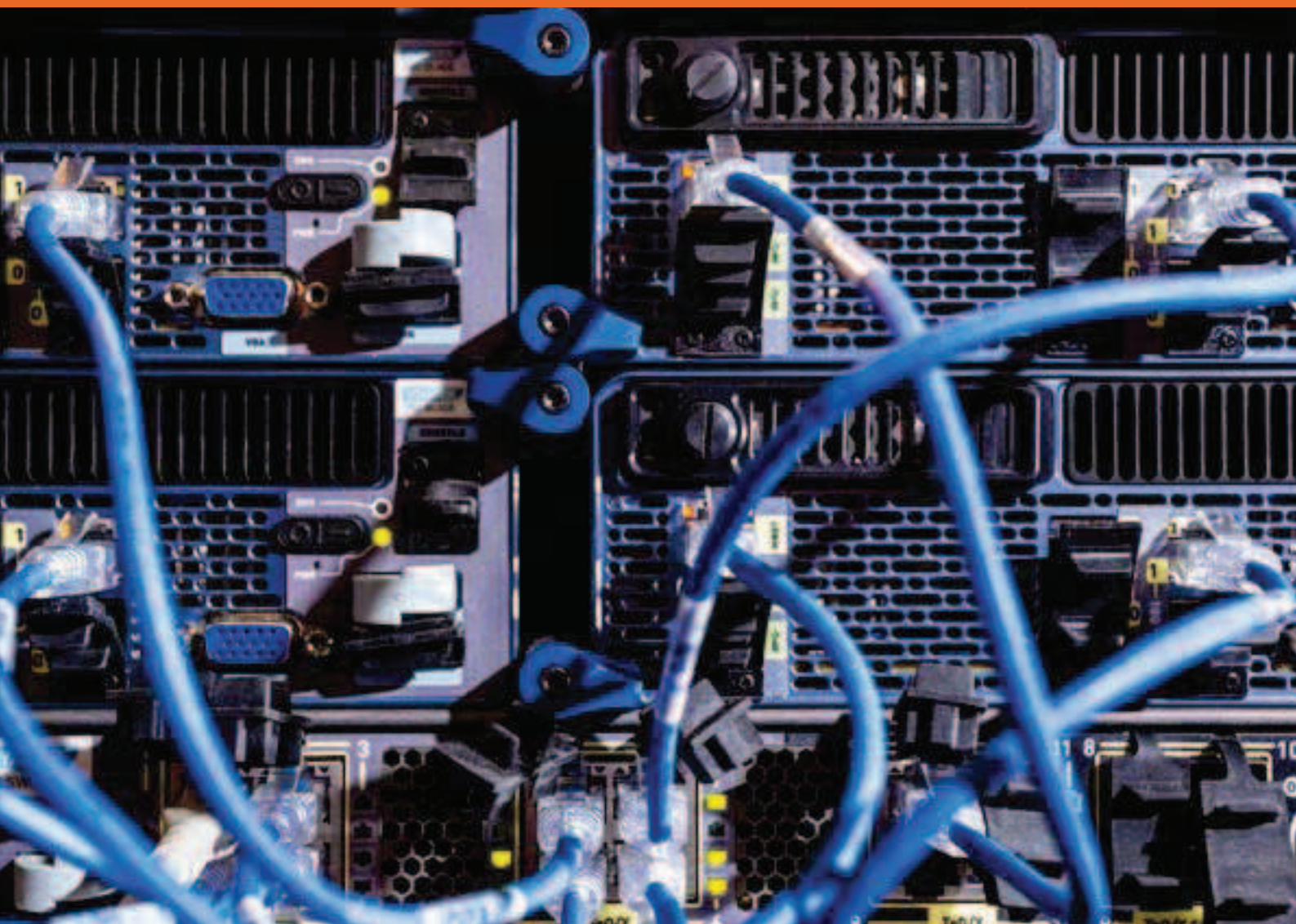
Ministry of Defence

ABDO

General Security Requirements for Defence Contracts



ABDO

General Security Requirements for Defence Contracts[1]

[1] This document is a translation of the original Dutch version of the document. The Minister of Defence cannot assume any responsibility for the accuracy or reliability of the translated version of this document and shall always refer to the original Dutch version of the document, nor shall this translation be construed as constituting any obligation on the part of the Minister of Defence.

Foreword

It regularly becomes clear that outsiders have great interest in the knowledge, information, materiel, goods and other objects of the Ministry of Defence, knowledge institutes and companies. Objectionable practices and covert means are not shunned in an attempt to lay hands on knowledge or gather information regarding these subjects. Proper security is therefore vital.

Your organization also has at its disposal valuable matters you do not want to yield to unauthorized persons. Unfortunately, not everyone is sufficiently aware of that. This, in combination with a (too) low level of security, makes an organization vulnerable. The security of knowledge, information, materiel and goods, as well as knowledge of the object used for production, processing and/or storage, therefore deserves the necessary attention.

Among others, the Civil Service Data Security - Special Information regulation (Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie; VIR) provides rules for the security of special information of the central government, in order to prevent the undesirable dissemination of, and unlawful access to, this information. It also describes how to act if a security incident occurs. For each ministry, these rules have been further detailed in security policy. For the Ministry of Defence, the security policy is the Defence Security Policy (Defensie Beveiligingsbeleid; DSP).

The scope of the Civil Service Data Security - Special Information regulation and other regulations is in principle restricted to the central government. It can however be necessary to release information, materiel, goods or even other objects – in other words an Interest to be Protected (IBP) – to parties outside of the Ministry of Defence, for example to an company that needs an IBP to execute a contract. This is only permitted if there is sufficient certainty that adequate security is guaranteed. This document is an overall revision of General Security Requirements for Defence Contracts (Algemene Beveiligingseisen voor Defensieopdrachten; ABDO), in other words ABDO 2019, which the Ministry of Defence imposes on organizations and companies with regard to the security of an IBP. The ABDO 2019 is derived from the aforementioned regulations, where necessary supplemented with new general security requirements and implementing provisions.

The ABDO 2019 replaces the ABDO 2017 and has been slightly amended in comparison. The ABDO 2019 thus satisfies the need of the Ministry of Defence for a modern regime of security requirements. The application thereof contributes to adequate security of not only the IBP handed over by the Ministry of Defence, but also companies' own 'crown jewels/intellectual property'.

The ABDO 2019 will come into effect on 1 November 2019.

On behalf of the Minister of Defence,

Acting Principal Director of Business Management/National Security Authority

W.S. Rietdijk
Brigadier General

Index

General

1 Interests to be protected

One must be able to count on the reliability (Availability, Integrity, Confidentiality) of personnel, Information, Materiel, Goods and Buildings under all circumstances. These are, however, constantly exposed to threats such as crime, extremism, sabotage, terrorism and espionage. Economic, strategic, military and technical scientific espionage form a real threat. Vital sectors such as the energy and telecommunication sectors could be hit by digital or physical extremist or terrorist attacks.

Security measures contribute to the resistance against these threats. The level of the measure depends on the nature of the Information, Materiel, Goods and Buildings in relation to the specific threat. The Ministry of Defence has a Classification and Marking system for this purpose. The Ministry of Defence has divided all Information, Materiel, Goods and Buildings to be protected into four categories of Interests to be Protected (IBP; with IBP 1 as the category to be Secured the most stringently).

2 ABDO risk management

The aim of risk management is to identify threats against an IBP, to identify the related risks and then to eliminate these risks or reduce them to an acceptable residual risk by means of security measures.

In this regard, risk is defined as the product of the likelihood that a threat will actually manifest and the effect thereof on the sustainability of the Ministry of Defence. In short, risk = likelihood x effect.

In order to establish the residual risk, the Ministry of Defence has allocated an IBP category to all Information, Materiel, Goods and Buildings on the basis of a risk analysis. Based on the reliability requirements set by the Ministry of Defence, the estimated threat, and a cost–benefit analysis, the ABDO 2019 includes a set of security measures for each IBP category, which is intended to prevent the operational processes of the Ministry of Defence from stagnating and the State or its allies from suffering unacceptable damage.

As the circumstances and threats are constantly subject to change, risk management is a cyclic process. Such changes can be reason to adjust the level of security. Depending on the company, the nature of the contract and the location, other combinations of measures may be necessary to meet the same level of security. For each situation, DISS/ISO indicates which requirements apply and which measures should be taken.

3 Special Information and Information that has a Marking

Information that has a Classification is referred to as Special Information (SI). SI is subdivided into State Secret and non-State Secret SI. State Secret applies if interests of the State or its allies are at stake and if cognizance by non-authorized persons could damage those interests. Non-State Secret SI applies if cognizance by non-authorized persons could disadvantage the interest of one or more ministries. Depending on the level of the Classification, SI is also allocated an IBP category.

The following table includes the four possible Classifications and the corresponding IBP category. Information that has one of these Classifications is referred to as SI. Note that unlike SI, an IBP is not necessary classified. A classified document is always an IBP, but an IBP is not always classified.[2]

NLD Classification	IBP category	Definition
Stg. ZEER GEHEIM (NLD TOP SECRET)	IBP 1	Cognizance by non-authorized persons could very seriously damage the interest of the State or its allies.
Stg. GEHEIM (NLD SECRET)	IBP 2	Cognizance by non-authorized persons could very seriously damage the interest of the State or its allies.
Stg. CONFIDENTIEEL (NLD CONFIDENTIAL)	IBP 3	Cognizance by non-authorized persons could damage the interest of the State or its allies.
DEPARTEMENTAAL VERTROUWELIJK (NLD RESTRICTED)	IBP 4	Cognizance by non-authorized persons could disadvantage the interest of one or more ministries.

[2] This distinction is relevant to Security Screening, because for unclassified IBP no Security Screening may take place. In this case a Certificate of Good Conduct is required.

Information may also have a Marking (whether or not in combination with a Classification). A Marking is intended to limit the set of persons authorized to take cognizance of the information to a specific group. The intention of a Marking may also be specific handling and security. Appendix 1 includes a table with the most common Markings and their definition, coupled to an IBP category. Unclassified Information of the Ministry of Defence that does have a Marking (such as Intern Gebruik Defensie, Intern Beraad, NLD-Eyes-Only) should be secured as IBP 4. Unclassified and unmarked information should be treated on the basis of "Need-to-Know".

A set of available Information that is sensitive to personnel (e.g. medical data, or information about the operational deploy ability of personnel) should be secured at least as IBP 4. If it concerns a large set of classified and/or marked Information, a (potentially higher) IBP may be allocated and IBP 4 may thus be exceeded. The damage resulting from the set being compromised is, after all, greater than from a single piece of information being compromised.

Information, Materiel, Goods and Buildings may also be of a Vital nature. An IBP category is allocated on this basis, even if a Classification or Marking does not apply. The incorrect implementation of the requirements set in the ABDO 2019 has a disadvantageous impact on the operations of the Ministry of Defence, the State and its allies, and results in damage to either the security of the state or other important interests of the State.

4 Special Contracts

Specific security requirements are set for the production, handling, processing, storage and destruction of an IBP. If it is necessary for the proper execution of a contract to hand over an IBP from the Ministry of Defence (the Commissioning Party) to a company (the Contractor), or if it is foreseen that the Contractor has or will generate an IBP itself, this is considered a Special Contract (SC). Transfer of an IBP can take place in several ways: orally, in writing, digitally, or in the form of Materiel. It must be ensured that the correct security regime is applied by the Contractor. In the case of an SC, the Contractor is contractually obligated to implement the security measures as described in the present document, the ABDO 2019.

5 Advice and inspection

According to The Netherlands Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017; Wiv 2017), Section 10, the Defence Intelligence and Security Service (DISS) is designated for the protection of IBPs of the Ministry of Defence which, if compromised, could damage the armed forces or allies. Within DISS, the Industrial Security Office (ISO) is responsible for inspecting the implementation of the required security-promoting measures by the Contractors in the context of an SC. To this end, DISS/ISO pays several visits to the Contractors, which are obligated to cooperate. The aim of the visit is:

- **engagement and authorization**: at the request of the procurement officer of the Ministry of Defence, DISS/ISO assesses whether a potential Contractor is willing and able to meet the ABDO 2019. If there is the intention to award the contract, an inspection of the implementation and adequacy of the security measures follows. In the event of a positive assessment, the procurement officer is authorized to award the contract. The company is thus authorized for IBP storage and processing. This authorization is awarded per contract and is therefore not a general authorization[3]. A detailed description of the procurement process is contained in the "ABDO procedure" guideline, see appendix 0;

- **advice**: DISS/ISO issues advice regarding the measures that must be implemented to meet the minimum security requirements of the ABDO 2019;

- **inspection**: DISS/ISO visits the Contractor, solicited or unsolicited, for an interim assessment of the implementation of the security measures and assesses whether the standards set have been met;

- **audit**: DISS/ISO performs a formal comprehensive audit announced in advance of the implementation and adequacy of the security measures. The results are recorded in an audit report that is adopted by the director of NLD DISS;

- **investigation**: following a report of a possible or actual Security Incident, DISS/ISO investigates the possible compromise of an IBP and the consequences thereof, with the aim to limit the damage and prevent repetition.

[3] A general or permanent authorization does not exist. A Facility Security Clearance Certificate (FSCC) is not a general or permanent ABDO authorization. A description of the procurement process is contained in the "ABDO procedure" guideline.

In the context of a NATO or EU SC, these organizations also carry out regular inspections. Contractors are also obligated to cooperate in this regard.

6 Access to Site

It is possible that employees of a Contractor who have not been appointed to a Confidential Position must be granted frequent access to locations, compartments or systems that contain IBPs that may or may not be classified. In these cases, the Ministry of Defence can nonetheless stipulate the ABDO 2019 and initiate the Screening of the employees involved.

7 Prohibited Place

High concentrations of State Secrets at a single location can be reason for the location to be designated as a Prohibited Place by Royal Decree. A Prohibited Place is secured at IBP level 1. Personnel who must have access (Need-to-be) must have a Security Clearance Level that corresponds to the highest level of Classification present.

8 Foreign contracts

Companies may also be considered for a NATO, EU or foreign government SC. In addition to national IBPs, NATO, EU or foreign IBPs may therefore also be relevant. For contracts related to the Ministry of Defence, DISS/ISO serves as the designated security authority for the company involved on behalf of these organizations and countries. In the case of civilian contracts, the General Intelligence and Security Service (GISS) fulfils this role. In that case it is often a condition that agreements are determined in a Security Covenant or a Memorandum of Understanding (MoU). DISS/ISO then has the role of Designated Security Authority (DSA).

9 International Classifications

The table in Appendix 2 includes the national Classifications in line with the NATO and EU Classifications, as well as the most common foreign national Classifications. For international use, the Netherlands Classifications can be extended to include the internationally more recognizable English classifications, such as NLD CONFIDENTIAL, in addition to Stg.CONFIDENTIEEL. See also Appendix 2 in this regard.

10 Export Control

If a contract involves Information, Materiel and/or Goods that are subject to the export control policy of the country of origin, separate or supplementary security requirements may be set. For example, in the context of a contract that involves Information, Materiel and/or Goods that fall under the US legislation for export control, such as the International Traffic of Arms Regulations (ITAR), separate security requirements are set. Information, Materiel and/or Goods of this kind usually fall into the category Controlled Unclassified Information/Item (CUI). In this case, agreements are often made by the company involved with the (foreign) Commissioning Party directly, in a Technical Assistance Agreement. The ABDO 2019 does not actually apply in this regard, but may be used as a guideline for the intended security regime if the contract is issued by the Ministry of Defence, the ABDO 2019 applies, at level IBP 4 as a minimum.

11 Patents

If an invention ensues from an SC and the Contractor is of the opinion that a patent application must be submitted for it, he must make this known to the Commissioning Party and DISS/ISO before applying. In view of the military nature, the patent application might be given a Classification (in accordance with Chapter 2, Part 3, Article 40 - 46 of the Netherlands Patents Act 1995 (Rijksoctrooiwet 1995). All SI related to the patent application must be secured in accordance with the ABDO 2019. The patent agent to which the classified patent application is submitted must also meet the ABDO 2019.

It is also possible for the Ministry of Defence to apply for the patent, for example, if the ownership of the intellectual property of the invention rests with the Ministry of Defence.

12 Escrow

If SI is filed with an Escrow Agent designated by the Ministry of Defence, this agent must also meet the ABDO 2019.

13 Regulatory framework

The ABDO 2019 is in part based on national and international regulatory framework, such as the NATO and EU regulations for the security of classified Information, the Netherlands Defence Security Policy (Defensiebeveiligingsbeleid; DSP), the Netherlands Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017), the Netherlands Security Screening Act (Wet veiligheidsonderzoeken), the Netherlands Protection of State Secrets Act (Wet bescherming staatsgeheimen) and the Netherlands Public Records Act 1995 (Archiefwet 1995).

14 Interim amendments to the requirements

Circumstances and threats are subject to constant change. Such change can be reason for the security level to be adjusted during the execution of the contract and for further requirements to be set. Further consultations should be held between the Commissioning Party and the Contractor regarding any consequences thereof (costs, terms).

15 Sanctions

The ABDO 2019 forms an integral part of the contract between the Commissioning Party and the Contractor. Non-compliance with the security requirements set in the ABDO 2019 is therefore considered breach of contract. This may result in the suspension or withdrawal of the authorization granted for IBP processing and storage, which may result in the termination of the contract. If the non-compliance can be traced back to a specific person, it may result in the withdrawal of that person's Certificate of No Objection (CNO). Upon termination of the contract, the IBP must be returned or destroyed. Intentionally withholding an IBP, disseminating an IBP to a non-authorized person, and making available an IBP to a non-authorized person are criminal offences in accordance with the provisions of the Netherlands Penal Code (Wetboek van strafrecht) (Sections 98, 98a, 98b, 98c, 272 and 273).

16 Transitional arrangements (ABDO 2017 to ABDO 2019)

The implementation of the ABDO 2019 means the ABDO 2017 is replaced in full. This means that for new contracts, sub-contracts, projects, subprojects and contracts under framework agreements, etc. to which the ABDO applies, ABDO refers to the ABDO 2019. The ABDO 2006 or the ABDO 2017 thus continues to apply to existing contracts.

17 ABDO 2019 versus ABDO 2017

The ABDO 2019 is an update of the ABDO 2017. In ABDO 2019 account has been taken of the numbering of the requirements, with previous duplicate numbering or new requirements that were difficult to fit with the existing numbering are numbered with .1 and further.

18 Citation of the ABDO 2019

These security requirements can be cited as the 'General Security Requirements for Defence Contracts 2019', abbreviated to ABDO 2019.

19 Reader's guide

The ABDO 2019 lists the requirements which need to be met for the security of an IBP. The degree to which the requirements are applied may vary based on a risk analysis. This could mean, for example, that a requirement is less strictly applied than stipulated. This is at the discretion of DISS/ISO.

The requirements cover four sub-areas: executive board and organization, personnel, physical and cyber. In the following chapters, the requirements are set out in a table per sub-area. These are explained in more detail or expanded on in the appendix where necessary. In the event of any conflict between a requirement in the table and the text in the introductory text or appendix, the requirement in the table prevails.

A filled-in circle (●) in the column under the highest applicable Classification or IBP category indicates which requirements apply. An empty circle (○) in this column means that it must be determined in consultation with DISS/ISO, whether or to what extent the requirement needs to be satisfied.

1 Executive Board and Organization

Introduction

Safeguarding an Interest to be Protected (IBP) starts with a widely supported and structurally enforced security policy which is endorsed by the highest executive body. Sound security is contingent on a security plan based on the security policy and on the implementation of comprehensive security measures. Security awareness is a factor of paramount importance: only when the whole organization, from top to bottom, is thoroughly aware of the importance of an IBP will it develop a company culture in which all personnel handle an IBP appropriately. This awareness must also encompass an understanding that Disclosure to third parties or publication of an IBP is prohibited.

This chapter pays particular attention to company structure, ownership and Control because these factors could negatively affect the company and thus the handling of an IBP. Such influence could also occur when SI is accessible to persons who only have non-Dutch nationality.

Furthermore, it is crucial for the entire logistical chain including Suppliers to be transparent when handling an SC. Undue influence on the service or product could be exerted through the supply of seemingly innocent components or parts.

Finally, this chapter deals with the handling of Security Incidents.

The executive board and the organization must also meet a number of security requirements, which are described in the table starting on the following page. These are explained in more detail or expanded on in the appendix where necessary. In the event of any conflict between a requirement in the table and the text in the introductory text or appendix, the requirement in the table prevails.

The ABDO 2019 lists the requirements which need to be met for the security of an IBP. The degree to which the requirements are applied may vary based on a risk analysis. This could mean, for example, that a requirement is less strictly applied than stipulated. This is at the discretion of DISS/ISO.

A filled-in circle (●) in the column under the highest applicable Classification or IBP category indicates which requirements apply. An empty circle (○) in this column means that it must be determined in consultation with DISS/ISO, whether or to what extent the requirement needs to be satisfied.

ABDO 2019 requirements						
CHAPTER 1 EXECUTIVE BOARD AND ORGANISATION			**SECURITY REGIME**			
1.1	**General**	**Reference**	**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The Contractor satisfies the ABDO 2019 requirements with regard to the Classified Contract in question.	Procedure ABDO	●	●	●	●
2	Upon expiry of the contract, all associated authorizations, Lists of Confidential Positions and Certificates of No Objection cease to be valid. Prior to this, the Contractor will return the IBP provided by the Commissioning Party unless the Commissioning Party, in consultation with DISS/ISO if applicable, has issued written consent to destroy or retain the IBP.	Procedure ABDO	●	●	●	●
1.2	**Setting up a security organization**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The Contractor pursues an integral security policy which describes organizational, personnel, physical (where necessary) and information security aspects relating to IBPs and which is endorsed by the highest executive body.	Appendix 3	●	●	●	●
2	The Contractor has a security plan drawn up by its SO, approved by DISS/ISO and signed by the highest executive body, describing the current security situation (on the basis of self-inspection) and detailing the ABDO security requirements in clear, manageable measures and procedures.	Appendix 3	●	●	●	●
3	The Contractor has unequivocally implemented in its organization the measures and procedures described in the security plan.	Appendix 3	●	●	●	●
3.1	The Contractor has implemented measures to enable the provision of a list of registered company resources in accordance with the appendix within 48 hours, at the request of DISS/ISO.	Appendix 27	●	●	●	●
4	The Contractor has, with prior written permission from DISS/ISO, appointed an SO and one or more Deputy SOs, depending on the size of the SC, and the number of locations and specializations involved.	Appendix 3	●	●	●	●
5	The SO has at least: - Dutch nationality, and is employed by the company in question; - sufficient autonomy, powers, leverage and seniority; - a Certificate of Good Conduct or a Certificate of No Objection for the highest applicable level of classification of the SC; - direct and independent access to all administrative bodies within the organization.	Appendix 4	●	●	●	●
6	All security measures are established in a layered structure to which the "Need-to-Be" principle applies.	Appendix 17 / 18	●	●	●	●
7	The “Need-to-Be” and “Need-to-Know” principles apply to all compiled measures.	Appendix 18	●	●	●	●
1.3	**The Security Officer**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The SO is tasked with the day-to-day implementation of security, supervision and periodic, i.e. at least once a year, self-inspections, the results of which are recorded in writing and reported to the Contractor’s executive board.	Appendix 4	●	●	●	●
2	The SO periodically, i.e. at least once a year, tests the security plan in practice, the results of which are recorded in writing and reported to the executive board with a copy to DISS/ISO. The security plan is updated if necessary.	Appendix 3 / 37	●	●	●	●
3	Policy and other changes which affect the company’s security policy are submitted to DISS/ISO for approval and incorporated into the security plan.	Appendix 4	●	●	●	●
4	Essential changes as the result of a raised threat level or a Security Incident are determined in the security plan by the SO within the deadline set by DISS/ISO.	Appendix 3 / 4	○	○	○	○
5	The SO ensures full cooperation during inspections, audits and investigations of the Contractor by DISS/ISO.	Appendix 4	●	●	●	●
6	The SO keeps up-to-date on matters pertaining to local security through contact with the municipal authorities, neighbouring companies and the police.	Appendix 4	●	●	●	○

7	The SO also carries out the duties as described in Appendix 4: Duties and responsibilities of the SO.	Appendix 4	●	●	●	●
1.4	**Control and company structure**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
A notification by the Contractor with regard to the requirements in 1.4 can give reason to formally submit it in writing to the DISS Director for review. This is at the discretion of DISS/ISO.						
1	The Contractor has drawn up Certificates of Propriety, Control and company structure and submitted them to DISS/ISO for the purpose of authorization.	Appendix 5	●	●	●	●
2	The Contractor reports to DISS/ISO in writing and without delay any proposed change in ownership/share ownership of the company.	Appendix 5	●	●	●	●
3	The Contractor reports to DISS/ISO in writing and without delay any proposed changes to Control, ownership and share ownership as a result of which this will fall largely or entirely into the hands of a sole natural person or legal entity or one or more foreign natural persons or legal entities.	Appendix 5	●	●	●	●
4	The Contractor reports to DISS/ISO in writing and without delay any proposed appointments to the executive board of persons who do not hold Dutch nationality.	Appendix 5	●	●	●	●
5	The Contractor reports to DISS/ISO in writing and without delay any proposed cooperation with foreign companies or governments.	Appendix 5	●	●	●	●
6	The Contractor reports to DISS/ISO in writing and without delay any proposed break-up, strategic partnership or merger, imminent partial or complete take- over, business cessation, suspension of payment or bankruptcy.	Appendix 5	●	●	●	●
7	The Contractor reports to DISS/ISO in writing and without delay any proposed changes to business activities, locations, sourcing, mergers or partial or complete takeovers.	Appendix 5	●	●	●	●
8	The Contractor provides clarity regarding the company/part of company by which and the location at which the SC will be carried out and does its utmost to ensure all SCs are placed with a single, clearly recognizable company/part of company that can be legally and organizationally shielded off.	Appendix 5	●	●	●	●
9	In the case of an SC in which large amounts of SI (to be determined by DISS/ISO in consultation with the Commissioning Party) are transferred, the Contractor is a Dutch legal entity.	Appendix 5	●	●	●	○
10	The Contractor guarantees that any large amounts of SI (to be determined by DISS/ISO in consultation with the Commissioning Party) are only generated, processed and stored on Dutch territory.	Appendix 5	●	●	●	●
11	The Contractor only appoints employees with Dutch nationality to Confidential Positions which require access to a large amount of SI (to be determined by DISS/ISO in consultation with the Commissioning Party).	Appendix 5	●	●	●	○
1.5	**Security awareness**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The Contractor implements a security awareness programme, in which participation is compulsory and measurable.	Appendix 6	●	●	●	●
2	The SO instructs employees tasked with carrying out an SC on ABDO 2019 procedures and their corresponding responsibilities on appointment to a Confidential Position, at the start of a new SC and subsequently periodically, i.e. at least once a year.	Appendix 6	●	●	●	●
3	If necessary, the SO advises and supervises on an individual basis employees who are tasked with an SC, who have foreign contacts or who are travelling to high-risk countries.	Appendix 6 / 16	●	●	●	●
1.6	**Security Classification Checklist / Project Security Instruction / Security Aspect Letter**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	A Security Classification Checklist (SCC) filled in by the Commissioning Party is on file for every SC.	Appendix 7	●	●	●	●
2	In the event that a foreign or Dutch SO makes specific additional security demands, a Project Security Instruction (PSI) or Security Aspect Letter (SAL) will be available.	Appendix 7	●	●	●	●
3	An EU and/or NATO IBP is only released to countries, organizations, or personnel involved in EU and/or NATO programmes, barring exceptions determined in advance.	Appendix 7	●	●	●	●

1.7	Logistical chain		IBP 1/ NLD TS	IBP 2/ NLD S	IBP 3/ NLD C	IBP 4/ NLD DV
1	The Contractor reports to DISS/ISO in advance any proposed outsourcing of work pertaining to an SC to domestic or foreign Subcontractors. This is at the discretion of DISS/ISO, which grants permission where possible.	Appendix 8	●	●	●	●
2	Once permission for outsourcing to the Subcontractor has been granted by DISS/ISO, the Contractor incorporates the ABDO 2019 in its contract with the Subcontractors coming into contact with an IBP. The Contractor submits to DISS/ISO a completed SCC in this regard.	Appendix 8	●	●	●	●
3	Once permission for outsourcing has been granted by DISS/ISO (on thebasis of a Facility Security Clearance submitted by the foreign Partner), theContractor incorporates the security requirements applicable in the countryin question in its contract with foreign Subcontractors coming into contactwith an IBP. A completed SCC is submitted to DISS/ISO in this regard.	Procedure ABDO	●	●	●	●
4	The Contractor stipulates the ABDO 2019 to its suppliers of system components requiring a certain degree of protection due to their critical/vital function.	Appendix 8	○	○	○	○
5	When companies work on an SC in partnership with other companies, any work on an IBP is centralized as far as is possible. (The Contractor bears responsibility for compliance with the requirements of the ABDO 2019 by any company it takes under its wing as a Subcontractor).	Appendix 8	●	●	●	●
6	The Contractor requests permission from DISS/ISO in advance for any plans to outsource work for an SC to a foreign Subcontractor. Outsourcing to a foreign company requires the permission of the Commissioning Party and authorization from DISS/ISO.	Appendix 8	●	●	●	●
1.8	**Press, internet, social media, publication, photographs, film footage**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The Contractor and its personnel must not make publicly known in any way whatsoever which SC they are executing for the Dutch government, foreign government and/or NATO/EU without the explicit prior consent of the Commissioning Party and DISS/ISO.	Appendix 3 / 6	●	●	●	●
2	Taking photographs of or otherwise recording an IBP, unless required for the execution of the SC, is prohibited, regardless of the device used, without the prior written consent of the Commissioning Party in consultation with DISS/ISO.	Appendix 6	●	●	●	●
3	The Contractor and its personnel will not make contact details and agreements with DISS publicly known in any way.	Appendix 6	●	●	●	●
1.9	**Security incidents**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	An Incident Response Procedure (IRP) for dealing with Security Incidents has been drawn up. It is familiar to everyone who is working on or has access to an IBP.	Appendix 9	●	●	●	●
2	Within the parameters given in the “Classification” table, Security Incidents must be reported to DISS/ISO in line with the IRP.	Appendix 9	●	●	●	●
3	Data regarding access to and examination of an IBP are determined and are retained during the period indicated, to enable investigation of suspected Security Incidents after the fact.	Appendix 9	**6 months**	**6 months**	**3 months**	**3 months**
4	Information regarding established Security Incidents will be retained by the SO for the period indicated.	Appendix 9	**3 years**	**3 years**	**3 years**	**2 years**
5	Personnel must report any weaknesses in security to the SO within the period indicated.	Appendix 9	**without delay**	**without delay**	**within 1 working day**	**within one week**
6	An evaluation mechanism has been defined with which specific lessons learned are identified and security procedures are adapted accordingly.	Appendix 4 / 9	●	●	●	●
7	Anyone causing a Security Incident may face disciplinary action.		●	●	●	●

2 Personnel

Introduction

Personnel security concerns measures aimed at attaining a certain degree of assurance that a person will not damage the interests of the Ministry of Defence. It does not include the physical or personal security of personnel. Personnel of the Ministry of Defence are subject to reliability requirements, as are personnel employed by companies executing SCs.

Personnel security in relation to acquiring knowledge of, working with, producing or coming into contact with an IBP mainly focuses on the Security Screening which is carried out for the purpose of attaining a Certificate of No Objection. In a number of cases a Certificate of Good Conduct issued by Justis, the Ministry of Justice Agency for Scrutiny, Integrity and Screening, suffices.

Furthermore, it is important to devote attention to security awareness among personnel, so that they are constantly aware of the risks and realize the value and necessity of sound security measures, which is also essential when travelling abroad.

The requirements for personnel security are described in the table starting on the following page. They are explained in more detail or expanded on in the appendix where necessary. In the event of any conflict between a requirement in the table and the text in the introductory text or appendix, the requirement in the table prevails.

The ABDO 2019 lists the requirements which need to be met for the security of an IBP. The degree to which the requirements are applied may vary based on a risk analysis. This could mean, for example, that a requirement is less strictly applied than stipulated. This is at the discretion of DISS/ISO.

A filled-in circle (●) in the column under the highest applicable Classification or IBP category indicates which requirements apply. An empty circle (○) in this column means that it must be determined in consultation with DISS/ISO, whether or to what extent the requirement needs to be satisfied.

ABDO 2019 requirements						
CHAPTER 2 PERSONNEL			SECURITY REGIME			
2.1	**The Security Screening, Certificate of No Objection and Certificate of Good Conduct**	**Reference**	**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	A formal List of Confidential Positions (LoCP) has been compiled by DISS.	Appendix 10	●	●	●	○
2	Security Screenings are requested on the basis of a formally compiled LoCP.	Appendix 10	●	●	●	○
3	A valid Certificate of No Objection for the fulfilment of an A-level Confidential Position is on file for all relevant personnel and it is no more than five years old.	Appendix 11	●			
4	A valid Certificate of No Objection for the fulfilment of a B-level Confidential Position is on file for all relevant personnel and it is no more than five years old.	Appendix 11		●		
5	A valid Certificate of No Objection for the fulfilment of a C-level Confidential Position is on file for all relevant personnel and it is no more than five years old.	Appendix 11			●	
6	A valid Certificate of Good Conduct for the fulfilment of a position at NLD Restricted level is on file for all relevant personnel and it is no more than four years old.	Appendix 11				●
7	Administrators, in particular administrators of digital environments, possess an A-level Certificate of No Objection.	Appendix 11	●	●		
8	Administrators, in particular administrators of digital environments, possess at least a B-level Certificate of No Objection.	Appendix 11			●	●
9	The Contractor's SO requests a new Security Screening at least three months before the end of the five-year period following the issue of the most recent Certificate of No Objection.	Appendix 11	●	●	●	○
10	In the event of interim necessity, for example in the case of a change in personal circumstances, the SO requests a new Security Screening.	Appendix 14	●	●	●	○
11	The appointment of a member of staff without Dutch nationality to a Confidential Position must be approved by DISS/ISO prior to the application for a Security Screening.	Appendix 13	●	●	●	○
12	The Contractor only appoints employees with Dutch nationality to Confidential Positions which require access to a large amount of SI (to be determined by DISS/ISO in consultation with the Commissioning Party).	Appendix 13	●	●	●	●
13	The SO has a list on file of all Certificates of No Objection, Certificates of Good Conduct and declarations of awareness of the duty of secrecy.	Appendix 4	●	●	●	●
2.2	**Declaration of awareness of the duty of secrecy**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The SO has drawn the attention of employees holding a Confidential Position or other position to the obligations entailed in holding a Confidential Position or other position.	Appendix 10 / 12	●	●	●	●
2	A 'Declaration of awareness of the duty of secrecy of employees holding a Confidential Position or other position' signed by employees holding a Confidential Position is on file and it is no more than five years old.	Appendix 12	●	●	●	
3	A 'Declaration of awareness of the duty of secrecy of employees holding a Confidential Position or other position' signed by employees holding a Confidential Position is on file.	Appendix 12				●
4	A 'Declaration of awareness of the duty of secrecy of employees holding a Confidential Position or a Crypto Position' signed by employees holding a Confidential Position that entails examining crypto, crypto-security or Information or materiel marked as a Controlled Cryptographic Item (CCImarked) is on file and it is no more than five years old.	Appendix 12	●	●	●	
2.3	**Release from a Confidential Position**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The SO reports to DISS/ISO the release of an employee from a Confidential Position in the case of: - change of job of an employee holding a Confidential Position; - dismissal of an employee holding a Confidential Position; - violation of security regulations by an employee holding a Confidential Position.	Appendix 15	●	●	●	○

2	A declaration of release from office signed by employees released from a Confidential Position or a Crypto Position is on file.	Appendix 15	●	●	●	○
3	The SO has given an explanation of the declaration of release from office, has revoked the Certificate of No Objection or copy thereof and ensured that the employee does not have any IBPs in his or her possession.	Appendix 15	●	●	●	○
4	If the employee holding a Confidential Position intentionally or unintentionally ignores or violates the Contractor's security regulations, the SO is required to take appropriate action and inform DISS/ISO. Gross negligence or intentionally compromising State Secret or Vital Information or Materiel may lead to criminal proceedings.	Appendix 15	●	●	●	○
5	Following termination of the contract, all digital IBPs are returned to the Commissioning Party. This process is described in more detail in the Security Plan.		●	●	●	●
2.4	**Travelling abroad**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	Employees holding a Confidential Position will report any proposed trip abroad for the purpose of the SC to the SO without delay.	Appendix 16	●	●	●	○
2	Employees holding a Confidential Position will report any proposed trip to a high-risk country to the SO without delay.	Appendix 16	●	●	●	○
3	If a Request for Visit (RfV) is required for a business trip, employees holding a Confidential Position submit an RfV to DISS/ISO via the SO for approval. Without an approved RfV, the trip cannot take place.	Appendix 16	●	●	●	○
4	The SO briefs and debriefs the employee holding a Confidential Position who has reported to the SO a proposed trip to a high-risk country.	Appendix 16	●	●	●	○
5	An employee holding a Confidential Position has immediately reported to the SO a foreign business or private trip of longer than six consecutive months undertaken by him or herself or his or her Partner.	Appendix 16	●	●	●	○
5.1	The SO will report to DISS/ISO any foreign business or private trip of longer than six consecutive months undertaken by an employee holding a Confidential Position or his or her Partner.	Appendix 16	●	●	●	○
6	The SO reports any business and/or private trips by an employee holding a Confidential Position to or in a high-risk country to DISS/ISO using the form in Appendix 16.	Appendix 16	●	●	●	○

3 Physical

Introduction

If an IBP is stored, processed or transported on the Contractor's own site, whether or not in designated compartments on site (e.g. a physical work area in a building), this site/compartment must be physically secured. A compartment may also have to be secured if discussions and/or presentations are held at a classified level there, despite the fact that no storage or processing usually takes place there.

Physical security measures are subdivided into measures of an Organisational (O), Constructional (C), Electronic (E) and Responsive (R) (OCER) nature. A carefully considered selection of OCER measures must make unlawful access to an IBP impossible, or in any case signal in good time attempts to do so. Organisational measures are primarily in place in order to prevent unlawful access to an IBP. Electronic measures are primarily intended to effect the timely signalling of unlawful access or attempts to gain unlawful access. Constructional measures should increase the Delay Time to such an extent that timely Intervention can be performed by the user, a security company, the police, or – in the event that the ABDO company has a Prohibited Place or is established on a site of the Ministry of Defence – the Ministry of Defence. The Delay Time is realised by constructional measures such as robust walls, floors and ceilings, and suitable doors, windows, etc. It is important to carry out an accurate timeline analysis in order to determine that security is effective. For IBP 1 and IBP 2 it is the norm that security must be effective. That means that Intervention can be carried out at all times before the perpetrator can compromise the IBP. The total Delay Time that is created by means of the layers of OCER security measures must thus be compared with the time that it takes a perpetrator to compromise the IBP.

The ABDO 2019 lists the requirements which need to be met for the security of an IBP. The degree to which the requirements are applied may vary based on a risk analysis. This could mean, for example, that a requirement is less strictly applied than stipulated. This is at the discretion of DISS/ISO. Contractors must comply with the requirements of the Physical chapter in the case of storage of one or more IBPs at the Contractor's own site.

The requirements for physical security are described in the table starting on the following page. These are explained in more detail or expanded on in the appendix where necessary. In the event of any conflict between a requirement in the table and the text in the introductory text or appendix, the requirement in the table prevails.

A filled-in circle (●) in the column under the highest applicable Classification or IBP category indicates which requirements apply. An empty circle (○) in this column means that it must be determined in consultation with DISS/ISO, whether or to what extent the requirement needs to be satisfied.

ABDO 2019 requirements						
CHAPTER 3 PHYSICAL			SECURITY REGIME			
3.1	Organisational measures	Reference	IBP 1/ NLD TS	IBP 2/ NLD S	IBP 3/ NLD C	IBP 4/ NLD DV
1	The physical security measures are established in a layered structure to which the “Need-to-Be” principle applies.	Appendix 17 / 18	●	●	●	●
2	When compiling the physical measures, the “Need-to-Be” and “Need-to-Know” principles are applied.	Appendix 18	●	●	●	●
3	IBPs must be secured to prevent them from being compromised and to detect/identify any instances in which they are compromised.	Appendix 19 / 21	●	●	●	●
4	Physical access to the compartment containing an IBP must be verifiable down to the level of the individual.	Appendix 19	●	●	●	○
5	Access to the IBP or compartment is only granted by means of Two- factor Authentication.	Appendix 19	●	●	○	
6	Only an Authorised Person can independently gain access to an IBP or to a compartment containing an IBP.	Appendix 18	●	●	●	
7	The SO arranges the Authorisation of the personnel regarding access to an IBP and the corresponding infrastructure.	Appendix 18	●	●	●	
8	Periodically, i.e. at least once a year, the involved personnel and security personnel are trained in implementing the security measures.	Appendix 18	●	●	●	●
9	Access by persons without Authorisation (e.g. visitors) is reported to the SO in advance.	Appendix 18	●	●	●	
10	Persons with an Authorisation are identifiable within the compartment by means of a pass worn visibly. The pass has on it at least the name of the person and a passport photo.	Appendix 18	●	●	●	
11	Persons without Authorisation (such as visitors) are identifiable within the compartment by means of a pass worn so it is clearly visible. The word “visitor” is clearly visible on the pass for all to see.	Appendix 18	●	●	●	○
12	In the event of access by persons without Authorisation, the personnel in the compartment in which work is carried out with or on an IBP are informed in advance. The personnel then take measures to prevent the IBP from being compromised.	Appendix 18	●	●	●	
13	In all compartments containing an IBP, personnel without Authorisation (such as visitors) are escorted by personnel with Authorisation. The identity of persons without Authorisation is determined and registered in advance. The registration hereof is retained for at least a year and is submitted to DISS/ISO on request.	Appendix 18	●	●	●	●
14	Access to a compartment containing an IBP by visitors without Authorisation who do not have Dutch nationality will be reported to DISS/ISO via the SO at least five working days in advance. Without the permission of DISS/ISO, this visit will not take place.	Appendix 18	●	●	●	●
15	Access checks are performed at every layer of security.	Appendix 17	●	●	●	
16	General security instructions are attached to the outside of the compartment containing an IBP.	Appendix 3 / 4 / 18	●	●	●	
17	The issue of keys for access to compartments and means of storage containing an IBP is registered. When issuing keys, it will be checked whether the person to which the key is being issued has Authorisation. The registration hereof will be retained for at least one year. The keys are accessible to as few people as possible.	Appendix 18	●	●	●	●
18	Only certified keys are used.	Appendix 19	●	●	○	
19	The SO manages the certificates, digit combinations and spare keys of storage systems and compartments. These must be stored/secured in accordance with the security level of the IBP.	Appendix 4 / 18	●	●	○	
20	Digit combinations for locks are changed to a combination that has not been used previously: - if a new means of storage or lock is put into use; - if an employee who knows the combination is transferred; - if it has been established or is suspected that the IBP has been compromised; - no more than six months after the last time the combination was changed.	Appendix 18	●	●	●	

21	Before applying to an IBP a procedure that deviates from the regular procedure described in the security plan, permission must be gained from DISS/ISO. The security of the IBP will be kept at the same level in this regard.	Appendix 18	●	●	●	●
22	The “Clear Desk Principle” and “Clear Screen Principle” are applied in all compartments that do or could contain an IBP. An IBP is not left unsecured.	Appendix 18	●	●	●	●
23	Management and maintenance measures are met to ensure the constant operation of security measures.	Appendix 18	●	●	●	●
24	The loss of a means of authentication, such as a key/digital key, will be treated as a Security Incident.	Appendix 18	●	●	●	○
25	There are no more compartments than strictly necessary.	Appendix 18 / 19	●	●	●	●
26	When companies work in partnership with other companies on an assignment, the compartments will be centralised as far as is possible.	Appendix 18 / 19	●	●	●	●
27	The compartment containing an IBP is in a zone that is screened off from public areas or uncontrolled compartments by means of access control.	Appendix 18 / 19	●	●	●	
28	Security personnel have the means to issue alerts.	Appendix 20	●	●	●	○
29	When leaving a compartment containing an IBP, a security round is completed, during which the door of the means of storage, the compartment and, where possible, the building is locked. Windows and doors are locked and the Intruder Detection and Alarm System (IDAS) is activated. In addition, intrusion checks are carried out and the seals of emergency doors are inspected.	Appendix 18 / 20	●	●	●	○
30	In the absence of Authorised personnel, effective security is safeguarded.	Appendix 18	●	●		
31	A Prohibited Place must comply with the IBP 1 standard in all security areas (organisational, personnel, physical and cyber security).		●			
3.2	**Constructional measures**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	Compartments containing an IBP can be locked.	Appendix 19	●	●	●	●
2	A locking plan and master key plan are included in the security plan. In the absence of Authorised personnel, windows, doors and storage systems are locked. Keys are secured at the same level as the IBP to which they provide access. Keys are stored in a key cabinet equipped with an EN 1300-certified lock. If a storage system or key cabinet is under detection, the EN 1300-certification of the key cabinet lock could lose its validity.	Appendix 18 / 19	●	●	●	●
3	A compartment in which an IBP is stored is locked with a lock that has a certified cylinder and keys. If a lock with a cylinder cannot be applied, a mechanism that is certified or tested to the same level will be used, whereby unauthorised entry is not possible without leaving traces of forced entry.	Appendix 19	●	●	○	
4	Access doors with an Electronic Access Control System (EACS) are fitted with a door spring and a (electronic and acoustic) alarm that sounds when it has been open for too long.	Appendix 19 / 20	●	●	●	
5	Emergency doors in the compartment only open outwards and can be sealed. An electronic or acoustic signal is given when they are opened.	Appendix 19	●	●	●	
6	The building in which an IBP is located is secured against being climbed. Movable items that can be used for climbing, such as containers, waste bins and ladders, have been removed. Rainwater pipes, low walls, etc., are fitted with security measures to prevent climbing in accordance with NEN1887.	Appendix 19	●	●	●	
7	Façade openings larger than 15 cm will be secured in accordance with NEN-EN 5096 and NEN-EN 1627 in the case of compartments.	Appendix 19	●	●	●	
8	Cellar windows and the like are screened off by bars or expanded metal in accordance with NEN-EN 5096 and NEN-EN 1627 in the case of compartments.	Appendix 19	●	●	●	○
9	Dome lights that are not impact-proof are fitted with bars or expanded metal in accordance with NEN-EN 5096 or NEN-EN 1627 in the case of compartments.	Appendix 19	●	●	●	○
10	Compartments and means of storage containing an IBP are fitted on all sides (three dimensional) with intruder-resistant measures in accordance with the norms in the table in Appendix 19.	Appendix 19	●	●	●	○
11	If a compartment or storage system containing an IBP abuts an outer façade, the intruder-resistance properties of the outer façade must comply with the requirements in accordance with the security level applicable to the IBP.	Appendix 19	●	●	●	
12	The windows and façade are fitted with intruder-resistant systems in accordance with the security level applicable to the IBP.	Appendix 19	●	●	●	

13	Storage systems up to 1,000 kilograms are chemically anchored.	Appendix 19	●	●		
13.1	Storage systems up to 1,000 kilograms are anchored.	Appendix 19			●	
14	Attachment points of means of storage that can be accessed from outside are fitted with secured screws, nuts and/or bolts.	Appendix 19	●	●	●	
15	Means of storage have Two-factor Authentication.	Appendix 19	●	●	●	
16	Means of storage are locked in such a way that intrusion can be traced retrospectively.	Appendix 19	●	●	●	●
17	Storage systems must comply with the NEN-1143 standard.	Appendix 19	●	●	●	
18	Site fencing with access control surrounds any building or grounds containing an IBP.	Appendix 19	●	●	●	
19	Security lighting is in place around the building containing an IBP.	Appendix 17 / 19	●	●	●	
20	When laying out land and water infrastructure, intruder-prevention measures must be taken into account by ensuring that there is a clear view of the whole site so an intruder cannot work unseen.	Appendix 17 / 19	●	●	●	
21	Windows and glass partitions in a compartment containing an IBP must be fitted with means to prevent people from looking in.	Appendix 19	●	●	●	
22	Measures have been taken to keep outside the compartment electronic equipment that is not strictly necessary for carrying out the work.	Appendix 19	●	●	○	
3.3	**Electronic measures**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	Compartments containing a means of storage containing an IBP are fitted with an IDAS.	Appendix 20	●	●	●	
2	The compartments adjacent to the compartment containing an IBP are fitted with an IDAS. A means of storage containing an IBP is itself fitted with an IDAS.	Appendix 20	●	●	●	
3	Activating and deactivating an IDAS is only possible by means of Two factor Authentication.	Appendix 20	●	●	●	
4	The IDAS functions 24 hours a day, 7 days a week, unless Authorised personnel are present in the compartment.	Appendix 18 / 20	●	●	●	
5	IDAS components are installed in such a way that if the IBP is compromised, or if attempts are made to do so, this will be detected and an alarm will be set off.	Appendix 20	●	●	●	
6	The work area containing an IBP is included as a separate zone in the IDAS. This zone is active when there are no Authorised personnel in the area.	Appendix 18 / 20	●	●	●	
7	The automatic alarm of the IDAS meets the quality stipulated in Appendix 19.	Appendix 19	●	●	●	
8	An alarm from an IDAS leads to an alarm response within the Intervention Time stipulated in Appendix 21.	Appendix 21	●	●	●	
9	The IDAS signals and registers failure of the power supply of the IDAS.	Appendix 20	●	●	●	
10	The IDAS has a guaranteed power supply.	Appendix 20	●	●	●	
11	It is not possible to sabotage or compromise the IDAS without this being noticed. Attempts to do so are presented as an actual alarm.	Appendix 20	●	●	●	
12	Detection takes place under all conditions, climatological and otherwise.	Appendix 20	●	●	●	
13	Motion detectors are fitted with anti-masking measures.	Appendix 20	●	●	●	
14	Only electronic equipment that is essential for executing the contract is permitted in areas containing an IBP. Equipment is selected on the basis of a risk analysis. A list of the equipment and accompanying risk analysis is drawn up in advance in consultation with DISS/ISO and included in the security plan.	Appendix 18 / 19 / 20 / 36	●	●	●	
15	No cameras, smart devices, microphones or other equipment with recording capabilities are permitted in areas containing an IBP.	Appendix 20	●	●	●	
16	Security systems are installed and periodically maintained by a certified company in accordance with NEN-EN 50130. In addition, the security systems are inspected periodically, i.e. at least once a year.	Appendix 19	●	●	●	
17	A security camera with a view of the entrance to the compartment is installed outside the compartment.	Appendix 20	●	●	○	

18	The retention period for camera images is three months. Camera images containing data relating to an incident will be retained for one year.		●	●	●	
19	An EACS for controlling access to the compartment is installed and in operation.	Appendix 20	●	●	○	
20	If electronic locks are used, measures are taken to detect forced entry.	Appendix 18	●	●		
21	The EACS is equipped with an Anti Pass Back (APB) system.	Appendix 20	●	●		
22	The EACS is equipped with a Logging function and the logs are retained for at least one year.	Appendix 20	●	●		
23	The EACS is set up in such a way that if the system turns off or fails, all entrances to the compartment are mechanically or electronically locked.	Appendix 20	●	●		
24	The EACS is set up in such a way that a panic button or panic release mechanism is installed in the compartment so that, in the context of safety, the Building can be left quickly in the event of an emergency.	Appendix 20	●	●		
25	The panic button or panic release mechanism is not accessible from outside. Following the use of the panic button or panic release mechanism, adequate security measures will be taken to protect the IBP.	Appendix 20	●	●		
26	If a security system (EACS or IDAS) is linked to a building management system, the security measures of the security system also apply to the building management system.	Appendix 20	●	●		
27	Before a compartment is used and when additional resources are placed in a compartment or the resources in a compartment are changed, a digital security investigation, sound reduction measurements and zoning measurements must be conducted in consultation with DISS/ISO. Any measures taken must be implemented in consultation with DISS/ISO.		●	●		
3.4	**Response measures**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	Signals from the IDAS and the EACS will lead to timely Intervention.	Appendix 21	●	●	●	
2	Intervention is carried out within the stipulated Intervention Time by personnel who have been designated and trained to do so.	Appendix 21	●	●	●	●
3	If an alarm only goes off in a compartment and not in the security layers around it, action must be taken as though the surrounding alarms have also gone off.	Appendix 21	●	●	●	
4	If it is established that an IBP has been compromised, security personnel inform the SO immediately.	Appendix 21	●	●	●	●
5	The response to the failure (technical or otherwise) will lead to the restoration of the required return on security.	Appendix 21	●	●	●	●
6	Following an alarm, inspection of the compartment containing an IBP will be carried out by the SO or the person to whom he/she has given a mandate to do so.	Appendix 21	●	●	●	○
7	Alarm verification takes place on the outside of the compartment containing an IBP. As part of this, all entrances, façade openings, roofs, and the like, are inspected.	Appendix 21	●	●	●	●
8	At the time of the alarm verification, the personnel who carry out the alarm verification do not have at their disposal the keys or codes that grant access to the IBP.	Appendix 21	●	●	●	●
9	Private-Sector Emergency Centres have judicial recognition and comply with the provisions of the NEN-EN 50518 standard.	Appendix 21	●	●	●	●
3.5	**Transport and post**					
1	An IBP is only taken out of the compartment if this is absolutely necessary for the continuation of the work.	Appendix 22	●	●	●	●
2	The SO draws up instructions for transporting and posting an IBP and supervises this.	Appendix 22	●	●	●	●
3	An IBP must never be taken home.	Appendix 22	●	●	●	○
4	Transport of an IBP is reported to DISS/ISO in advance.	Appendix 22	●	●	●	
3.6	**Transport and post within the Netherlands**					
1	Transport of an IBP only occurs through the agency of DISS/ISO.	Appendix 22	●			
2	An IBP may only be transported in a means of transport that can be locked and has been approved by DISS/ISO.	Appendix 22	●	●	●	

3	Transport of an IBP is carried out: - by hand, whether or not by private transport, by one Authorised employee, or - by engagement of a transport/courier company approved by DISS/ISO.	Appendix 22		●	●	
4	An IBP is only be transported in a lockable means of transport.	Appendix 22				●
5	Transport of an IBP is carried out: - by hand, whether or not by private transport, by one Authorised employee, or - by engagement of a transport/courier company approved by DISS/ISO, or - by engagement of a transport/courier company.	Appendix 22				●
6	The transport/courier company to which the IBP is entrusted without the supervision or escort of an employee holding a confidential position, has been registered with DISS/ISO as a Subcontractor.	Appendix 22		●	●	○
7	An IBP is transported via the shortest possible route without interruptions. The IBP is kept under supervision and vehicles are not left unattended.	Appendix 22		●	●	
8	Sending SI by post is not permitted.	Appendix 22	●			
9	Sending SI by post is only permitted within the Netherlands by registered post with a track and trace number in double packaging according to the provisions of Appendix 22, with an acknowledgement of receipt being issued without delay.	Appendix 22		●	●	
10	Sending SI by post is only permitted in the Netherlands in double packaging in accordance with the provisions of Appendix 22.	Appendix 22				●
3.7	**Transport and post abroad**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	Transport of an IBP only occurs through the agency of DISS/ISO.	Appendix 22	●			
2	Without the permission of DISS/ISO, an IBP will not be taken abroad.	Appendix 22		●	●	●
3	International transport of an IBP takes place following approval of the transport plan by DISS/ISO.	Appendix 22		●	●	●
4	For transport of SI to a foreign country, it is possible to fall back on DISS/ISO (”Government-to-Government”procedure).	Appendix 22		●	●	●
5	Sending SI by post is not permitted.	Appendix 22	●	●	○	
6	Sending SI by post is permitted by registered post with a track and trace number in double packaging, with an acknowledgement of receipt being issued without delay.	Appendix 22			○	●
3.8	**Physical storage, processing and development**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	The SO or person designated and authorised to do so has an up-to-date list on file of all SCs at the company.	Appendix 23	●	●	●	●
2	A register is kept of who has SI in his/her possession.	Appendix 23	●	●	●	
3	A register is kept of who has performed work on or seen SI.	Appendix 23	●	●		
4	If Information is produced by the company and the author suspects that the State could be damaged if it were compromised, it is classified. The Classification is determined and registered by the SO/Deputy SO.	Appendix 23	●	●	●	
5	SI is registered and labelled.	Appendix 23	●	●	●	
6	SI is registered and given a unique copy number.	Appendix 23	●	●		
7	Classifications and Markings are applied in accordance with Appendix 23.	Appendix 23	●	●	●	●
8	Information is only reproduced with permission from the person who determined the Classification.	Appendix 23	●	●	●	
9	Reproductions created are registered.	Appendix 23	●	●	●	
10	Creating reproductions is only permitted by the designated authorised personnel, who are also responsible for the registration	Appendix 23	●	●	●	
11	Reproductions have the same Classification as the original, even if only parts of the original are used.	Appendix 23	●	●	●	●

12	No more reproductions are made than is strictly necessary.	Appendix 23	●	●	●	●
13	Creating reproductions is only permitted using means permitted by DISS/ISO.	Appendix 23	●	●	●	
14	Means of reproduction are considered Information Systems and are secured at least the same level as the information processed.	Appendix 23	●	●	●	●
15	In the case of destruction, an official report of the destruction is drawn up by the SO or the designated employee with the correct authorisation.	Appendix 23	●	●	●	
16	Information is destroyed in accordance with Appendix 23.	Appendix 23	●	●	●	●

4 Cyber

Introduction

The national Cyber Security Assessment Netherlands (CSAN) is drawn up periodically by public- and private-sector parties working in close collaboration. One of the key findings of the CSAN is that states and cybercriminals form a major threat to the Netherlands. This is evident from the growing number of digital attacks on the Ministry of Defence, the Defence industry and allies' networks. The attacks are becoming increasingly complex and are aggressive in nature. The expectation is that this trend will continue over the coming years. Up-to-date and stricter measures are needed to safeguard digital resilience.

As of the ABDO 2019, measures in the digital domain are referred to as Cyber Measures. The term Cyber refers not only to IT infrastructure, but also the system of activities (including operations) that is made possible by the infrastructure. It is these activities that must be protected. The thorough Security of information forms the basis for Cyber Security. In addition to information security requirements, this edition of the ABDO also includes requirements relating to the Cyber Security Organisation, incident management, and Logging and Monitoring of an organisation in order to enable a rapid response to threats posed to Cyber Activities.

The ABDO 2019 requires the organisation to designate an employee to take on the role of Cyber Security Officer (Cyber SO). The Cyber SO oversees the Cyber Activities that are performed within the organisation for the Ministry of Defence and the measures to protect them.
The Cyber SO is the contact person for DISS/ISO regarding the Cyber Domain.

New requirements are not only demanded by the increasing threat, but also by the innovations in the digital domain that offer new functionalities. This chapter also sets requirements pertaining to Cloud Computing and the use thereof, bring/choose your own device (BYOD/CYOD) and Virtualization.

The ABDO 2019 lists the requirements which need to be met for the Security of an IBP. The degree to which the requirements are applied may vary based on a risk analysis. This could mean, for example, that a requirement is less strictly applied than stipulated. This is at the discretion of DISS/ISO.

The requirements relating to Cyber Security are detailed in the following table. These are explained in more detail or expanded on in the appendix where necessary. The table of requirements has the same global structure as the ISO 27000 series and the content is in line with the Defence Security Policy. In the event of any conflict between a requirement in the table and the text in the introductory text or appendix, the requirement in the table prevails.

A filled-in circle (●) in the column under the highest applicable Classification or IBP category indicates which requirements apply. An empty circle (○) in this column means that it must be determined in consultation with DISS/ISO, whether or to what extent the requirement needs to be satisfied.

ABDO 2019 requirements						
CHAPTER 4 CYBER			SECURITY REGIME			
4.1	**Information security policy**	**Reference**	**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.1	Policy rules for Information Security					
1	There is policy relating to cyber security.		○	○	○	○
4.2	**Organizing Information Security**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.2	Internal organization					
1	A Cyber Security Officer (Cyber SO) has been appointed. Like the SO, the Cyber SO has direct access to the board of directors of the organization. The Cyber SO can have third parties within the organization carry out subtasks.	Appendix 24	●	●	●	●
2	On behalf of the board of directors, the Cyber SO has been authorized to take appropriate security measures in the Cyber Security domain, or arrange for them to be taken.	Appendix 24	●	●	●	●
3	The Cyber SO oversees, on behalf of the board of directors, the secure set-up of the digital infrastructure within the organization.	Appendix 24	●	●	●	●
4	Each year and at the request of DISS/ISO, the Cyber SO provides DISS/ISO with the organizations external IP addresses and domain names, the names of its internet service provider(s) and details of the hardware/software used to execute the classified contract.	Appendix 41	●	●	●	●
5	The Cyber SO oversees, by means of a log, the location, issue, intake and origin of all digital IBPs received by or taken into the management of the organization.	Appendix 24	●	●	●	
6	The Cyber SO has, at all times, an overview of the digital IBPs in use.	Appendix 24				●
7	The Cyber SO also carries out the tasks as described in the appendix.	Appendix 24	●	●	●	●
8	The Cyber SO ensures full cooperation during inspections, audits and investigations of the Contractor's IT infrastructure by DISS/ISO.	Appendix 24	●	●	●	●
4.2	Division of tasks					
9	The rights of a user do not include a full cycle of actions in a critical Information System.	Appendix 31	●	●	●	●
10	There is a division between IT-administrator tasks and user tasks.	Appendix 31	●	●	●	●
11	Before configuration data that could compromise the Integrity of information systems is processed, the data is inspected and accepted by a second person. A log is kept of acceptance.	Appendix 31	●	●	●	●
12	Role-based access control (RBAC) is implemented for IT management.	Appendix 31	●	●	●	●
4.2	Mobile devices and teleworking					
13	An IBP that is saved on a mobile device is only permitted with the application of the procedures and means approved by DISS/ISO: - approved Encryption; - no more information saved than is necessary; - not used in public spaces.	Appendix 22 / 25	●	●	●	
14	An IBP that is saved on a mobile device is only permitted with the application of the procedures and means approved by DISS/ISO: - approved Encryption; - no more information saved than is necessary; - not used in public spaces; - a connection approved by DISS/ISO.	Appendix 22 / 25				●
15	User instructions have been drawn up for the use of mobile devices and teleworking.					●
16	Mobile devices do not have any characteristics that make them directly traceable to the Ministry of Defence.					●

17	There are provisions to guarantee the currency of anti-Malware software on mobile devices.		●	●	●	●
18	After a report of loss or theft, the functionality to communicate with the central applications is shut down without delay.					●
19	Mobile devices in the context of BYOD or CYOD are only permitted following the approval of DISS/ISO.	Appendix 25 / 28				●
20	Data is stored, processed and transported on BYOD/CYOD on the basis of the same conditions imposed on NLD Restricted networks. For local storage of data, encryption approved by DISS/ISO is applied.	Appendix 25 / 28				●
4.2	Teleworking					
21	Teleworking is not permitted.		●	●	●	
22	Teleworking provisions on the basis of a terminal server connection is set up in such a way that no company information is saved on the workstation ("zero footprint") and any Malware from the workstation cannot enter the trusted section.					●
23	If access to an IBP is possible via a remote log-in facility, a procedure for this is included in the Security Plan.					●
24	For remote access, use is made of solutions and means approved by DISS/ISO.					●
25	During teleworking, all communications to and from mobile devices must be routed via approved encrypted connections with the NLD Restricted information network.					●
26	Measures to ensure screen privacy (e.g. privacy filters) are implemented for mobile equipment located outside a compartment.					●
4.3	**Secure personnel**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.3	Awareness, qualification courses and training regarding Information Security					
1	Personnel involved in handling IBPs complete Cyber security- awareness training annually. See Appendix 26 for a list of focal areas.	Appendix 26	●	●	●	●
2	The SO, Cyber SO, IT administrator and other employees who are involved in handling digital IBPs have the necessary experience, competences and knowledge from relevant qualification courses and training.		●	●	●	●
4.3	Employment termination and changes to responsibilities					
3	A procedure has been determined for changing and terminating a position, employment, a contract, a project or an agreement in which at least the following is detailed: the withdrawal of access rights, the collection of Company ICT Resources, and which obligations will continue to apply after termination of the contract.		●	●	●	●
4.4	**Management of company resources**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.4	Inventory of Company ICT Resources					
1	There is an up-to-date log of Company ICT Resources. See the appendix for an overview of the information to be logged.	Appendix 27	●	●	●	●
2	An up-to-date description of the ICT infrastructure is available.	Appendix 27	●	●	●	●
3	All equipment and systems are recorded in a network or configuration diagram, in which the location and function of the components are clearly indicated.	Appendix 27	●	●	●	●
4.4	Ownership of Company ICT Resources					
4	A responsible line manager is appointed for each company process, application, collection of data and other Company ICT Resources.	Appendix 27	●	●	●	●
4.4	Acceptable use of Company ICT Resources					
5	Rules have been determined and documented for the use of Company ICT Resources and the users have taken cognizance of them. The rules are determined in an appendix to the Security Plan.		●	●	●	●
6	Only applications that have been installed on a system by IT Management are used.		●	●	●	●
4.4	Classification of information					
7	The author of the information proposes a Classification and/or Marking and puts it on the information. The Cyber SO lays down the Classification of the information.	Appendix 23 / 30	●	●	●	

8	The author of the information determines the Classification and/or Marking and puts it onto the information.	Appendix 23 / 30				●
4.4	Labelling information					
9	The highest Classification and Marking of Information is stated on removable and mobile data carriers.	Appendix 23 / 30	●	●	●	●
4.4	Handling Company ICT Resources					
10	System documentation that contains specific information about security measures of IBPs on the system are secured at the same level as this IBP.		●	●	●	●
11	System documentation is available that describes the implementation of a system in order to enable management.	Appendix 29	●	●	●	●
12	Procedures have been established and put into operation for the removal of an IBP and the destruction thereof.		●	●	●	●
13	Upon expiry of the contract or disposal, the data carriers are physically destroyed. An official report is drawn up of the destruction.	Appendix 23	●	●	●	
14	The deletion of data carriers is only permitted if DISS/ISO-approved means are used.		●	●	●	●
14.1	All digital data carriers in compartments labelled SI are encrypted. The proposed solution must be approved in consultation with DISS/ISO prior to use.		●	●	●	
4.4	Management of Removable Data Carriers					
15	Removable Data Carriers must not be left behind unattended.		●	●	●	●
16	In the case that data carriers have a shorter expected service life than the data that they contain, the data is copied when 75% of the service life of the data carrier has passed.		●	●	●	●
4.5	**Access security**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.5	Policy for access security					
1	Only authorized users have access.	Appendix 31	●	●	●	●
2	The system prevents unauthorized access.		●	●	●	●
3	Access by third parties for the purpose of supervision, inspection and/or audit is approved by DISS/ISO.		●	●	●	●
4	The manner in which users have access is described in the Security Plan.		●	●	●	●
5	There is a single master database of user authentication information, on the basis of which users are identified and authorized in advance.		●	●	●	●
4.5	Access to networks and network services					
6	Remote administration is not permitted.		●	●	●	
7	A procedure has been determined whereby remote maintenance is only accessible if it is strictly necessary and a connection can only be activated by an authorized employee (in accordance with the Security Plan).					●
8	Access for remote maintenance by a Supplier is only made available on the basis of a request for change or notification of a malfunction.					●
9	Remote management of equipment is only permitted if DISS/ISO-approved means are used.	Appendix 25				●
4.5	Registration and deregistration of users					
10	On the basis of a risk analysis it has been determined where and in what way the roles will be split and which access rights will be assigned. The risk analysis, results and measures are included in the Security Plan.		●	●	●	●
11	The account mechanism guarantees that actions can be traced back to a natural person.		●	●	●	●
12	Accounts do not give any indication of the privilege level or the name of the user.		●	●	●	●
13	When issuing means of authentication, the identification of the user is verified as well as the fact that the user has the right to the means of authentication.		●	●	●	●
4.5	Management of special access rights					
14	Users only have rights in so far as this is necessary for them to perform their task ("Need-to-know", "need-to-use").		●	●	●	●
15	Users only have access to the set of applications and commands that is considered necessary for the position.		●	●	●	●

16	Systems processes are run under the user's own name in the event that these processes perform actions for other systems or users.		●	●	●	●
17	Authorizations and user roles are issued per user in accordance with a fixed authorization procedure.		●	●	●	●
18	There is an emergency procedure whereby an administrator account and corresponding password can be accessed in the case of emergencies. This must describe who grants permission for use of this account.		●	●	●	●
19	The requirements that apply to the password for an administrator account are one (1) classification level higher than the system that they manage, with the highest classification level being NLD TOP SECRET.		●	●	●	●
20	There are measures taken to combat the unauthorized use of the workstation/workstation session i/o ports (such as parallel, serial, USB and firewire ports).		●	●	●	●
21	If a user is logged onto a workstation/workstation session, the workstation/workstation session can only be taken over once permission has been granted by the user. There is the possibility for the user him/herself to terminate the takeover of the workstation/workstation session or notification is given that the workstation/workstation session has been ended.		●	●	●	●
22	Administrator or root rights are assigned to a limited group of IT administrators. A register is kept of these IT administrators.		●	●	●	●
23	The IT administrators manage the use of the administrator accounts.		●	●	●	●
24	The system indicates which authorizations have been granted to persons and/or systems.		●	●	●	●
4.5	Management of secret Authentication information of users					
25	The following applies to passwords: - passwords are issued in a secure manner (verification of the identification of the user as well as the fact that the user has the right to the means of authentication); - temporary passwords are replaced by a new password the first time they are used; - passwords are not be issued at the same time as the user account; - passwords that are included with software as standard are changed during installation.		●	●	●	●
26	The requirements that apply to the password for a user account are of the same classification level as the system to which they grant access.		●	●	●	●
4.5	Assessment of users' access rights					
27	Access rights of users are evaluated periodically, i.e. at least once a year. The interval is described in the Security Plan.					●
28	Access rights of users are evaluated periodically, i.e. at least every three months. The interval is described in the Security Plan.			●	●	
29	Access rights of users are evaluated periodically, i.e. at least once a month. The interval is described in the Security Plan.		●			
30	Accounts that are not used for more than 60 days are blocked.		●	●	●	●
31	A blocked account is unblocked by the intervention of the Cyber SO.		●	●	●	
4.5	Use of secret Authentication information					
32	A code of conduct is issued to users, which states at least the following: - passwords will not be written down; - users will never share their passwords with anyone; - a password will be changed without delay if it suspected that it is known to a third party; - passwords will be not used in automatic log-in procedures (e.g. saved using a function key or in a macro).		●	●	●	●
33	The minimum length of passwords is the following number of characters: IBP 1: 12; IBP 2 and 3: 10; IBP: 9.		●	●	●	●
34	Passwords are changed every so many days: IBP 1: 60, IBP 2: 90, IBP 3: 90, IBP 4: 90. When doing so, the last 10 passwords used may not be used again.		●	●	●	●
35	Authentication of users on the basis of passwords.		●	●	●	●
36	Two-factor Authentication is used, whereby one factor is something you know (a password) and the other is something you have (e.g. your phone).		●	●	●	
37	Two-factor Authentication, whereby one factor is a password and the other is selected according to preference, is used to grant external access.					●

38	Applications must not run under a system account unnecessarily or for longer than necessarily.		●	●	●	●
39	If tokens or biometric applications are used, it is not possible to easily disable these applications.		●	●	●	●
40	Passwords consist of at least three of the following elements: upper- and lowercase letters, punctuation marks and numbers.		●	●	●	●
4.5	Restriction of access to information					
41	When assigning authorizations, a distinction is at least made between read and write permissions.		●	●	●	●
42	Hardware of an IBP system is physically permanently assigned to that system.		●	●	●	●
4.5	Secured log-in procedures					
43	Before log-in the user is shown a notification that only authorized use is permitted for purposes explicitly determined by the organization.		●	●	●	●
44	The number of active sessions/workstations per user is limited to two.					●
45	The number of active sessions/workstations per user is limited to one.		●	●	●	
46	After an incorrect password for a user account has been entered five times, the account will be blocked for at least 10 minutes. If a lock-out period cannot be imposed, the account will be blocked until the user requests the lockout be lifted or the password is resetted.					●
47	After an incorrect password for a user account has been entered three times, the account will be blocked for at least 10 minutes. If a lock-out period cannot be imposed, the account will be blocked until the user requests the lockout be lifted (see 46). The Cyber SO grants permission in this regard.				●	
48	After an incorrect password for a user account has been entered three times, the account will be blocked until the user requests the lockout be lifted (see 46). The Cyber SO grants permission in this regard.		●	●		
49	After an incorrect password for an administrator account has been entered three times, the account will be blocked until the IT administrator requests this lockout be lifted (see 46). The Cyber SO grants permission in this regard.		●	●	●	●
50	Using group accounts in order to change data in operation-critical applications that do not have Identification, Authentication and authorization mechanisms is not permitted.					●
51	The use of group accounts is not permitted.		●	●	●	
52	Group accounts are permitted under the following conditions: - a group account is only in use if there is a major operational need and the use of personal accounts is very inefficient; - the Cyber SO grants permission for the use of a group account; - the use of a group account can be traced back to a natural person; - the use of a group account via external access is not permitted; - accessing external systems (e.g. the internet) using a group account is not permitted; - processing personal or non-work related information using a group account is not permitted.					●
53	System accounts are permitted under the following conditions: - the use of a system account via external access is not permitted; - accessing external systems (e.g. the internet) using a system account is not permitted; - processing personal or non-work related information using a system account is not permitted.		●	●	●	●
4.5	Password management system					
54	Compliance with the password policy is controlled automatically.		●	●	●	●
55	The password is not displayed on screen when it is entered. No information is shown that can be traced back to the authentication information.		●	●	●	●
56	Reset passwords and initial passwords are unique and are not reused.		●	●	●	
57	Users have the possibility to choose and change their own password. The following applies in this regard: - before a user can change his/her password, the user is authenticated again; - there is a confirmation procedure for the purpose of preventing typing errors in the newly chosen password.		●	●	●	●
58	Passwords are not stored or sent in their original form (plain text).		●	●	●	●

59	If the log-in process is completed successfully, the date and time of the last login or log-in attempt is displayed. This information can provide the user with information about the authenticity and/or abuse of the operating system.		●	●	●	
4.5	Using special system tools					
60	Ports, services and similar tools on the network or computer that are not required are blocked.		●	●	●	●
61	All unnecessary software, services, protocols and accounts are disabled, as well as functionalities such as scripts, drivers, file systems and system tools.		●	●	●	●
62	The security measures prescribed and advised as a minimum by the manufacturer of the equipment have been implemented (Hardening).		●	●	●	●
4.5	Access security for programme source code					
63	Access to the Source Code is limited to protect the code from unintentional changes. Only authorized persons have access.		●	●	●	●
4.6	**Cryptography**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.6	Policy on the use of cryptographic controls					
1	For the Security of an IBP, DISS/ISO-approved cryptographic security provisions, components and procedures are used.		●	●	●	●
2	A Crypto Custodian is appointed. The Crypto Custodian also carries out the tasks as described in the appendix.	Appendix 40	●	●	●	●
3	It is determined with which agreements, laws and regulations the application of cryptographic techniques must comply. This is documented in the Security Plan.		●	●	●	●
4.6	Key management					
4	Key management at least considers the process, the actors, and their responsibilities.		●	●	●	●
5	The period of validity of cryptographic keys is determined according to the intended application and is determined in the cryptographic policy as part of the Security Plan.		●	●	●	●
6	The Confidentiality of cryptographic keys is safeguarded during the generation, use, transport and storage of the keys.		●	●	●	●
7	A procedure has been established which determines how compromised keys will be dealt with.		●	●	●	●
4.7	**Physical Security and Security of the environment**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.7	Secured areas					
1	Systems that contain a large concentration of unclassified or unmarked IBPs are installed in an area that is secured to the IBP-4 level.	Appendix 32				●
2	Systems that contain a large concentration of NLD Restricted IBPs are installed in an area that is secured to IBP-3 level.	Appendix 32				●
3	Systems that contain a large concentration of NLD Confidential IBPs are installed in an area that is secured to IBP-2 level.	Appendix 32			●	
4	Systems that contain a large concentration of NLD Secret IBPs are installed in an area that is secured to IBP-1 level.	Appendix 32		●		
4.7	Installing and protecting equipment					
5	Equipment and cabling is installed and protected in such a way that the risk from outside of damage and failure is minimized.		●	●	●	●
6	TEMPEST measures are taken to prevent emissions from being compromised. The measures are coordinated in advance with DISS/ISO.	Appendix 36	●	●	●	
6.1	In order to prevent emissions, unused power/data cables and separate metal conductors must be removed.	Appendix 36	●	●	●	
6.2	All equipment related to the storage, processing and transport of an IBP is equipped with a feed filter.		●	●		
4.7	Equipment maintenance					
7	Equipment, software and data carriers are installed, used and maintained in accordance with the manufacturer's instructions insofar as this is compatible with the use and maintenance plan of the organization.		●	●	●	●
8	Maintenance is performed on site and is only permitted with the application of procedures approved of by DISS/ISO.		●	●	●	●
4.7	Removal of company resources					
9	Equipment, information and software of the organization may not be taken		●	●	●	●

	from the location without permission being given in advance. The Cyber SO grants permission for IBP-1, IBP-2 and IBP-3 systems. The line manager does so for IBP-4 systems.					
4.7	Secure removal or reuse of equipment					
10	Reusing Company ICT assets is permitted as long as the same IBP is concerned and is deleted using means approved by DISS/ISO. An official report of destruction (deletion) is drawn up.	Appendix 23.2.2	●	●	●	
4.7	Unattended user equipment					
11	When leaving the workstation, the user locks the workstation (clear screen).		●	●	●	●
4.7	"Clear Desk" policy					
12	The "Clear Desk" Policy at least states that the user puts away an IBP in the designated place if the Information is not being used. This information is always kept in a lockable means of storage of the correct IBP level.		●	●	●	●
13	When printing an IBP from a printer in a different area to the workstation, the "secure printing" function is used (e.g. PIN code verification).		●	●	●	●
14	A workstation session is automatically blocked after so many minutes of inactivity: IBP 1 and 2: 5, IBP 3: 10, IBP 4: 15.		●	●	●	●
15	An access security lock is automatically activated when a token is removed (if used).		●	●	●	●
16	When disabling/delaying screen lock for a specific workstation session, the following conditions apply: - screen lock is only turned off/delayed if there is a major operational need to do so; - before screen lock is turned off/delayed, permission must be given by the Cyber SO; - The Cyber SO keeps a workstation/workstation session log including the need for the exemption to be granted.		●	●	●	●
4.8	**Security of business operations**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.8	Documented operating procedures					
1	Operating procedures include current and accurate information regarding turning on, shutting down, backing up, recovery actions, dealing with errors, keeping logs, contact persons, emergency procedures, and special measures for Security, and are available to all users who need them.		●	●	●	●
2	There are procedures for handling data carriers, which detail receipt, storage, Classification, access restrictions, sending, reuse and destruction.		●	●	●	●
3	System components – such as Firewalls, routers, switches, servers – are set up according to standard configuration. This configuration has been determined and is regularly checked for currency.		●	●	●	●
4	The responsibilities and procedures for the adequate administration and correct use of IT assets that process classified information have been determined.		●	●	●	●
4.8	Change management					
5	A change-management process has been set up for IBP systems. This process includes at least the following: - recording significant changes, so activities can be traced back to the natural person; - an impact analysis of possible consequences of the changes; - an approval procedure for changes. The Cyber SO is included in this regard.		●	●	●	●
6	The settings of information security functions (e.g. security software) on the interface between trusted and unreliable networks are automatically checked for changes.		●	●	●	●
4.8	Capacity management					
7	The availability requirement of an ICT asset and the impact of failure is determined on the basis of a risk analysis. Based on this, measures are determined such as automatic mechanisms to accommodate for the failure of (primarily physical) ICT assets, including connections. The ICT assets meet the level of Availability agreed for the services. Provisions have been implemented to safeguard the Availability of components (e.g. checks that a component is present and measurements that determine the use of a component). On the basis of predicted use, action is taken in good time to put into effect any necessary extension to the capacity.		●	●	●	●

8	Restrictions are imposed on users and systems with regard to the use of shared resources to ensure a single user (or system) cannot demand more of these resources than is necessary for his/her task and thus jeopardize the Availability of the systems for other users (or systems).		●	●	●	●
9	At connection points with external or untrusted segments, measures have been taken to signal attacks including DOS/DDOS ((Distributed) Denial of Service attacks) and respond to them. These attacks intend to overload the processing capacity so the computers cannot be accessed or fail.		●	●	●	●
4.8	Separation of development, testing and production environments		-	-	-	-
10	There are separate environments for Development, Testing, Acceptance and Production (DTAP). The systems and applications in these environments do not influence the systems and applications in the other environments.		●	●	●	●
11	There is a physical divide between the development and testing environment on the one hand (DT environment) and the acceptance and production (AP environment) on the other hand.		●	●	●	
12	Users have separate user profiles for the Development, Testing, Acceptance and Production systems to reduce the risk of error. It is clearly visible in which system work is being carried out.		●	●	●	●
13	If there is an experimental or laboratory environment, it is physically separated from the other environments.		●	●	●	●
14	The separation of the Development, Testing, Acceptance and Production systems (DTAP systems) is supported by formal handover procedures.		●	●	●	●
15	Data from the Production environment are only used in the Acceptance environment if it is secured in the same way as the Production environment. This data is not used in the Development or Testing environment.		●	●	●	●
4.8	Measures of control against Malware		-	-	-	-
16	When opening files, these are automatically checked for Malware. The update for the detection definitions is carried out frequently, i.e. at least once a day.		●	●	●	●
17	Incoming and outgoing emails are checked for Malware. The update for the detection definitions is carried out frequently, i.e. at least once a day.		●	●	●	●
18	Files on file systems, whether server-based or host-based, are automatically scanned for Malware. Upon the detection of Malware, these files are placed in quarantine.		●	●	●	●
19	Anti-Malware software from several different suppliers has been applied to various links of the chain within the infrastructure of an organization.		●	●	●	●
20	Measures have been taken to combat the spread of Malware and thus limit the damage (e.g. quarantine and Compartmentalization)		●	●	●	●
21	There are continuity plans for recovery after Malware attacks in which minimum measures for back-ups and recovery of data and software are described.		●	●	●	●
22	Users check all digital data carriers obtained from external parties or used by external parties using special Scrubber functionalities set up for this purpose.		●	●	●	●
23	Deviations from the norm (anomalies) regarding perimeter-device sessions are investigated for threats such as “covert channels”. There is constant Monitoring for unusual creations and the presence and/or termination of processes for the purpose of detecting infiltration.		●	●	●	●
4.8	Back up of information		-	-	-	-
24	Tested procedures are in place for back-up and recovery of information to re-establish processing and correct errors.		●	●	●	●
25	Back-up strategies are determined on the basis of data type (files, databases, etc.), the maximum permitted period for which data may be lost, and the maximum permitted back-up and recovery time.		●	●	●	●
26	A log is kept of back-up activities and the location of data carriers.		●	●	●	●
27	Back-ups are kept at a location that has been chosen on the basis of the fact that an incident at the original location will not damage the back-up.		●	●	●	●
28	The physical and logical access to back-ups, of both system drives and data, is arranged in such a way that only authorized persons can gain access to these back-ups.		●	●	●	●
29	Back-ups are secured in accordance with the highest Classification of the data.		●	●	●	●
30	Back-ups are saved at least a year and are kept for no longer than the duration of the project.		●	●	●	●

4.8	Registering events		-	-	-	-
31	Per system events are recorded in the Log. See the appendix for the information to be recorded. Any additional information to be logged is determined on the basis of a risk analysis. This Log may be context specific. The results of the analysis are included/recorded in the Security Plan.	Appendix 33	●	●	●	●
32	The threshold values for alerts and alarms are generated.	Appendix 33	●	●	●	●
33	Monitoring of log storage: if the capacity of means of storage for log files exceeds a certain amount, the IT administrators are alerted automatically. This also applies if saving log data is not or is no longer possible (e.g. because a log server cannot be accessed/is no longer available).		●	●	●	●
4.8	Protecting information in log files		-	-	-	-
34	If log files are overwritten or deleted (either automatically or manually), this is logged in a newly created log.		●	●	●	●
35	Only IT administrators can consult log files. Their access is restricted to reading rights only.		●	●	●	●
36	Log files are protected in such a way that they cannot be changed or manipulated.		●	●	●	●
37	The settings of logging mechanisms are protected in such a way that they cannot be changed or manipulated. If the settings have to be changed, two people are present when the changes are made (four-eye principle).		●	●	●	●
38	The Availability of log information is safeguarded for the period for which the log analysis is considered necessary and for at least three months.		●	●	●	●
39	Log data about an incident or suspected incident is kept for five years.		●	●	●	●
40	Log data has at least the Classification of the information that it corresponds to.		●	●	●	●
4.8	Clock synchronization		-	-	-	-
41	System clocks are synchronized in such a way that a reliable analysis of log files is possible at all times.		●	●	●	●
4.8	Software installation on operational systems		-	-	-	-
42	Only authorized IT administrators can install or activate functions and software.		●	●	●	●
43	Software is not installed on a production environment until a formal test and the acceptance procedure have been completed.		●	●	●	●
44	Only software (or versions of the software) maintained by the Supplier is used.		●	●	●	●
45	There is a roll-back strategy.		●	●	●	●
46	There is an integrity control mechanism to ensure the continuity of the Integrity of the software and system files.		●	●	●	●
47	Unauthorized software is detected.		●	●	●	●
4.8	Management of technical vulnerabilities		-	-	-	-
48	A process has been set up for detecting and mitigating technical vulnerabilities which at least includes penetration tests, risk analyses of vulnerabilities, and patching.		●	●	●	●
49	Checks are carried out to determine whether the latest updates (patches) have been installed for the software of the Technical Infrastructure. Updates are not installed automatically, unless special agreements have been made with the Supplier in this regard.		●	●	●	●
50	Critical (security) updates and (security) patches are installed as soon as possible.		●	●	●	●
51	The use of a TOR (The Onion Router)/Darknet web browser is not permitted.		●	●	●	●
4.9	**Communication security**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.9	Networks controls		-	-	-	-
1	Networks have routing controls based on mechanisms for the verification of source and destination addresses.		●	●	●	●
2	Technical measures are in place to prevent internal network address being routed externally.		●	●	●	●
3	The use of wireless communication is not permitted.		●	●	●	
4	The use of wireless communication is permitted with the application of DISS/ISO-approved procedures and assets.					●

5	In the case of an external connection, a “Demilitarized Zone” (DMZ) is applied. In the DMZ, Monitoring systems are set up that at least monitor and log Packet Header information and preferably the full packet headers and payload of the data traffic.					●
6	Only identified and authorized equipment is connected. The safeguarding hereof is described in the Security Plan.		●	●	●	●
7	All TOR (The Onion Router)/Darknet traffic is blocked.		●	●	●	●
8	On the basis of a risk analysis, limit the internal and external data traffic to only the necessary protocols and sessions.		●	●	●	●
9	The network is monitored and managed in such a way that attacks, disruptions and errors are detected and can be repaired and that the Availability of the network does not drop below the agreed minimum.		●	●	●	●
10	Networks are monitored for unauthorized connections.		●	●	●	●
11	On the instruction of DISS/ISO, cooperation is extended for the following: - the installation of monitoring boxes; - the monitoring of network traffic and hosts by means of monitoring boxes.		●	●	●	●
4.9	Security of network services		–	–	–	–
12	In the case of an external connection, network-based IDS (intrusion detection system) or IPS (intrusion prevention system) Monitoring is applied.					●
13	A network-based IDS or IPS contains up-to-date Signatures.					●
14	A filter is installed for outgoing data traffic.					●
15	A DMZ Proxy Server and/or sandbox has been applied for incoming and outgoing data traffic to and from an insecure environment.	Appendix 35				●
4.9	Network separation		–	–	–	–
16	A network on which an IBP is saved is not connected to another network unless DISS/ISO-approved procedures and assets are applied.		●	●	●	
17	The Technical Infrastructure is divided into segments. A record is kept of which systems are installed in which segment. There is a periodic evaluation, i.e. at least once a year, of whether the system is still in the optimal segment or whether it should be moved.		●	●	●	●
18	Workstations are set up in such a way that it is not possible to route traffic between different segments and networks.		●	●	●	●
19	Information that is transferred between networks and systems may contain Malware and is potentially unsafe. Measures have been taken to avoid contamination.		●	●	●	●
20	Each segment has a defined classification level. When transferring between segments, checks are carried out with regard to protocol, content and the direction of communication.		●	●	●	●
21	Segments are managed and audited from a separate segment that is at least logically separate.		●	●	●	●
22	Segmenting is set up with provisions of which the functionality is limited to what is strictly necessary.		●	●	●	●
23	The network is segmented (Compartmentalized) on the basis of the principles “Need-to-be”, “Need-to-know” and “least privilege”.		●	●	●	●
4.9	Policy and procedures for information transport		–	–	–	–
24	All IBPs that are not in the designated physical compartment are encrypted. The Encryption to be applied has been approved by DISS/ISO.		●	●	●	●
25	An IBP is only sent over an insecure connection when DISS/ISO-approved Encryption is applied.		●	●	●	●
26	Incoming software (both on physical media and downloaded) is checked for unauthorized changes (integrity control) using a checksum or certificate delivered by the Supplier through a separate channel.		●	●	●	●
27	Accessing an IBP on a network between various company locations (WAN) is not permitted.		●			
28	Accessing an IBP on a network between various company locations (WAN) is only permitted if the connection between the locations has DISS/ISO approved Encryption.			●	●	●
4.9	Cloud computing		–	–	–	–
29	The use of a public Cloud service (computing, storage, transport) is not permitted.		●	●	●	●
30	The use of a Private Cloud Service (computing, storage, transport) is permitted.					○

31	Private Cloud services (computing, storage, transport) will be carried out on Dutch territory, at a Dutch legal entity and by personnel with the Dutch nationality.					○
4.9	Virtualization		–	–	–	–
32	A risk analysis is carried out when applying virtualization. The following conditions apply in this regard: - security functions run on physically separate virtualization platforms; - only system components that have the same classification level are combined; - the design and implementation has been approved by DISS/ISO.	Appendix 34	●	●	●	●
33	The application of VLANs is only permitted on networks with the same classification level. The design and implementation has been approved by DISS/ISO.	Appendix 34	●	●	●	○
4.10	**Acquisition, development and maintenance of information systems**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
1	Security risk analyses and measures of control are included in projects as part of the design. In the case of changes to the design, the consequences for security are taken into account. These fall under Change and are checked for currency annually.		●	●	●	●
2	The connections between Company ICT assets are set out on a network drawing.	Appendix 27	●	●	●	●
4.10	Principles for engineering secured systems		–	–	–	–
3	Checks are carried out on data entry, including at least checks of limit values, invalid characters, incomplete data, and data that does not comply with the format requirements and inconsistent data.		●	●	●	●
4	The Information system contains functions that can determine whether data is correctly processed, that is to say an automatic check, whereby (obvious) transaction and processing errors can be detected.		●	●	●	●
5	The output functions of programmes makes it possible to determine the completeness and accuracy of the data.		●	●	●	●
4.10	System acceptance tests		–	–	–	–
6	A log is kept of acceptance tests.		●	●	●	●
7	Acceptance criteria have been determined for testing the Security.		●	●	●	●
8	Before systems and/or components are taken into production, test data and test accounts are deleted.		●	●	●	●
9	Acceptance of systems/software takes place after it has been determined that the ABDO security requirements have in fact been implemented.		●	●	●	●
4.11	**Suppliers**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.11	Information security policy for suppliers		–	–	–	–
1	If an external party is involved in the management of an IBP environment, an ABDO Authorization has been issued for this party by DISS/ISO.	Appendix 8	●	●	●	●
2	If data storage of an IBP is facilitated by an external party, an ABDO Authorization has been issued for this party by DISS/ISO.	Appendix 8	●	●	●	●

5 Explanation of abbreviations and terms used

ABDO	General Security Requirements for Defence Contracts. Regulations for the adequate Security of Interests to be Protected and Special Information in particular that is entrusted to a party external to the civil service.
APT	Advanced Persistent Threat. A long-term, complex and targeted digital attack with espionage as its purpose.
Authentication	The process that verifies whether a person, (other) computer or application is in fact who/what he/she/it claims to be.
Authorization	The process that assigns rights to a person, (other) computer or application to access a site, building, system, data file, etc.
Availability	The guarantee that within their role authorized users or systems have timely access to information and corresponding company resources at the correct moments in time.
Baseline	A set of technical administrative measures or settings for the set-up of an IT resource without taking into consideration the requirements of a specific IT service. A baseline serves as a point of departure for the security standards of specific IT services.
Blacklist	A list of domains or IP addresses, for example, with which no digital communication is permitted.
Building(s)	Buildings, constructions or engineering structures produced or realized by humans.
BYOD/CYOD	Bring Your Own Device. The possibility for an employee to use their own device for commercial applications. Choose Your Own Device. The possibility for an employee to choose from a number of devices offered by the employer.
CA/RA	Certificate Authority. The CA safeguards the integrity and authenticity of certificates, and guarantees the identity of the holder of the certificate. Registration Authority. The RA determines to whom certificates can be awarded and oversees their issue.
CCTV	Closed Circuit Television. A closed system of cameras as a tool to prevent or process incidents.
Central Government	The Central Government, as part of the government of the Netherlands, is the administration at national level and is formed by all ministries and implementation organizations that fall under the responsibility of a minister.
CGC	Certificate of Good Conduct (Verklaring Omtrent Gedrag; VOG). A declaration issued by Justis, the Ministry of Justice Agency for Scrutiny, Integrity and Screening, needed for access to or cognizance of information at NLD Restricted level.
Change	Every addition, change or removal regarding an IT service or IT resource.
Civil Service	The ministries and their directorate-generals, central departments, staff departments, external departments, and internal private public services.
Classification	The establishment and indication that an IBP is Special Information or contains Special Information, and the determination or indication of the degree of security thereof.
Classified Contract	A Defence contract whereby Special Information must be made known to an external organization or is generated.
Clear Desk Policy	Unlike the Clean Desk Policy whereby the desk is completely empty, the Clear Desk Policy means that no confidential information is on the desk.
Cloud Computing	Making available on request hardware, software and data via a network.
CNO	Certificate of No Objection (Verklaring van Geen Bezwaar; VGB). The declaration that from the point of view of national security there is no objection to appointing a specific person to a specific Confidential Position.
Code Security Review	Software that supports the search for errors in the source code of software.
Command & Control (C2) Server	Infrastructure (servers and other components) used as a target to spread Malware and/or to direct it, in particular botnets and APTs.
Company ICT Resource	A (physical or logical) technical resource (such as hardware, software, application or facility) with which an IT service is realized wholly or partially and directly or indirectly.

Company Resource	All resources on which or using which company information can be stored and/or processed and with which access to buildings, work areas and ICT facilities can be gained: an operational process, a defined group of activities, a building, a piece of equipment, an ICT facility or a defined set of data.
Compartmentalization	The allocation and securing of (usually partitioned-off) physical or digital locations where an IBP is permitted to be processed or stored, as well as the allocation of the persons or groups of persons who may access or take cognizance of an IBP.
Compromise	The unauthorized access to or cognizance of an IBP, usually SI.
Commissioning Party	(The Kingdom of The Netherlands for) the Central Government or a natural or legal person or a foreign body that commissions a Special Contract (SC).
Conditional Authorization	The declaration from DISS/ISO for the Commissioning Party stating that from a security point of view there is no objection to a company being a Contractor candidate.
Confidentiality	The safeguard that information is only accessible to those authorized.
Confidential Information	Information that must not be made generally known (source of Dutch definition: Van Dale). Within the framework of the Netherlands Civil Security Data Security Baseline 2012 (Baseline Informatiebeveiliging Rijksdienst 2012; BIR), compliant measures are described for the handling of classified information up to NLD Restricted (according to the definition in the Netherlands Civil Service Information Security (Classified Information) Decree 2013 (Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013; VIRBI 2013)) and personal and confidential information in risk classes 1 and 2 as defined in the explanatory notes to the Netherlands Personal Data Protection Act Background Studies and Surveys 23 (Wet bescherming persoonsgegevens achtergrond studies en verkenningen 23; WBP: AV32).
Confidential Position	A position that in principle affords the opportunity to damage the security or other important interests of the State.
Configuration Item (CI)	IT resource that is important for the provision of an IT service.
Configuration Management Database (CMDB)	A structured set of information (database) of relevant details of configuration items and information about how they relate to one another.
Contractor	A natural person or a legal entity (a legal person as referred to in Book 2 of the Dutch Civil Code (Burgerlijk Wetboek; BW) or a partnership as referred to in Book 7A of the Dutch Civil Code, or a commercial partnership or a limited partnership as referred to in Book 1, Title 3 of the Dutch Commercial Code (Wetboek van Koophandel) that is involved in a Defence Contractor has received and accepted a Defence Contract, as well as third parties after they have been involved in the execution of such a contract.
Control	“Control” is understood to mean the possibility to exert influence on the policy of an organization on the ground of actual or legal circumstances. Having relevant influence on the policy of an organization can arise from financial, organizational and formal ties (power of appointment, voting shares), direct or indirect ties (subsidiary companies and sister companies), cooperation in a group, or informal cooperation ties.
Controllability	The extent to which reality or representations thereof can be tested, that is to say can be compared to other “realities or representations thereof”, so it is possible to form an opinion objectively.
COTS	Commercial Off The Shelf. A term to indicate commercial goods and services that are directly available in the private sector.
Crypto Position	A confidential position is a position in which it is necessary to handle or take cognizance of materiel marked CRYPTO, CRYPTO SECURITY or CRYPTO CONTROLLED ITEM (CCI).
CUI	Controlled Unclassified Information/Item. A category of information or goods that require a certain degree of security under the American ITAR framework despite being unclassified.

Cyber	The term Cyber refers not only to the IT infrastructure, but also the system of activities (including business operations) that is made possible by the infrastructure. It is these activities that must be protected. Often used as a prefix for further specification of terms (such as cyber-crime, cyber security, cyber threat).
Darknet	Part of the World Wide Web of which the content is only accessible with the aid of specific software (browser) and/or configurations.
Declaration of awareness of the duty of secrecy	The declaration in which one declares to be familiar with the provisions and obligations with regard to dealing with an IBP, and SI in particular.
Defence Contract	A contract agreed between (the State of the Netherlands for) the Ministry of Defence or a foreign Defence body on the one hand and a natural or legal person on the other hand, whereby the transfer or handling of Information, Materiel, Goods or Buildings takes place.
Definitive Authorization	The declaration from DISS/ISO for the Commissioning Party stating that from a security point of view there is no objection to an SC being awarded to the selected Contractor.
Delay Time	The time between detection/verification of an intrusion and an IBP being compromised.
Digital Signature	A digital signature is a method for confirming the accuracy of digital information by means of cryptographic techniques. The electronic signature consists of two algorithms: one to confirm that the information has not been changed by third parties, the other to confirm the identity of the person “signing” the information. The techniques are applied with the help of a PKI.
Disclosure	The disclosure of an IBP, whereby it is made available or known to one or more third parties.
DISS	Defence Information and Security Service (Militaire Inlichtingen- en Veiligheidsdienst; MIVD) that is responsible for national security.
DISS/ISO	The Industrial Security Office (ISO) (Bureau Industrieveiligheid; BIV) of DISS that oversees on behalf of the Ministry of Defence the security of IBPs at Contractors and their subcontractors.
DMZ	Demilitarized zone. A physical or logical part of the network that contains the external services of an organization that can be accessed via the Internet without the internal services and workstations being accessed (such as email- and webservers).
Document(s)	Everything in which information is recorded for consultation (e.g. letters, notes, reports, memorandums, messages, telegrams, drawings, photos, footage, maps, tables, notebooks, stencils, magnetic and optic data carriers, etc.).
DoS/DDoS	Denial of Service. Making a computer, computer network or service unusable by overloading the broadband, memory or processing capacity. Distributed Denial of Service. A DoS attack is carried out from several computers at once.
DSP	The Defence Security Policy as described in Directive SG/003 (Aanwijzing SG/003).
EACS	Electronic Access Control System.
Employee holding a Confidential Position	A person who has been appointed to a confidential position.
Encoding	See Encryption
Encryption	Changing information using an algorithm so it becomes illegible and incomprehensible to non-authorized persons.
Escrow agency	A reliable third party at which keys or a Source Code are stored.
EU	European Union.
Facility Security Clearance	Facility Security Clearance (FSC) (FSCC Certificate).The declaration by DISS/ISO for a (usually foreign) applicant that a company is capable of performing the SC from a security point of view.
Firewall	All software and any hardware provisions that prevent unwanted traffic from one network zone from accessing another, in order to increase the security of the latter.
FTP	File Transfer Protocol. A protocol that facilitates the exchange of files between computers.

GISS	General Information and Security Service (Algemene Inlichtingen- en Veiligheidsdienst; AIVD) that is responsible for national security with State security on behalf of the Minister of the Interior and Kingdom Relations.
Goods	All materiel and intangible goods (products and services) that can be used to meet a need.
Hardening	The process of securing a system by reducing the possibilities in the system for an attack. This is achieved by, among other means, disabling superfluous functions in operating systems and/or deleting them from the system and set security settings to values that create maximum security.
Honeypot or Honeynet	A computer system or network that is intentionally made vulnerable to worm viruses and other viruses and attacks so the attacker and/or its properties become perceptible.
Hypervisor	A set-up (software) that serves to enable several operating systems to run on a host computer at the same time.
IBP	Interest to be Protected. All Information, Materiel, Goods and Buildings that require a certain degree of protection are divided up by the Ministry of Defence into four categories of Interests to be Protected (IBP 1 to IBP 4, where IBP 1 is the most highly protected category).
Identification	Making known the identity of a subject (a user or a process).
IDS(S)	Intrusion Detection and Signaling (System).
Incident	The term incident includes all events that are not part of the standard operation of an IT service and that can cause an interruption to or a reduction in the quality of that service. The term incident does not include requests from the user for support or the provision of information, advice or documentation (also referred to as “Service Request”).
Information	Knowledge that is transferable in any form whatsoever. This includes both Documents and materiel on which knowledge can be stored or from which knowledge can be derived.
Information security	The process of determining the required reliability of information processing in terms of confidentiality, availability and integrity, as well as meeting, maintaining and monitoring a comprehensive package of associated measures.
Information system	A comprehensive system of data sets and the associated persons, procedures, processes and software, as well as the provisions in place for storage, processing and communication provisions for the information system.
Integrity	The safeguarding of the accuracy, completeness and timeliness of information and the processing thereof.
Intelligence and Security Services Act	The Netherlands Intelligence and Security Services Act (Wet op de inlichtingen- en veiligheidsdiensten; Wiv) as published in 2002 (see Bulletin of Acts and Decrees 2002, 148) or its legal successor.
Intervention	Intervention is the response to an alarm (suspected breach of an IBP) with the intention to verify the alarm and if necessary stop the breach of the IBP or secure the IBP. This therefore concerns all measures and/or activities with the purpose of preventing or repairing damage to the security level of an IBP.
Intervention Time	The time between detection/verification of an attempt to intrude and the intervention by security, police or Defence personnel on site.
Introspective Capacity	The capacity of an IDS to assess the legitimacy of the internal activities of a system (network) and to take action if necessary.
IP address	Internet Protocol address. A numeric label given to a device (e.g. computer, printer) that is part of a network that uses the Internet Protocol for communication.
IRP	Incident Response Procedure. A procedure that states the steps that must be taken during the investigation and sign-off stages if an Incident is reported.
ITAR	International Traffic of Arms Regulations.
LoCP	List of Confidential Positions. The list of the number of Confidential Positions divided into position category and Security Authorization Level.
Logging	Recording data that relates to access or attempted access (either physical or digital) to an IBP.
Malware	Software with undesirable/damaging functions, such as viruses and Trojans.
Marking	Indication on an IBP that entails a specific manner of handling and restriction of distribution.

Materiel	The necessaries of the armed forces such as weapons, ammunition, vehicles, etc., regardless of whether they are intended for use or consumption.
Memorandum of Understanding	See Security MoU.
MISWG	Multinational Industrial Security Working Group. An informal form of cooperation regarding Industrial Security.
Mitigation	The minimization of the impact of a compromised IBP, especially digitally.
Monitoring	Measuring data flows and activities in a network via digital ports.
NAT	Network Address Translation is an umbrella term for techniques that are used for screening off private IP addresses from the outsider for whom only the publicly known IP address is visible.
NATO	North Atlantic Treaty Organization.
Need-to-Be	An employee holding a Confidential Position only has physical access to work areas and locations where Vital Information is available if this is necessary for carrying out his/her duties. Employees not holding a Confidential Position never have access.
Need-to-Know	An employee holding a Confidential Position may only take cognizance of Special Information if that is necessary for carrying out his/her duties. In addition, he may not share this knowledge with colleagues for whom this knowledge is not necessary and/or do not hold a Confidential Position.
Network Perimeter Devices	Devices that ensure the security, access, transmission or receipt of data at the perimeter of the trusted network.
Network Segmentation	The splitting up of a network into smaller coherent parts for the purpose of preventing larger parts of the network from being compromised by a malicious action.
NLD R	NLD Restricted (Departmentaal Vertrouwelijk; DV) information is Special Information with the lowest possible classification. NLD R is not classified as State Secret but does require a certain level of security.
NLNCSA	The Netherlands National Communication Security Agency (Nationaal Bureau Verbindingsbeveiliging) provides the Central Government with primarily technical means (cryptography) for the security of Special Information.
Packet Headers	Data that is placed at the start of a digital block that is necessary for the interpretation of the data to be transported.
Partner	Partner refers to: - the husband, wife or registered partner of the individual in question; - the person with which the individual in question shares a household, unless this person is a blood relative in the first or second degree; - the person with whom the individual in question has an affective - relationship as found by the security screening, unless this person is a blood relative in the first or second degree.
Patch	A piece of software that the software supplier issues to repair errors in software produced by it.
The Penal Code	The Netherlands Penal Code (Wetboek van strafrecht; Wvs) that contains the Netherlands penal law that applies to everyone that commits a criminal offence in the Netherlands.
Penetration test	A test of the vulnerabilities of one or more computer systems with the aim to better secure the systems.
Personal Information Form	Personal Information Form on the basis of which a Security Screening will be carried out.
Phishing	An attempt to cheat people out of information by enticing them to a fake website that is a copy of a known existing website. To this end, the attacker pretends to be a trusted body or person, often by means of an e-mail with infected files.
PKI	PKI (Public Key Infrastructure) supports the issue and management of digital certificates. PKI gives users additional guarantees on information exchanged via networks. The guarantees given by a PKI provide greater certainty for the sender and receiver of exchanged information.
Private cloud service	A form of cloud computing whereby information is made available to the contractor on specifically designated (usually isolated) hardware and/or software.

Privileged Accounts	A user account that has additional rights, such as: - Administrator accounts, - Service accounts, - Emergency accounts, - Change accounts, - Group accounts.
Proxy	A computer system or application that functions as an intermediary between workstation requests and server resources.
PSC(C)	Personnel Security Clearance (Certificate). The declaration that a person is authorized to access or take cognizance of an IBP and SI in particular.
PSI	Project Security Instruction. A Document in which further security requirements are determined, usually in the context of a foreign contract.
Reliability	The extent to which the organization can rely on an information system for its information provision. (Civil Service Data Security regulation 94 (Voorschrift informatiebeveiliging rijksdienst; VIR))
Remote Administration	Administration activities performed externally on equipment internal to the organization.
Remote Maintenance	Maintenance activities performed externally on equipment internal to the organization.
Removable data carriers	Means of storage that can be removed from equipment and taken away, such as CD-ROMS, USB sticks, removable disks, tapes or printed media.
RfV	Request for Visit. A request to the relevant security authorities for permission to visit a Ministry of Defence location or a company abroad.
SAL	Security Aspect Letter. A Document in which further security requirements are determined, usually in the context of small foreign projects.
SC	Special Contract. A contract that involves an IBP with the government as the Commissioning Party and a civilian party as the Contractor.
SCL	Security Clearance Level. The required level at which the Security Screening must be carried out for the Confidential Position (A, B or C).
Screening	See Security Screening.
Scrubber	A standalone system that monitors information carriers for the presence of Malware and where necessary renders them harmless.
Securing	The protection of an IBP and SI in particular from access or cognizance by non-authorized parties.
Security	Information security in the broadest term of the word, i.e. including physical security, Business Continuity Management (BCM) or availability of business processes and personnel security and integrity.
Security Briefing	The provision of information intended to increase security awareness.
Security Covenant	A bilateral covenant that facilitates the exchange and mutual protection of classified information between two countries.
Security Incident	A security incident is a real or suspected event that could lead to or has led to a disruption of the usual course of affairs regarding integral security, as a result of which the State and/or one or more ministries and/or employees thereof, external parties and/or visitors are in danger or could be in danger.
Security MoU	Memorandum of Understanding. A bilateral agreement between parties in which mutual security agreements are determined.
Security Officer	Security Officer (SO). The employee tasked with implementing and performing the prescribed security measures.
Security Plan	The total of all security measures, and/or their locations, which apply to an information system or area of responsibility.
Service Provider	A company that provides services. The term service provider is often associated with internet and telephony services.
Security Screening	The process that results in the issue, denial, extension or retraction of a CNO.
Security Screening Act	The Netherlands Security Screening Act (Wet veiligheidsonderzoeken; Wvo) as published in 1996 (see Bulletin of Acts and Decrees 1996, 525) and amended in 2015 (see Bulletin of Acts and Decrees 2015, 208).
Security Standard	As set of technical management measures or settings for the set-up of an IT resource for a specific IT service.
SG	The Secretary General of the ministry in question.

Signatures	Properties of Malware on the basis of which it can be recognized.
Social Engineering	The collection of information from communication under false pretences, whereby advantage is taken of the other person's intrinsic motivation to be helpful, with the intention to gain access to an IBP and SI in particular.
Source Code	A computer programme in readable form as written by the programmer in a programming language.
Span Port	A physical port on an active component (router or switch) that makes it possible to make a diagnosis on a piece of equipment or network traffic.
Special Information	State secrets or other special information of which cognizance by non-authorized persons could disadvantage the interests of the State, its allies or one or more ministries. Special Information (SI) is information that has a Classification and must be secured for that reason.
SRC	Security Requirements Checklist. A list that indicates by subject the classification of the relevant IBP in the context of an SC.
State Secret	Special Information which is subject to secrecy because of the interest of the State or its allies.
Statement of Personal Details	Statement of Personal Details on the basis of which the Security Screening will be carried out.
Subcontractor	A company to which the Contractor outsources specific work on an IBP.
Supplier	A company that supplies goods or services in exchange for money.
Sub-supplier	A company that supplies goods to another company that in turn processes these Goods into a product for the end user.
Technical Infrastructure	All ICT facilities for general use, such as servers, firewalls, network equipment, operating systems for networks and servers, database management systems and management and security tools, including corresponding system files.
TEMPEST	The combating of possible compromising emissions of electronic systems that could lead to the unauthorized receipt, processing and reproduction of data.
Trusted	In conformity with a security level set by a competent authority. For example, trusted zones or trusted networks.
Two-factor Authentication	Two-factor authentication requires the use of two of the following three authentication methods: 1. Something that the user knows (e.g. password, PIN); 2. Something that the user has (e.g. access pass, key); and 3. Something that the user is (e.g. biometric information such as a fingerprint).
unPrivileged accounts	A user account that has limited rights, for example: - User accounts
virtualization	The creation of a computer system virtually rather than as a combination of hardware and software, whereby computers, operating systems, data storage systems and other active components work together virtually.
Vital	The term with which a contract is marked if it involves an IBP that would negatively impact the operations of the State, the Ministry of Defence or its allies if it were compromised. A Vital Contract can be Classified.
VPN	Virtual Private Network. An encrypted connection between two systems, whereby the integrity and confidentiality of the data remains safeguarded.
Watering Holes	A strategy whereby an attacker infects a website with Malware after having ascertained that a certain group of users regularly visits the website.
WAN	Wide Area Network. A term for the connection of Local Area Networks (LAN) over an urbanized area or larger geographic area.
Zero Day	A (usually unintended) vulnerability in software that is not yet known to the software developer or others. A Zero-Day exploit is software that takes advantage of this kind of vulnerability in software.
Zone	The logical set of ICT facilities with the same security level that can exchange information via secure interfaces.

Index

Appendix 0

Appointment of companies in the context of a Defence contract to which the ABDO applies.

DISS/ISO contacts the potential Contractor at the request of the following applicants:

1. a Defence procurement officer or project leader (preferably via the Security Coordinator) or;
2. a foreign Defence organization (bilateral, NATO, EU) or;
3. an established Contractor that wants to outsource activities or supplies to a Subcontractor in the context of an Special Contract (SC). In this situation, the Contractor takes on the role Commissioning Party and the Subcontractor the role of Contractor.

NB: DISS/ISO will not contact a potential Contractor if this is at the request of a company that wants to gain an ABDO authorization in order to be considered for an SC. An exception may be made for NATO or EU calls for tender which require a Facility Security Clearance (FSC) in advance.

A Contractor to which an SC is granted must comply with the ABDO 2019. The ABDO 2019 is stipulated in the contract terms between the Ministry of Defence and the Contractor. The declaration that a Contractor complies with the ABDO 2019 is issued per SC to the applicant and the Contractor in the form of an (conditional) ABDO authorization or a Facility Security Clearance Certificate (FSCC)[1]. The applicant must receive this authorization or FSCC from DISS/ISO before a Contractor is issued an IBP in any form. The authorization is issued per contract and does not relate to doing business with a specific company in general[2].

The process that leads up to the award of an SC to companies by the Ministry of Defence, whereby one or more IBPs are entrusted to those companies and/or are commissioned to be generated at those companies, is divided into three stages: the orientation stage, the negotiation/quote stage and the award stage.

Orientation stage
During the orientation stage, the special nature of the contract should be determined as early as possible. To this end consultations are held between the requisitioner, the applicant, the procurement officer (the Commissioning Party), the project leader, the Security Coordinator and, if necessary, the Security Authority (SA). In addition, the applicable marking, IBP category and/or classification level will be determined as well as the security level from the ABDO 2019 to be included in the contract.

Subsequently, a Security Requirements Checklist (SRC, Appendix 7) is drawn up, on the basis of which the applicant provides information about the nature of the contract to be given and, if applicable, the marking, the IBP category and/or the classification level.

Before contact is made with potential Contractors, the applicant reports its intention of orientation to the Security Coordinator and indicates which companies may be considered for being approached by the Commissioning Party in the orientation stage.

The Security Coordinator can provide this list of companies to DISS/ISO for an administrative check. DISS/ISO has the possibility of issuing advice to exclude a company from the follow-up process.

Negotiation stage (quote stage)
After the orientation stage, the number of companies invited for further negotiations, or to submit a quote, is limited. If an applicant has selected a potential Contractor to submit a quote for an SC and the potential Contractor should have available, or be able to examine, Special Information (SI) during the quote stage, the applicant reports this to DISS/ISO in advance using the form 'Request for authorization of natural or legal persons for classified Defence contracts' ('Aanvraag voor autorisatie van natuurlijke of rechtspersonen voor gerubriceerde defensieopdrachten'). These companies will be visited by DISS/ISO for an inspection of the state of affairs regarding security. The required (additional) security measures and the level thereof for the possible final award of the contract are discussed with the company on the basis of the ABDO 2019.

[1] A FSCC is not a general or permanent authorization and can be withdrawn if the necessary security requirements are not in place.
[2] The applicant is responsible for informing the contractor about the issued authorization.

It may be necessary for a potential Contractor to require an IBP as early as the negotiation stage. Before an IBP is provided to potential Contractors during the negotiation stage, DISS/ISO must have issued a "conditional authorization" to the applicant and to the potential Contractor. In this case, an FSCC could also be issued as the FSCC is solely used during the negation stage to demonstrate that a facility/installation/location complies with the standardization of the ABDO 2019 up to, and including the level of classification as detailed in the FSCC. If during this stage an IBP will only be examined at a Defence site and there are no IBPs on the company site, the conditional authorization will be issued to the applicant after:

- DISS/ISO has carried out an investigation into the selected companies;
- (in the case of an NLD Restricted IBP) the employees have submitted a Certificate of Good Conduct (CGC) and signed statement of non-disclosure;
- (in the case of an NLD Confidential IBP or a higher classification), DISS/ISO has determined a conditional List of Confidential Positions (LoCP, see Chapter 5 Personnel) and the relevant employees of the company have received a Certificate of No Objection (CNO) and have signed a statement of non-disclosure.

In addition, if an IBP is needed at the company site during this stage, the company site will be investigated in more detail by DISS/ISO with regard to:

- security organization and procedures;
- physical security;
- digital security.

If the ABDO investigation is completed successfully, DISS/ISO issues a conditional authorization to the applicant, which entails permission to share an IBP with the potential Contractors in question. Should the investigation conclude a lack of one or more (safety) guarantees, DISS/ISO reserves the right to issue a negative advice regarding authorization. In the event a company is unwilling or unable to comply with the ABDO 2019, the applicant will be sent a refusal of the requested authorization.

If the quote does not lead to a contract, the applicant will ensure that no IBPs remain on the company site. Any LoCPs and CNOs are nullified.

Award stage and execution of the contract

If the Ministry of Defence wishes to issue an SC to a potential Contractor whereby this Contractor ought to receive and/or examine only until after being awarded the contract the applicant reports this in advance to DISS/ISO using the form 'Request for authorization of natural or legal persons for classified Defence contracts' ('Aanvraag voor autorisatie van natuurlijke of rechtspersonen voor gerubriceerde defensieopdrachten'). The selected Contractor is subjected by DISS/ISO to a comprehensive security inspection at the concerned company site(s) and a definitive LoCP is drawn up. Following the successful completion of the Security Screening, a CNO is issued to the relevant employees involved in the contract. The definitive authorization is subsequently issued to the applicant and the potential Contractor, whereby DISS/ISO declares that from a security point of view there is no objection to the SC being awarded to the selected Contractor. When awarding the contract, the ABDO 2019 must be stipulated in the contract itself and must include the required security level. This authorization:

- will not obligate the State to a (subsequent) contract;
- will not be disclosed to third parties without written permission from DISS/ISO;
- will not be used for promotional purposes or advertisements without written permission from DISS/ISO.

With regard to security aspects, DISS/ISO maintains contact with the Contractor during the execution of the contract for as long as necessary afterwards.

Termination of the contract and bankruptcy

Upon termination of the contract all associated authorizations, all CNO's and the LoCP cease to be valid. If the Contractor executes an additional SC, the LoCP is amended and the applicable CNOs remain valid.

Prior to termination of the contract (or bankruptcy), the Contractor will return the IBP provided by the Commissioning Party unless the Commissioning Party, in consultation with DISS/ISO if applicable, has issued written consent to destroy or retain the IBP. If necessary, DISS/ISO can at the request of the Commissioning Party check whether all relevant IBPs have been returned, destroyed or, with the permission of the Commissioning Party been retained by the Contractor. The Contractor provides DISS/ISO with a detailed statement in this regard. IBPs generated by the Contractor that may also relate to other (inter)national SCs may be retained with the permission of the Commissioning Party, provided the correct security requirements can be adhered to.

In the event a Contractor is formally declared to be in a state of bankruptcy, all confidential positions, CNOs, the LoCP as well as all applicable authorizations will consequently expire.

Finally, employees involved are debriefed by the Security Officer (SO) of the Contractor, whereby the continued obligation of secrecy as well as possibly other relevant security matters will explicitly be pointed out.

Appointment of a foreign company

Permission from DISS/ISO is required for the appointment of a foreign Contractor. If there is the intention to appoint a foreign company for a SC, or as a Subcontractor to an existing ABDO company, an authorization request must be submitted to DISS/ISO. If this is not in conflict with national interests, DISS/ISO contacts the competent authority in Industrial Security in the relevant country. At the request of DISS/ISO, this authority submits a "Facility Security Clearance" (FSC) to the company in question on the basis of the prevailing system of security requirements of that country. On the basis of this FSC, DISS/ISO issues the authorization to the applicant. In principle it is not possible to simply refer to the ABDO 2019 in the contract with a foreign Contractor in connection with national legislation. Nonetheless, all necessary security requirements must be included integrally in the contract to be entered into. It is also possible to refer in the contract to the national system of security requirements equivalent to the ABDO 2019. This includes the screening of the employees of the foreign company. If necessary, additional security requirements can be included in the contract, for example with regard to cyber security or foreign influence. DISS/ISO then consults with the competent authority in order to ensure that the implementation of the additional requirements will be monitored.

Appointment of a Dutch company at the request of a foreign nation

If a foreign nation wants to appoint a Dutch company for an SC, DISS/ISO receives a request to issue an FSC with regard to that company. In that case DISS/ISO does not do so unless the company complies with the security requirements laid down in the ABDO 2019, whereby the procedure described above is followed.

Bilateral security agreements

A condition for the bilateral international appointment of companies in the context of an SC is that a security covenant, security agreement or security MoU must be in place between the Netherlands and the foreign nation, in which the exchange of IBPs is facilitated and the mutual security of the exchanged IBPs is guaranteed. DISS/ISO has entered into agreements with many countries in a multilateral context and a few countries on a bilateral basis with the purpose of facilitating efficient mutual appointment.

Appendix 1

Table of the most common Markings linked to an IBP category

DUTCH MARKINGS	Applicable IBP category	Meaning
NLD ONGERUBRICEERD	-	Unclassified Information is not intended for general knowledge (“Need-to-Know”).
PERSONEELS-VERTROUWELIJK	IBP 4	Added to Information containing personal details. Cognizance by non-authorized persons could damage the interests of a person.
COMMERCIEEL VERTROUWELIJK	IBP 4	Added to Information containing company and manufacturing details. Cognizance by non-authorized persons could damage the interests of the company or the State.
MEDISCH GEHEIM	IBP 4	Attached to Information about the physical or mental health of a person. Cognizance by non- authorized persons could damage the interests of a person.
NLD-EYES-ONLY	Depends on the classification level	Usually in combination with a Classification added for the Identification of sensitive national Information. Cognizance by non-Dutch nationals could damage the interests of the Ministry of Defence.
RELEASABLE TO (country, mission, organization)	Depends on the classification level	Usually added in combination with a Classification. Cognizance by individuals who do not belong to the category indicated could damage the interests of the State, an ally, a mission or an organization.
CRYPTO	Depends on the classification level	Added to Information that relates to classified key resources. This Information may only be handled by persons who are registered as having access to crypto information.
CRYPTO SECURITY	Depends on the classification level	Added to documents that could contain crypto Information. Cognizance by non-authorized persons could contribute to the decryption of encrypted Information by non-authorized persons.
COMSEC	Depends on the classification level	Applied with the purpose of identifying assets to safeguard communication security that is not marked as CRYPTO or CRYPTO SECURITY, but to which special rules apply for handling.
EXPORT CONTROLLED	Depends on the classification level	Attached to Information that must be handled in a specific way under export regulations.

Appendix 2

Table of foreign Classifications

Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Departmental VERTROUWELIJK
Optional for int. use: Classification plus	NLD TOP SECRET	NLD SECRET	NLD CONFIDENTIAL	NLD RESTRICTED
EU Classification	TRÈS SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
NATO Classification	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
	COSMIC TRÈS SECRET	OTAN SECRET	OTAN CONFIDENTIEL	OTAN DIFFUSION RESTREINTE
UN Classification		UN STRICTLY CONFIDENTIAL	UN CONFIDENTIAL	
Albania	TEPËR SEKRET	SECKRET	KONFIDENCIAL	I KUFIZUAR
Belgium	TRÈS SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
	ZEER GEHEIM	GEHEIM	CONFIDENTIAL	BEPERKTE VERSPREIDING
Bulgaria	СТОГО СЕКРЕТНО	СЕКРЕТНО	ПОВЕИТЕЛНО	ЗА СПУЖЕБНО ПОЛЗВНЕ
Canada[3]	TOP SECRET	SECRET	CONFIDENTIAL	
	TRÈS SECRET	SECRET	CONFIDENTIEL	
Cyprus	ΆΚΡΩΣ ΑΠΌΡΡΗΤΟ	ΑΠΌΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΌ	ΠΕΡΙΟΡΙΣΜΈΝΗ Σ ΧΡΉΣΗΣ
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Germany	STRENG GEHEIM	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Estonia	TÄIESTI SALAJANE	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITETTU
	YTTERST HEMLIG	HEMLIG	KONFIDENTIELL	BEGRÄNSAD TILLGÅNG
France[4]	TRÈS SECRET DÉFENSE	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	
Greece	ΆΚΡΩΣ ΑΠΌΡΡΗΤ	ΑΠΌΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΌ	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ
Hungary	SZIGORÚAN TITKOS!	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTTÉÜ!
Ireland	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Iceland	ALGERT LEYNDARMAL	LEYNDARMAL	TRUNADARMAL	THJONUSTJSKJAL
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Latvia	SEVIŠĶI SLEPENI	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	VISIŲKAI SLAPTAI	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDJIMO
Luxembourg	TRÈS SECRET LUX	SECRET LUX	CONFIDENTIEL LUX	DIFFUSION RESTREINTE LUX
Malta	L-OGHLA SEGRETEZZA	SIGRIET	KUNFIDENZJALI	RISTRETT
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENTSIELT	BEGRENSET
Austria	STRENG GEHEIM	GEHEIM	VERTRAULICH	EINGSCHRÄNKT
Poland	ŚCIŚLE TAJNE	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Romania	STRICT SECRET DE IMPORTANTĂ	STRICT SECRET	SECRET	SECRET DE SERVICIU
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Slovakia	PRÍSNE TAJNÉ	TAJNÉ	DÕVERNÉ	VYHRADENÈ
Slovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Czech Republic	(TOP SECRET) PŘISNĚ TAJNÉ	(SECRET) TAJNÉ	(CONFIDENTIAL) DŮVĚRNÉ	VYHRAZENÉ
Turkey	ÇOK GİZLİ	GİZLİ	ÖZEL	HIZMETE ÖZEL

[3] Canada does not have an equivalent Classification. Canada handles and secures this Information in accordance with the C-M(2002)49 supporting directives and the supporting documentation for the securing of NATO RESTRICTED Information.

[4] France does not use an equivalent Classification to NLD Restricted. France handles and secures this information in accordance with the CM(200)49, supporting directives and the supporting document for the securing of NATO RESTRICTED Information.

United Kingdom[5]	TOP SECRET	SECRET	NO EQUIVALENT TO CONFIDENTIAL	OFFICIAL-SENSITIVE
United States[6]	TOP SECRET	SECRET	CONFIDENTIAL	
Sweden	KVALIFICERAT HEMLIG	HEMLIG	HEMLIG	HEMLIG
Switzerland - French speaking - German speaking	TRÈS SECRET DÉFENSE	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	DIFFUSION RESTREINTE
	STRENG GEHEIM	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DENDIENSTGEBRAUCH
- Italian speaking	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO

[5] As of 2 April 2014, the United Kingdom only uses the classification levels TOP SECRET, SECRET and OFFICIAL. The Classification UK CONFIDENTIAL is no longer in use and this information is handled as UK SECRET. Information that was previously marked as RESTRICTED is now marked as OFFICIAL - SENSITIVE.

[6] The US does not have an equivalent Classification. The US handles and secures this information in accordance with the C-M(200)49, supporting directives and the supporting document for the securing of NATO RESTRICTED Information.

Appendix 3

Set-up of security organization

Each company that has sensitive company Information should have an adequate security policy and security plan, essential instruments to protect this information from unwanted access. However, for many companies the security of information remains a low priority. Unfortunately, risks are also often underestimated, especially the risks that are associated with social media, mobility and the “Cloud”: means of making confidential company information available beyond the safe boundaries of the work station, thus also making them more accessible for third parties. The responsibility for the security policy, the security plan and the security measures and their implementation must lie with the highest management level. For the supervision of security, an SO must be appointed with the prior approval of DISS/ISO, who has sufficient autonomy, authority, powers and seniority and who has direct access to the highest management level.

In order to guarantee the confidentiality of IBPs, the Contractor must set up the management of the IBPs provided to it or generated by it in such a way that it is possible to find out at all times where and with whom the IBPs are and who accessed them. It is therefore essential that this is carefully registered, as well as unauthorized examination and handling and attempts to do so. This requires structure in the organization as well as clear unambiguous procedures and processes for accessing and handling IBPs that are recorded in the security plan. The following should be taken into consideration in this regard: standardized procedures for registering, transferring, modifying, copying, distributing, storing, communicating and destroying IBPs, both in physical and digital form. This therefore also includes the systematic management of the information system and the Information on it as well as access to these. Careful management can prevent unauthorized examination and handling of an IBP and thus prevent an IBP from being compromised.

Security plan
The Contractor must have a security plan. The security plan includes a short and clear description of the manner in which the security of the IBP will be implemented. The development of a security plan starts with an analysis of the current situation and threats in particular, a list of the security provisions already in place and an analysis of necessary additional measures. The security plan will be further detailed on the basis of the security requirements as referred to in Chapter 1, 2, 3 and 4. Subsequently, the necessary additional measures and procedures will be implemented. If the subsequent plan is approved by DISS/ISO it will then be definitively adopted and implemented. Periodically, i.e. at least once a year, an evaluation must be carried out that determines if the security plan is still satisfactory or whether it needs amending.

In addition to planned monitoring whether the measures are still adequate, an incident or an amended threat analysis may be a reason to run through the process or cycle again. This system ensures that IBPs are secured in accordance with the current threat level, with the application of adequate security measures. This applies to both the physical security of an IBP as to the digital security of Special Information that is processed in IT systems and networks.

Appendix 3.1

Security plan guideline

ABDO security plan
Description of how the security of the IBP will be carried out.

The security plan includes at least the following:
- a short description of the current Special Contracts and/or projects with a high Classification;
- details of the company (address, organizational chart, extract from the Chamber of Commerce, introduction to the company);
- contact details of the Security Officer and his/her position within the company;
- allocation of the responsibilities within the executive board regarding the Special Contracts;
- a clear description of the IBPs on the company site.

Clear and manageable measures and procedures in accordance with the requirements in the ABDO 2019 are detailed for the following areas, if applicable:

Executive board and organization
- Set-up of the security organization;
- The Security Officer;
- Structure, property and control of the Contractor;
- Security awareness;
- Security Requirements List;
- Subcontracting;
- Press, internet, social media, publication, photos, etc.;
- Incident Handling.

Personnel
- Management of the number and details of the Confidential Positions and the correct Security Clearance Level in accordance with the Special Contract(s);
- Security screening requests;
- Up-to-date list of valid CNOs and CGCs in relation to the Special Contracts;
- Statement of non-disclosure for the duty of secrecy;
- Non-Dutch national holding a Confidential Position;
- Responsibilities of employees holding a Confidential Position;
- Travel abroad for employees holding a Confidential Position.

Physical
Layered structure and the associated security measures regarding:
- Organizational measures:
  - access control;
  - Authorizations;
  - Logging.
- Constructional measures:
  - Delay Time;
  - Compartmentalization;
  - constructional layers;
  - site and parking facilities;
  - measures to restrict visuals and acoustics.
- Electronic measures:
  - IDSS;
  - EACS;
  - CCTV.
- Response measures:
  - alarm response process;
  - alarm verification.
- Transport and post;
- Safety;
- Physical storage, processing and development;

Cyber

- Information security policy:
  - Policy rules for information security.
- Organizing information security:
  - Internal organization;
  - Division of tasks;
  - Mobile devices and teleworking;
  - Teleworking.
- Secure personnel:
  - Awareness, training programmes and training courses regarding information security;
  - Employment termination and changes to responsibilities.
- Management of company resources:
  - Inventory of company ICT resources;
  - Ownership of company ICT resources;
  - Acceptable use of company ICT resources;
  - Classification of information;
  - Labelling information;
  - Handling company ICT resources;
  - Management of removable data carriers.
- Access security:
  - Company requirements for access security;
  - Policy for access security;
  - Access to networks and network services;
  - Registration and deregistration of users;
  - Management of special access rights;
  - Management of secret authentication information of users;
  - Assessment of users' access rights;
  - Use of secret authentication information;
  - Restriction of access to information;
  - Secured log-in procedures;
  - Password management system;
  - Using special system tools;
  - Programme source code access security.
- Cryptography:
  - Policy on the use of cryptographic controls;
  - Key management.
- Physical security and environmental security:
  - Secure areas;
  - Installing and protecting equipment;
  - Security of cabling;
  - Equipment maintenance;
  - Removal of company resources;
  - Secure removal or reuse of equipment;
  - Unmanaged user equipment;
  - 'Clear desk' and 'clear screen' policy.
- Security of business operations:
  - Documented operating procedures;
  - Change Management;
  - Capacity Management;
  - Separation of development, testing and production environments;
  - Measures of control against Malware;
  - Back-up of information;
  - Registering events;
  - Protecting information in log files;
  - Clock synchronization;
  - Software installation on operational systems;
  - Management of technical vulnerabilities.

- Communication security:
    - Network controls;
    - Security of network services;
    - Division of networks;
    - Policy and procedures for information transport;
    - Cloud Computing;
    - Virtualization.
- Acquisition, development and maintenance of information systems:
    - Analysis and specification of information security requirements;
    - Principles for engineering secured Systems;
    - System acceptance tests.
- Suppliers:
    - Information security policy for suppliers.

Appendix 4

Security Officer

Security Officer and Deputy Security Officer

The Security Officer (SO) is tasked with day-to-day responsibility for security and may be supported in these activities by one or more dedicated deputy Security Officers, for example, to cover during the absence of the SO, or one for each company site. A deputy SO can also be appointed due to a specialization, such as cyber expertise. For more information about the role of the cyber SO, see Appendix 24. The senior management proposes the candidate SO/Deputy SO who meets the requirements, tasks and responsibilities described in the ABDO 2019 to DISS (for SO and Deputy SO applications, see the forms in this appendix). The applicant is obliged to fill in all required fields of the form.

Minimum requirements for the appointment of an SO Deputy/SO

As a minimum, the SO/Deputy SO must:

- have Dutch nationality and be employed by the company in question;
- have sufficient autonomy, authority, powers and seniority;
- have been screened to the highest applicable level of the Special Contracts that the company performs;
- have direct and independent access to the CEO, senior management or executive board.

Tasks and responsibilities

With regard to ABDO Authorizations, the SO/Deputy SO is responsible for:

- being the first point of contact on behalf of the Contractor for DISS and GISS, representing the Contractor for all security aspects, being authorized to take the required measures and decisions;
- day-to-day responsibility for the security;
- supervising the reliability of the security of the IBP in accordance with the security requirements as described in ABDO 2019. When necessary, taking measures to improve the security policy;
- recording data regarding access to and examination of IBPs and retaining it during the period indicated, to enable investigation of suspected incidents after the fact.
- drawing up a security plan in relation to the Special Contracts and IBP in accordance with the requirements of ABDO 2019;
- implementing necessary changes to the security plan within the set period as a result of an increased threat level or an incident;
- ensuring full cooperation during inspections, audits and investigations of the Contractor by DISS/ISO;
- regularly updating the security plan (approved by DISS/ISO) on the basis of the progress of Special Contracts and having an IBP on site;
- periodically testing the security plan in practice and reporting this to the executive board and DISS/ISO in writing. For a full assessment of the security, the SO draws up a self-inspection report at least once a year and sends this to the executive board;
- giving full cooperation during inspections, audits and investigations by DISS/ISO;
- reporting, investigating and taking measures regarding incidents. This is carried out according to the Incident Handling process (see Appendix 9);
- maintaining an up-to-date list of all Special Contracts, IBPs and employees to which a CNO or CGC and the corresponding statement of non-disclosure for the duty of secrecy have been issued;
- managing the number and details of the Confidential Positions and ensuring the correctness and validity of the Security Clearance Level;
- requesting in good time the initial/renewed Security Screening for employees holding a Confidential Position;
- management of the access to an IBP and determining the Authorizations for this;
- providing insight into where and with whom IBPs are located and who has taken cognizance of them and when;
- the SO coordinates and checks the receipt and sending of Special Information and, where necessary, the use of courier passes;
- the SO advises with regard to the Marking and Classification of new Information;
- periodically, i.e. at least once a year, checking the presence and completeness of registered IBPs (and copies);
- where necessary, directly and independently advising the executive board about security matters;
- providing information, in the context of Security Awareness, to employees holding confidential positions at the start of a new Special Contract and periodically during Special Contracts regarding ABDO procedures and the related responsibilities;

- if necessary, providing advice and supervision to employees who are working on Special Contracts, who have foreign contacts or who are travelling to high-risk countries.
- mediates in international visit announcements in the context of 'International Visits'
- applying to DISS/ISO for a Subcontractor in the event of proposed subcontracting of activities in the context of a Special Contract (see Appendix 8). ABDO 2019 is incorporated in the terms of the contract with the Subcontractor;
- the SO ensures he/she is up to date regarding the acquisition of the company and informs DISS regarding proposed export to high-risk countries, taking into account whether the proposed export is directly or indirectly related to defence technology or whether the development is initially paid for by the Ministry of Defence;
- regularly informing the Deputy SO of procedures and incidents so that it can perform the tasks in the absence of the SO

Appendix 4.1

Appointment of Security Officer

Appointment of Security Officer and assigning responsibilities		
To:	Industrial Security Office Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands	T: +31-70-4419463 E: indussec@mindef.nl

Appointment of the Security Officer

I, _____ of _____
(highest administrative body, executive board and/or owner) *(Company/Organization)*

appoint, following approval from DISS/ISO, the following employee as Security Officer (SO) in accordance with the provisions laid out in the ABDO 2019.

_____
(full name of SO)

Date _____

Signature_____
(Signature of highest administrative body, executive board and/or owner)

I, _____
(full name of appointed SO)

Employee of _____

Position _____

Appointed establishment _____

hereby declare to understand and accept the tasks and responsibilities of the SO as described in Appendix 4 of the ABDO 2019 and to comply with them.

Signature_____
(signature of the SO)

Details SO (mandatory)	
Gender:	
First Name:	
Last Name:	
identity card number:	
Telephone number:	
E-mail address:	

Solely when DISS/ISO refuses the appointed SO, the applicant will be notified.

Appendix 4.2

Appointment of Deputy Security Officer

Appointment of Deputy Security Officer and assigning responsibilities		
To:	Industrial Security Office Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands	T: +31-70-4419463 E: indussec@mindef.nl

Appointment of the Deputy Security Officer

I, _____ of _____
(highest administrative body, executive board and/or owner) *(Company/Organization)*

appoint, following approval from DISS/ISO, the following employee as Deputy Security Officer (DSO) in accordance with the provisions laid out in the ABDO 2019.

_____
(full name of DSO)

Date _____

Signature_____
(Signature of highest administrative body, executive board and/or owner)

I, _____
(full name of appointed DSO)

Employee of _____

Position _____

Appointed establishment _____

hereby declare to understand and accept the tasks and responsibilities of the DSO as described in Appendix 4 of the ABDO 2019 and to comply with them.

Signature_____
(signature of the DSO)

Details DSO (mandatory)	
Gender:	
First Name:	
Last Name:	
identity card number:	
Telephone number:	
E-mail address:	

Solely when DISS/ISO refuses the appointed DSO, the applicant will be notified.

Appendix 5

Control and company structure

Initial information provision about Control, company structure, etc.
In principle, the executive board of a Contractor is responsible for the day-to-day management of a company. Sometimes, however, other people can influence the decisions taken by the executive board in such a way that the protection of an IBP can be jeopardized. It is therefore necessary to always have insight into who or what has Control, whether Control lies with foreign parties, whether there are (foreign or domestic) business relations, including cooperative arrangements, whether activities are performed at foreign locations, etc.

In order to protect the security of the State and its allies, the influence of third parties that could have conflicting interests must be monitored. In order to assess whether there is undesirable (foreign or domestic) influence, as part of the authorization procedure to be followed the company must hand over all data to DISS/ISO which DISS/ISO deems necessary to assess this, including at least:

- Certificate of propriety, information about Control, shareholders and company structure;
- information about business activities, sites and cooperative arrangements;
- name, date and place of birth, address and nationality of the director(s), supervisors (e.g. supervisory board members), management and other persons who could have decisive influence on the policy of the company;
- a copy of the articles of association and the latest annual report.

The Contractor is obliged to provide additional information at DISS/ISO's first request.

2. Changes to stated Control etc.
Changes to the above-mentioned information should be assessed for possible undesirable influence.

Proposed changes to the stated details and information under section 1, as well as proposed business cessation, mergers, sourcing, division, suspension of payment or forthcoming bankruptcy must be reported to DISS/ISO without delay.

At the discretion of DISS/ISO, the DISS Director will communicate in writing within four weeks whether there are objections on the grounds of security to the proposed change in Control, ownership or share ownership, proposed merger, cooperation or forthcoming bankruptcy and what the possible consequences are thereof. Depending on the possible security risks, the DISS Director may decide to suspend or withdraw the ABDO authorization granted.

3. Company sites
A company may have registered offices in one or more locations (in the Netherlands and/or abroad). The Contractor must at all times have insight into the locations and indicate where the IBPs are stored, edited or generated. It must also be stated what the company structure is at the locations involved in the contract and who is responsible for the security. Changes to company locations and/or responsibilities must be reported to DISS/ISO.

If a Contractor divides work on an IBP across its locations, this must be incorporated in a contract-specific security plan. It must be stated which location is tasked with activities on an IBP. The requirements set in the ABDO 2019 must be complied with at each location, taking into account the IBP category applicable for the specific location.

4. Manner of providing information
The form "Declaration of propriety, Control and company structure of the Contractor" is available on the next page. This should be completed and signed and sent to DISS/ISO in the case of a regular declaration or a change. The applicant is obliged to fill in all required fields on the form.

Appendix 5.1

Form: Declaration of propriety, Control and company structure or changes to these

Name of Subcontractor	
Correspondence address and post code	
Primary place of business and post code	
Telephone number	
Fax number	
E-mail address	

Business activities	
Other places of business and post codes, if applicable	
Locations	

Share ownership [a] [b]	
Structure within company	
Control within company [c]	
Appointment and discharge policy [d]	

Full personal details (surname, first names, date and place of birth, home address, current and previous nationalities)	1. The owner(s)/shareholders 2. The partners 3. Executive director(s)/Director(s) 4. Member(s) of the supervisory board

Is there any form of cooperation with a foreign company or a Dutch company under foreign influence under such terms that the organization has gained influence of the company policy or can demand the provision of company data and/or allow representatives or authorized persons to examine company data? **(If this question is answered in the affirmative, particulars must be stated in a separate appendix)**

Has the organization entered into any financial obligations under such obligations that a foreign national, group of foreign nationals, or a foreign and/or Dutch organization under foreign influence has gained influence in the company policy or can demand the provision of company data and/or providing insight thereof to representatives or authorized persons? (If this question is answered in the affirmative, particulars must be stated in a separate appendix)

Add the most recent annual report of your company to this declaration.

The undersigned _____

Position _____

declares that the above information is in accordance with the truth *)

Date _____ Place _____

Signature_____

*) Providing information that is not in accordance with the truth or purposefully withholding information to which the above questions relate can lead to the rejection, suspension or revocation of the ABDO authorization.

a. Description of the amount of the share capital and/or membership rights, the composition in type of shares and/or membership rights and the distribution among the shareholders and/or members (together with contractual or statutory rights attached to the shares/membership rights) of 1. the Contractor; 2. everyone that has direct or indirect shares and/or membership rights in the contractor and 3. all of the legal persons and partners that belong to the group of companies, in so far as the members of the group of companies have shares (directly or indirectly) in the Contractor.
b. A schematic overview of those who have direct or indirect shares or membership rights in the contractor as well as the group of companies of which the Contractor is part, together with every legal person and partner belonging to the group of companies, every member of the executive board and if applicable every member of the body supervising the executive board of that legal person and/or partner, with their registration number in the trade register or a comparable register.
c. As far as applicable, a description of the (actual or potential) direct or indirect control of the shares or membership rights in the Contractor. And if applicable a description of Control by anyone other than the holders of shares and/or membership rights (for example as a result of powers of attorney, rights of pledge, rights of usufruct, management agreements or voting agreements).
d. In so far as applicable, a description of how the members of the executive board and/or supervisory body are appointed and discharged.

Appendix 6

Security Awareness

Regardless of how far-reaching the security measures may be, ultimately people are the most important link in the chain. The vulnerability of an IBP and the likelihood of it being compromised increases when a Contractor and its employees are not aware of the value of these interests and the risk of them falling into the wrong hands. Employees must be aware at all times of how and where to process and save the IBP and with whom they are permitted to share it. Employees that have cognizance of sensitive Information or have access to keys or passwords that grant access to special (digital or paper) files must realize that they have access to interesting Information and therefore are of interest themselves and may be a risk.

Experience has shown that employees and/or Contractors often do not realize that they have sensitive Information at their disposal that is interesting to third parties. This relates not only to IBPs, but also to sensitive company information. Foreign intelligence services, as well as the competition, may be very interested in this Information.

Employees may unintentionally give away important Information if they cannot make an accurate assessment of the value thereof. Only once the value of the Information has been fully appreciated by the whole organization of the Contractor, from the top to the bottom, can there be a culture in which the IBP is in fact handled as such by all employees.

It is important that security awareness is expressly promoted by directors at the highest level. The Contractor is therefore obliged to subject all employees to information sessions for the purpose of increasing security awareness. In such information sessions, relevant parts of the ABDO 2019 will be addressed and attention will be paid to developments relating to threats and security measures. The structure and content of the information session can be coordinated with DISS/ISO if necessary.

Information provision of this kind ensures that each employee in the organization understands the importance and the extent of the security, recognizes his/her individual responsibility in the matter and acts accordingly. In addition to structural information provision, there may be the need for individual meetings, for example in the event of travel abroad or when preparing to receive visitors (especially foreign visitors).

Finally, an employee must receive a proper security briefing before being posted on a SC, in which the importance of the security of the entrusted IBP is addressed with regard to transport and storage. As part of this, the benefit and, in particular, the need for a security regime will be explained in detail. The obligations resulting from holding a Confidential Position or other position on an SC must also be explained (Appendix 10). Once appointed to a Confidential Position or other position on an SC, the employee involved will be subject to security supervision on a regular basis. Security instructions or training courses must be provided by the SO on a regular basis (see also the requirements in chapter 1).

Appendix 6.1

Security awareness: different forms of espionage

Espionage can take many different shapes and forms. The links below give explanations of the different ways of approaching espionage.

- www.aivd.nl - Under 'Onderwerpen' (incl. cyberdreiging & economische spionage).
- www.ncsc.nl - Security Assessment Netherlands Whitepapers link.
- www.alertonline.nl – Security awareness, ransomware, security of personal data.
- www.veiliginternetten.nl - phishing and cybercrime.
- www.fraudehelpdesk.nl – phishing and action patterns.
- www.csacademy.nl - information, developments, Glossary (right column)
- www.veiligbankieren.nl - Fraud (incl. phishing and social engineering).

Brochures/general information (at the time of writing, available via the url below):

General information about Espionage:
www.aivd.nl/onderwerpen/spionage

Espionage when travelling abroad:
www.aivd.nl/onderwerpen/spionage/aivd-publicaties-over-spionage

Long-term stay abroad:
www.defensie.nl/onderwerpen/militaire-inlichtingenen-en-veiligheid/veiligheidsonderzoek/langdurig-verblijf-in-het-buitenland

Appendix 7

Security Requirements Checklist

The special nature of the contract must be determined by the Commissioning Party at as early a stage as possible. On the basis of a Security Requirements Checklist (SRC), the Commissioning Party provides Information about the nature of the contract to be awarded, the IBP to be handed over to the company, or to be generated there and the relevant security level. On the basis of the SRC, the Contractor can apply the security measures in order to correctly protect the IBP.

An SRC drawn up by the Commissioning Party gives the Contractor insight into which sub areas apply for the specific Special Contract.

Equivalent foreign SRC
Companies may also be eligible for a Defence-related Special Contract for NATO, the EU or a foreign Defence organization. In addition to the national IBP there may also be NATO, EU or foreign IBPs involved. DISS/ISO serves as the designated security authority for the company involved on behalf of these organizations and countries. In that case it is often a condition that agreements are laid down in a security covenant or a Memorandum of Understanding (MoU). DISS/ISO then has the role of Designated Security Authority (DSA).

NATO and EU regulations and many international treaties prescribe that a specific “Project Security Instruction” (PSI) be included in contracts with NATO, the EU and foreign organizations for the security requirements of large projects. For smaller projects, a “Security Aspect Letter” (SAL) is often used in this context. With regard to content, PSIs and SALs have much in common with the ABDO 2019. For example, the PSI has a “Security Classification Guide” and the SAL has a “Security Classification Checklist”, the equivalent of the SRC from the ABDO 2019. Companies that are awarded contracts of this type are inspected on the basis of the ABDO 2019, as the security requirements of the ABDO 2019 are at least of the same level as the requirements set by NATO and the EU for such cases.

Appendix 7.1

Security Requirements Checklist Form

General

Nº	DESCRIPTION	NLD TS /IBP 1	NLD S /IBP 2	NLD C /IBP 3	NLD R /IBP 4	None	COMMENTS
1	Contract						
2	Staff requirements						
3	Description of the composition of the main team						
4	Composition of the main team						
5	Composition of the sub-team						
6	Description of the project						
7	Final product (complete)						
8	Outer shape/appearance						
9	Correspondence relating to the contract						
10	TMT requirements						
11	Drawings, tracings, requirement sheets, models, photos, etc. Calculations and reports regarding the construction						
12	Development schedule						
13	Production schedule						
14	Technical specifications						
15	Analysis						
16	Operational and technical results						
17	Testing and measurement data						
18	Price calculations						
19	Parts						
20	Prototypes						
21	Requirement						
22	Quantity to be delivered/already delivered						
23	List of spare parts						
24	Packaging and sending instructions						
25	Operating instructions/handbooks						
26	Documentation (general)						
27	Inspection/delivery documentation						
28	Manufacturer documentation						
29	Software						
30	ECM / ECCM						
31	Crypto equipment and handbooks						
32							
33							
34							
35							

Signed by: _____

Unit: _____

Date: _____

Appendix 7.2

Security Requirements Checklist Form

INFRASTRUCTURE / BUILDINGS

Nº	DESCRIPTION	NLD TS /IBP 1	NLD S /IBP 2	NLD C /IBP 3	NLD R /IBP 4	None	COMMENTS
1	Correspondence						
2	Sketch design						
3	Final design						
4	Drawings, tracings, models, photos, etc.						
5	Project description						
6	Price calculations						
7	Purpose/function of the building						
8	Purpose/function of work areas (specification)						
9	Layout of the building						
10	Set-up of the work areas (application)						
11	Construction of the building						
12	Construction elements of work areas						
13	Electronic system (or parts thereof)						
14	Emergency power system						
15	Lighting system (or parts thereof)						
16	Heating system						
17	Air conditioning, gas valve/gastight provisions Water supply system						
18	Emergency water system						
19	Telephone/intercom system						
20	Telex/crypto system						
21	Electronic/electrical alarm system						
22	EMP security						
23	NBC security						
24	Computer area						
25	Testing and measurement data						
26	Operating instructions						
27	Maintenance instructions (specifications)						
28	Special technical systems						
29							
30							
31							
32							
33							
34							
35							

TERRAINS/SITES

Nº	DESCRIPTION	NLD TS /IBP 1	NLD S /IBP 2	NLD C /IBP 3	NLD R /IBP 4	None	COMMENTS
1	Destination						
2	Water regime - sewerage - drainage - watercourse						
3	Layout						
4	Assembly (specification)						
5	Electrical system - high-voltage installation - low-voltage installation						
6	Gas distribution system						
7	Water supply system - cooling water - drinking water - water as an extinguishing agent						
8	Sewage draining system - sewerage - water purification plant(s)						
9	Fencing						
10	Electric/electronic alarm system(s)						
11	EMP security						
12							
13							
14							
15							

Signed by: _____

Unit: _____

Date: _____

Appendix 8

Logistics chain

The Contractor will normally not carry out the Special Contract independently from third parties, but will represent a logistics chain of companies when in communication with the Commissioning Party. From a security point of view, it is necessary to gain insight into the chain and to set requirements for links in the chain if necessary.

The basic structure of the logistics chain consists of several Subcontractors and Suppliers alongside the Contractor. These are other companies (i.e. other legal entities than the Contractor) to which the Contractor outsources certain activities on an IBP.

The ABDO 2019 therefore applies to the Contractor itself as well as all Subcontractors (and any sub-Subcontractors and Suppliers and sub-Suppliers) that could come into contact with or have access to an IBP or produce an IBP. The ABDO 2019 should also apply to Subcontractors and Suppliers/sub-Suppliers of system components that need a certain level of protection due to their critical/vital function. On the basis of the insight gained by the Contractor, it will be determined in consultation with DISS/ISO to which of the Subcontractors and/or Suppliers/sub-Suppliers involved the ABDO 2019 applies. In this way, all involved parties in the chain are put under supervision with regard to security. If the intended Subcontractor and/or Supplier/sub-Supplier is based abroad, the prevailing regulations with regard to industrial security in force in the country in question will be referred to rather than the ABDO 2019. In these cases, DISS/ISO requests a Facility Security Clearance from the foreign partner.

Subcontractors and Suppliers/sub-Suppliers
If a Contractor subcontracts work on an IBP or uses vital system components from third parties, the Subcontractors and/or Suppliers/sub-Suppliers will be registered with DISS/ISO in writing by the Contractor prior to the contract. See the attached form in this regard. At the discretion of DISS/ISO, the Contractor will then be granted or denied authorization to appoint them in accordance with the procedure described in the ABDO procedure guidelines of the ABDO 2019. The Contractor must incorporate the ABDO 2019 in the contract with them. The regular ABDO 2019 procedure will therefore be followed to impose the ABDO 2019 requirements on them before they can start their activities and/or supply vital system components.

If they are based abroad, the prevailing industrial security regulations in force in the country in question will be referred to, rather than the ABDO 2019. In these cases, DISS/ISO requests a Facility Security Clearance from the foreign partner.

Self-employed worker without employees
Self-employed workers without employees (hereinafter self-employed worker) are a special legal form. A self-employed worker performs all tasks and holds all positions that in a company are normally divided among different people and business units. Due to the flexibility of this legal form, the Ministry of Defence and Subcontractors make frequent use of self-employed workers. From a security point of view, a self-employed worker is in principle assessed as a Contractor or Subcontractor. That is to say that a self-employed worker that works on an IBP to which the ABDO 2019 applies must comply with the security requirements as referred to in the ABDO 2019. The special circumstances of a self-employed worker, who frequently does not carry out activities in business premises but in a work area in his own home that is set up for this purpose, may mean, however, that not all requirements of the ABDO 2019 can be met. Individual arrangements should provide the solution in this regard.

In a number of cases it is not necessary to treat self-employed workers as a company from a security point of view, for example if the activities/classified activities are performed on the Contractor's site or at a Ministry of Defence site, using the approved IT infrastructure of the Contractor or the Ministry of Defence. If a self-employed worker is considered a company for the purposes of the ABDO 2019, the self-employed worker serves as his own SO and must therefore request his/her own Security Screening.

In the case of a foreign Commissioning Party, the self-employed worker is always considered a company.

Service Providers

A Service Provider provides certain help/support to the Contractor or Subcontractors and/or Suppliers/sub-Suppliers, which may range from facilities services (cleaning, surveillance, catering) to IT services. The term Service Provider is often exclusively associated with internet and telephony services. The ABDO 2019 applies to Service Providers who may come into contact with or have access to an IBP or produce one, or deliver a product that is not an IBP in itself but that influences the integrity of the final system. Any internal service providers fall under the Contractor, which means the ABDO 2019 automatically applies.

Appendix 8.1

Application form for Subcontractors and/or Suppliers/sub-Suppliers

Request for permission to appoint a Subcontractor
If a Subcontractor has to be appointed for the purpose of performing a Special Contract, permission for this must be requested in advance from DISS/ISO by means of this form. 'Subcontractor' refers to (Internal) Subcontractors, (sub) Suppliers, (internal) Service Providers, and self-employed workers without employees. The applicant is obligated to complete this entire form
To: **Industrial Security Office** Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands T: +31-70-4419463 E: indussec@mindef.nl

Requisitioner/Commissioning Party	
Name:	
Address:	
Post code / Place:	
Contact:	
Telephone number:	
E-mail:	

Subject related Special Contract	
Contract name:	
Reference ABDO authorization:	
Prevailed ABDO:	
Classification:	
A completed SRC must be added to this application.	

Subcontractor / Contractor	
Name:	
Address:	
Post code / Place:	
Contact:	
Telephone number:	
E-mail:	

Subject Special Contract		
Contract name:		
Contract description:		
Duration of contract:	From:	Till:
Location of activities? Location Contractor ☐ Location Subcontractor ☐ Both of the locations ☐ Location Ministry of Defence _____ Other locations _____		

Will an IBP be processed, stored and/or generated physically on the site of a Subcontractor? If so, which location? Location Contractor ☐ Location Subcontractor ☐ Both of the locations ☐ Location Ministry of Defence _____ Other locations _____
Will an IBP be processed, stored and/or generated digitally on the site of a Subcontractor? If so, which location? Location Contractor ☐ Location Subcontractor ☐ Both of the locations ☐ Location Ministry of Defence _____ Other locations _____
Is the ABDO incorporated in the contract? Yes ☐ No ☐ (If not, then this must nevertheless be incorporated in the contract to be entered into.)
A completed SRC must be added to this application.

Signature	
Name of Security Officer:	
Date:	
Signature:	

Appendix 9

Incident Handling procedure

If an IBP is compromised or an attempt to do so has been made or is suspected, this is referred to as a Security Incident. If it has been indicated that this is the case or has been the case, adequate handling is required in accordance with the Incident Response Procedure (IRP). In addition, the incident must be reported to DISS/ISO without delay. The main aim in this regard is to act as quickly as possible to contain the damage and take measures to prevent recurrence. This is accomplished by:

- recording all Information about the incident;
- perform a conditional analysis and validation in order to determine the possible damage;
- informing stakeholders;
- taking measures to contain the damage;
- adapting the use of or work on the IBP;
- adapting the security measures in order to prevent recurrence.

A plan has been included in this appendix (Appendix 9.1), an 'initial incident report' for making the first written report of the incident/possible incident (Appendix 9.2), a step-by-step plan, according to which structured handling of a Security Incident must take place (Appendix 9.3) and a breakdown according to classification which indicates the level of urgency (Appendix 9.4).

Appendix 9.1

Incident Handling plan

This appendix contains the six (6) steps for the purpose of an incident handling plan. These steps need to be periodically repeated to keep the plan up-to-date.

Step 1: Identify and prioritize assets
Ensure to identify critical assets and prioritize these critical assets based on importance and risk. Ask the question: which assets will lead to the most damage in case of theft, damaging or if compromised?

Step 2: Identify risks
Ensure to identify the risk profile of your company. The threat for each company varies and therefore the risks and measures will be different.

Examples of threats which may be a risk:
- Sabotage;
- Espionage;
- Subversion;
- Terrorism;
- Extremism;
- Cyber.

Step 3: Determine procedures
It is important to determine policy and procedures to ensure all personnel is informed and able to respond correctly in the event of an incident.

For example:
- Identification and mitigating or stopping an incident;
- Retrieve and secure information;
- A communications plan with notification and escalation;
- A business continuity plan including procedures for incidents outside office hours;
- Training of personnel.

Step 4: Form an incident response team
Ensure to form incident response teams based on types of incidents and ensure these teams are able to be contacted when necessary.

Examples of important roles in teams:
- (Cyber) Security Specialist;
- Communication Specialist;
- Branch Manager;
- Legal department;
- Responsible Director;
- Information Officer.

Step 5: Inform personnel
Ensure the plan is coordinated and widely supported within the company. As a result, personnel will do what is required and this will also ensure the allocation of time and means as needed.

Step 6: Train personnel
All personnel should be aware of expectations of each individual in the event of an incident. Practice incidents periodically, for example by re-enacting scenarios or by actually simulating an incident. Apply lessons identified by amending the plan if applicable.

Appendix 9.2

Initial Incident Report

ABDO 2019 INCIDENT Initial Report	
Incident number:	
Date:	
Name:	
E-mail:	
Telephone number:	

Date and time incident was detected:		
Status of the incident:	☐ Active	☐ Inactive
Incident type	☐ Cat 1 ☐ Cat 2 ☐ Cat 3 ☐ Cat 4 ☐ Cat 5	
Brief description of the incident		
Confidentiality of the data involved	☐ IBP 1 / NLD Top Secret ☐ IPB 2 / NLD Secret ☐ IBP 3 / NLD Confidential ☐ IBP 4 / NLD Restricted	
How was the incident detected and by whom?		
First analysis		
Signature		
Print this page, fill it in and send it to DISS/ISO: indussec@mindef.nl		

Appendix 9.3

Incident Handling step-by-step plan

In the case of digital incidents, additional steps must be taken in the Incident Handling process. This is indicated in the step-by-step plan with a *.

Step	Purpose	Execution
1.Identification	Validating, identifying and reporting.	1. Collect the audit logs and analyze them; 2. After discovering the incident, report without delay via an initial report to DISS/ISO and own management (by phone via the Duty Officer AND via Incident Handling form, found in Appendix 9.1); 3. Put together the investigation team; 4. Determine the initial impact of the incident and classify it.
2. Recording the incident	Record the details of the incident.	1. Record the date and the time; 2. Who is reporting the incident? 3. Details of the incident.
3. Initial response	Collect sufficient information to determine the correct response.	1. Investigate the incident (real or 'false positive'); 2. Record details; 3. Adjust the composition of the team if necessary; 4. Communicate to employees working on the Defence project.
4. Communication	Communication and coordination with stakeholders.	1. In the event of a non-Cyber incident: Discuss the incident with the team members of the incident response team and the DISS/ISO; 2. In the case of a Cyber incident: Discuss the incident in a session with team members of the incident response team and with the DISS/ISO Cyber auditor *; 3. Determine the measures and further coordination to reduce the impact.
5. Containment	Limit the scope and impact of the incident.	1. Possibilities; 2. Turn off the system; 3. Stop the service; 4. Unlink accounts; 5. Make a full back-up of the infected system; 6. Restore the infected system.
6. Response strategy	Determine the response. Dependent on the situation.	Research the most appropriate response. Take political, technical and legal factors into consideration.
7. Classification	Determine the classification of the incident using the "classification" table.	1. Sub-step; 2. Categorize; 3. Prioritize; 4. Allocate resources. N.B.: Take into consideration at all times: 1. How critical the system is; 2. Manifestation of the incident (disaster or type of digital attack) *; 3. Scope of the incident; 4. Legal working framework.
8. Incident investigation	Collect evidence relating to the incident.	1. Identify; 2. Incident description; 3. Date and time of the incident; 4. Source of the incident (actor); 5. Mitigation steps to prevent recurrence.
9. Data collection	Collecting facts and evidence on hosts, network devices, and other media needed for Forensic examination.	1. Hosts: Collect logs, system backups, data in volatile memories, such as: date/timestamps, application logs, open ports, listening applications and the status of network interfaces *; 2. Network devices: IDS/IPS logs, router logs, wire taps, authentication servers *; 3. Other: collect information from other sources via interviews and social media.
10. Forensic analysis	Analyze and review collected data.	Steps: a. Photograph material to be investigated; b. Software analysis, keyword search, date/time chronology *; c. Investigate data that has been systematically deleted from the system *; d. Document forensics on processes and activities.
11. Protecting evidence	Necessary in order to be able to use the information for legal steps.	1. Make a full back up on a data carrier that has never been used *; 2. Protect against physical and logical damage; 3. Document the chain of custody.

12. Neutralization	Solve the cause of the incident.	1. Remove vulnerability; 2. Prevent the vulnerability being exploited again by implementing the measure.
13. System recovery	Bring the system back to its normal operational circumstances. Systems and networks are monitored and validated.	1. Determine the procedure to full recovery *; 2. Monitor the system for network loggers, system files and possible backdoors *; a. Set up the operating system *; b. Restore the data from the back up *; c. Investigate possible protection and detection measures *; d. Install security patches and log functionality *.
14. Incident documentation	Document the steps and conclusions directly after completing the forensic investigation.	Describe: 1. The Security Incident; 2. The cause; 3. Measures taken; i. Who; ii. Which; iii. When. For sending the documentation to DISS/ISO, use is made of the report template for Incident Handling and reporting, found in appendix 9.2.
15. Incident damage assessment	Determine the impact of the security incident.	Determine in collaboration with DISS/ISO what the effect of the incident is on the Special Contract of the Ministry of Defence.
16. Review & update response procedure	Lessons learned.	1. Determine how the security plan must be amended as a result of the incident; 2. Update the security plan.
17. Reporting	Closure	Write a report containing the details of the abovementioned steps and submit it to DISS/ISO.

Appendix 9.4

Incident Handling classification

Category	Name	Description Digital	Description Physical	Time frame
Cat 0	Exercise and (network) test After reporting in advance: EXERCISE EXERCISE EXERCISE	This category is used during network tests and in exercise situations. This category is reported both orally and in writing by reporting EXERCISE three times, in order to prevent confusion with a real incident.	This category is used during network tests and in exercise situations.	Not applicable.
Cat 1	Unauthorized access	An individual has purposefully gained unauthorized logical or physical access to special information on a network, system, application or data.	An individual has purposefully gained unauthorized access to special information or has gained unauthorized to a secure area.	Within **1 hour** of detection.
Cat 2	Denial of Service (DoS)	An attack that successfully prevents authorized employees from gaining or having access to Special Information. This situation also includes being the victim in a DoS attack.	Activities that lead to authorized persons not being able to gain access to Special Information or secure areas.	Within **2 hours** of detection, if the attack takes place or has taken place.
Cat 3	Malicious software	Successful contamination with malicious software (worm, virus, Trojan horse or other form of malware) that contaminate operating systems or applications. As an exception, the duty to report does not apply to the successful mitigation of contamination of a non-classified network or host.	It has been established that a category O, C, E or R measure has been disabled.	Within **1 day**. Note: If the contamination is of a state secret network, within **1 hour**. If applicable to a secure area, within **1 hour**.
Cat 4	Unauthorized use	An individual breaches the ABDO regulations.	An individual breaches the ABDO regulations.	Within **1 week**.
Cat 5	Scans/Probes/ Access attempts	This category contains all more or less targeted activities that are used to later exploit a network, host, open port, protocol, service or a combination of these. This duty to report does not apply to untargeted scans.	This category contains all more or less targeted activities that serve to provide access to the Special Information or secure areas (such as scans, incl. periphery) at a later date. This duty to report does not apply to untargeted scans/attempts.	Within **1 month**. In the case of a classified network or a secure area, within **1 hour**.

Appendix 10

Confidential Positions

A Confidential Position is a position as referred to in the Central and Local Government Personnel Act 1929 (Ambtenarenwet 1929) and in the Security Screening Act (Wet veiligheidsonderzoeken; Wvo). The Minister of Defence may only allocate a position as a Confidential Position if the duties of the position have the potential to damage national security. This is the case if:

- it concerns a position in which cognizance can be taken of State Secrets; positions that involve taking cognizance or Crypto Information or Crypto Materiel fall into a special category in this regard;
- the position is of Vital importance for the continued existence of the social order;
- it concerns a position in which access to military installations is necessary.

Activities for which cognizance can or must be taken of an IBP, and Special Information (SI) in particular, as well as activities that are important in a different sense in connection with the security of State Secrets, may solely be assigned to employees who hold a Confidential Position.

Obligations of employees holding a Confidential Position
Important obligations of employees holding a Confidential Position include:

- closely observing the security regulations of the Contractor;
- social control (keeping each other in check and pointing out responsibilities);
- reporting negligence;
- responsible behavior on social media;
- reporting incidents;
- reporting changes in personal circumstances;
- exclusive use for Special Contracts (SCs) of mobile equipment and other equipment and data carriers such as telephones, laptops, notebooks, USB sticks, etc. that have been approved by the Ministry of Defence.

List of Confidential Positions
The List of Confidential Positions (LoCP) – see the form in this appendix – is a list of the maximum number of Confidential Positions, divided into 13 job categories that are needed to perform one or more SCs on the site of the Contractor. For each category, the number of Confidential Positions is divided up into the required Security Clearance Level (A, B or C). In the NATO (and the EU) column an indication is given of the number of Confidential Positions which require that the holder can demonstrate externally (for example on a visit to the NATO headquarters) that he/she has the required security clearance. A NATO Personnel Security Clearance Certificate (PSCC) is issued to these employees.

The LoCP will be drawn up by the SO of the Contractor in consultation with DISS/ISO.

Confidential Positions Decree
The LoCP is formally adopted by DISS on behalf of the Minister of Defence, as appropriate in agreement with GISS on behalf of the Minister of Foreign Affairs[7], by means of a "Confidential Positions Decree". Security Screenings can be requested pursuant to this decree. The amounts stated in the LoCP may not be exceeded without the prior permission of DISS/ISO. In the event of changes to the contract or the number of contracts, the LoCP will be reviewed. The changed LoCP will then be formally adopted by means of a Decree amending the Confidential Positions Decree. If a Contractor continuously performs one or more classified contracts for the Ministry of Defence, an integral, permanent LoCP can be drawn up.

If a company comes into contact with an IBP during the quote stage, a temporary LoCP is drawn up. This is withdrawn if the contract is not awarded. If the contract is awarded, it is extended to become the definitive LoCP. After completion of the contract or contracts, the LoCP is withdrawn after, if applicable, the IBP has been returned to the Ministry of Defence in accordance with the contract or is destroyed, and access to and cognizance of the IBP are no longer possible for the Contractor. The company is informed in writing of its removal from DISS/ISO's active list of ABDO contractors. The LoCP and Certificates of No Objection (CNO) must be destroyed.

[7] Agreement with GISS is necessary if GISS is responsible for providing the CNO to the employees of the Contractor

Appendix 10.1

Example of List of Confidential Positions

DATE:		CATEGORY:				
NAME OF ORGANISATION: PLACE OF BUSINESS:		EMPLOYER CODE: E-MAIL:				
AREA OF WORK/CONFIDENTIAL POSITION		**SECURITY CLEARANCE LEVEL**			**PARTICIPANT**	
		(A) 011 (NLD TS)	(B) 012 (NLD S)	(C) 013 (NLD C)	NATO (SC)	EU (SC)
D	POLICY AND MANAGEMENT DIRECTOR/CEO					
E	POLICY AND MANAGEMENT POLICY AND MANAGEMENT EMPLOYEE					
F	IT IT EMPLOYEE					
G	ADMINISTRATION/SUPPORT ADMINISTRATION/SUPPORT EMPLOYEE					
H	PROCUREMENT/TENDERING PROCUREMENT/TENDERING EMPLOYEE					
K	SURVEILLANCE/SECURITY SURVEILLANCE/SECURITY EMPLOYEE					
L	PERSONNEL SERVICES PERSONNEL SERVICES EMPLOYEE					
M	FINANCE FINANCE EMPLOYEE					
N	RESEARCH RESEARCH EMPLOYEE					
P	PRODUCTION PRODUCTION EMPLOYEE					
R	COMMERCIAL COMMERCIAL EMPLOYEE					
S	TECHNOLOGY/SYSTEMS TECHNOLOGY/SYSTEMS EMPLOYEE					
T	OTHER EMPLOYEE					
U	SECURITY OFFICER/DEPUTY SECURITY OFFICER SECURITY OFFICER EMPLOYEE					
Total amount:						

Appendix 11

Security Screening, CNO and CGC

The Security Screening and the Certificate of No Objection
Employees that are appointed to a Confidential Position by the Contractor must have a valid CNO. Only then are they permitted to be appointed to a Confidential Position. In order to obtain a CNO, they must be subjected to a Security Screening. They must give permission for this, as well as for updated security screenings for the period that they hold the Confidential Position, by completing and signing a (paper or digital) Statement of Personal Details. The process that leads to the issue, extension, withdrawal or denial of a CNO is referred to as the Security Screening. Costs are associated with applying for a CNO. These are charged to the applicant. The rates depend on the Security Clearance Level applied for.

Security Screening is applied for by the SO of the Contractor by means of attaching a completed application form to the completed Statement of Personal Details or Personal Information Form and sending this to DISS/ISO or DISS, respectively, for the attention of Unit Veiligheidsonderzoeken (Netherlands Ministry of Defence security screening Unit). If the conclusion of a Security Screening is that there are sufficient guarantees that the person involved will faithfully perform all duties entailed in the Confidential Position under all circumstances, the CNO will be issued/extended. If this is not the case, the CNO will not be issued or will be withdrawn and the employee will not be permitted to continue to hold a Confidential Position or be appointed to a Confidential Position. It is possible to register a notice of objection to a (proposed) rejection or withdrawal of a CNO.

Depending on the Security Clearance Level (hereinafter referred to as SCL) applicable to the position, the Security Screening will be performed for the following levels:

- Level A, activities are to be performed that relate to State Secrets classified as NLD TOP SECRET or lower;
- Level B, activities are to be performed that relate to State Secrets classified as NLD SECRET or lower;
- Level C, activities are to be performed that relate to Information classified as NLD CONFIDENTIAL or lower;

If activities are involved that relate to Vital (not classified) Information or large amounts of Information with a low classification and/or marking, an A, B or C SLC may be assigned to a position, deeming a Security Screening necessary. This is at the discretion of DISS/ISO on the basis of the DSP and if necessary in consultation with the Security Authority (Beveiligingsautoriteit) of the Ministry of Defence. For example, system administrators with ‘full administrative privileges’ who have access to large amounts of unclassified data are assigned SLC B.

Pursuant to the Security Screening Act (Wet veiligheidsonderzoek; Wvo), the Security Screening is, in principle, performed by GISS. If it concerns a position that is marked as a Confidential Position on the ground of the necessity of access to military systems, the Security Screening is performed by DISS.

Temporary contract
In connection with the undesirable dissemination of State Secrets and with a view to the costs and benefits of the Security Screening, with regard to both time and money, the utmost restraint should be exercised with regard to appointing temporary employees (such as interns and temps) to Confidential Positions.

Renewed Security Screening
A Security Screening of an employee holding a Confidential Position is performed every five years. At least three months before the end of the period of five years following the issue of the CNO, a new security screening must be applied for by the SO and a newly completed Statement of Personal Details must be added.

Certificate of Good Conduct
If activities are involved that relate to Information that is classified no higher than NLD Restricted (IBP 4), a Security Screening is, in principle, not performed. In such cases, a Certificate of Good Conduct (CGC) is required that relates to specific categories of judicial records. A CGC is issued by Justis, the Ministry of Justice Agency for Scrutiny, Integrity and Screening and can be applied for via the municipality in which the employee resides. Justis applies a range of profiles for the assessment. Under the general screening profile on the application form, a cross must be put next to the aspects of the position that correspond to the position to be held.

Appendix 11.1

Requesting a Security Screening and/or Certificate of Good Conduct

Security Screening
For requesting a Security Screening at DISS: www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/veiligheidsonderzoeken
For requesting a Security Screening at GISS: www.aivd.nl/onderwerpen/veiligheidsonderzoeken/voor-de-werknemer/een-veiligheidsonderzoek-welk-formulier-heeft-u-nodig

CGC
For more information about CGC: www.justis.nl/producten/vog/
For requesting a CGC: www.justis.nl/producten/vog/vog-aanvragen/

Appendix 12

Statement of non-disclosure for the duty of secrecy for employees holding a Confidential Position

Employees of the Contractor that must take cognizance of or have access to an IBP must sign a Statement of non-disclosure for the duty to secrecy in which they declare that they are aware of the provisions regarding the duty to secrecy and the sanctions pursuant to the Criminal Code (Wetboek van strafrecht; Wvs) in the event that he/she fails to perform his/her duty (appendix 12.1). Employees who also have to take cognizance of Crypto, Crypto Security or CCI-marked information or materiel must sign a Statement of non-disclosure for the duty to secrecy in the context of a Crypto position (appendix 40.1).

With regard to IBP 3 and higher, the Statement of non-disclosure for the duty to secrecy must be renewed every 5 years.

Appendix 12.1

Statement of non-disclosure for the duty of secrecy for employees holding a Confidential Position

The undersigned:

Name :_____

Date of Birth :_____

Place of Birth :_____

Hereby declares that he/she:

- is aware of the duty of secrecy of classified Information of which he/she has taken cognizance;
- will faithfully comply with the provisions that have been issued or will be issued for the protection of this Information;
- will not reveal the Information to non-authorized persons;
- has taken cognizance of the provisions in the Criminal Code concerning secrecy, namely Sections 2, 3, 4, 5, 23, 98, 98a, 98b, 98c, 272 and 273 and that he/she has understood the meaning and importance of these provisions.

Place :_____ Date:_____

Signature :_____

Appendix 13

Permission to appoint a person who does not have Dutch nationality to a Confidential Position

Appointing a person who does not have Dutch nationality to a Confidential Position is only permitted following the permission of DISS. A request to this end must be submitted to DISS/ISO by the Contractor. See this appendix for the application form.

The request must include the reason why the Confidential Position must be held by a non-Dutch national and details of the special project and/or assignment to which the person involved will be assigned.

DISS/ISO assesses in consultation with the Commissioning Party/project leader of the Ministry of Defence whether the intention is possible from a security point of view and in addition is not in conflict with the obligations entered into by or on behalf of the government of the Netherlands or the Minister of Defence, whether national, bilateral or with regard to allies. If applicable, permission must also be requested, through the agency of DISS/ISO, from any party with a joint interest, for example a third country with which cooperation is undertaken on the relevant project.

The permission acquired relates solely to deployment on the Special Contract and/or the project stated in the application. If the person involved must be deployed on other projects and/or assignments, permission must be granted per project and/or assignment. Once permission has been granted, a Security Screening must be requested, for which Information is often required from the country of origin of the person involved. This can complicate the Security Screening and, as a rule, delay it too. In some cases, the screening is even impossible and a CNO cannot be issued, meaning the person involved cannot be appointed to a Confidential Position.

Appendix 13.1

Application for permission to appoint a person who does not have Dutch nationality to a Confidential Position

PERSONNEL CONFIDENTIAL
(If completed)

Personal details	
1. Contractor:_____ requests permission to appoint the person detailed below, who does not have Dutch nationality, to a Confidential Position.	
2. Surname:_____ _____	Given names_____
3. Current address:_____ Town/city:_____	Country: _____
4. Date of birth: _____ Country of birth: _____	Place of birth: _____ Citizen service number: _____
5. Nationality/nationalities: _____	Living in the Netherlands since: _____
6. Employed by: _____	Since: _____

Assignment details
1. Description of the assignment to which the candidate is to be assigned: _____ _____ _____
2. Ministry of Defence commissioning party:_____
3. Nature of the activities:_____
4. Motivation for assignment: _____ _____ _____ A clear description of the motivation, in which the necessity for assigning the person involved to the activities is explained.
5. Classification of the assignment:_____ Foreign Classification: _____
6. “Eyes Only” markings? □ Yes □ No

The section below must not be completed by the applicant!

Decision Commissioning	□ Approved	□ Not approved
Name		
Date		
Signature		

Decision of DISS	□ Approved	□ Not approved
Correspondence nº		
Signature	Head of the Industrial Security Office on behalf of Director of the Defence Intelligence and Security Service	
Date		
Comments	_____ _____ _____	

Appendix 14

Changes to personal circumstances

Changes to personal circumstances

During the five-year period, there may be reason to carry out a new Security Screening, in particular due to a change in personal circumstances[8]. If such changes occur, the person involved is obliged to report to the SO. The SO informs DISS/ISO, using the changes form attached in this appendix, as a result of which a new Security Screening may be started. Relevant changes include the following examples:

- divorce, a new relationship or partner;
- financial situation amendments;
- contact with the criminal justice system or the police;
- membership of organizations or associations that may be in conflict with the interests of the Ministry of Defence;
- use of excessive alcohol or drugs;
- long-term stay abroad (for business or private purposes);
- change of position;
- change to the required SCL.

[8] See: Leidraad Persoonlijke gedragingen en omstandigheden (Guide to behavior and circumstances outside of work) https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/downloads/brochures/2015/02/05/leidraad-gedrag-bij-veiligheidsonderzoek

Appendix 14.1

Notification form of change to personal circumstances

PERSONNEL CONFIDENTIAL
(If completed)

Subject	
Organization	

I hereby inform you that:

Name:_____ Initials:_____

Date of Birth:_____ Citizen service number:_____

Hereby declares that he/she:

□ no longer holds a Confidential Position.
□ the person detailed in the appendix no longer holds a Confidential Position.
□ the Security Screening for the person involved can be terminated.
□ has been married to*/ engaged to*/ or cohabiting with* the following person since:

Date:_____ Name:_____

Date of Birth:_____ Place of Birth:_____

Nationality/nationalities:_____

Other notifications:

_____
_____
_____

Security Officer			
Signature		**Date**	

Not to be completed by the applicant

At DISS on	_____	To GISS on	_____	To UVO on	_____
Changed on	_____	Changed on	_____	Changed on	_____
By	_____	By	_____	By	_____

Appendix 15

Release from a Confidential Position or Crypto Position

The employee will be relieved of all duties of the Confidential Position and the CNO will lapse by operation of law:

- in the event of insufficient guarantees that the employee involved will faithfully perform all duties related to the Confidential Position under all circumstances;
- if the employee involved no longer holds a Confidential Position and reassignment cannot be arranged within three months;
- if the employee holding the Confidential Position leaves the company; If the person involved accepts a Confidential Position at a different Contractor, a new Security Screening must be performed.

If the employee holding the Confidential Position intentionally or unintentionally ignores or breaches the security regulations of the Contractor, appropriate measures must be taken and DISS/ISO must be informed. Gross negligence or intentionally compromising State Secrets or Vital Information or Materiel may lead to criminal proceedings.

Employees of the Contractor who are relieved of all the duties of the Confidential Position or Crypto Position for one or more of the above-mentioned reasons must sign a declaration of release from office (Appendix 15.1 and Appendix 40.3). The SO ensures that an explanation is given for the declaration of release from office, that the CNO or copy thereof is withdrawn and that the employee does not have any IBPs, and in particular SI or Crypto, in his or her possession.

Appendix 15.1

Declaration on release from a Confidential Position

PERSONNEL CONFIDENTIAL
(If completed)

Declaration of release from office	
The undersigned (Surname, initials):	
Date of birth:	
Citizen service number:	
E-Employed by the company:	
Released from the position of:	

Declares that he/she:

- will not reveal to non-authorized persons the classified Information that he/she has taken cognizance of while performing his/her duties;
- understands that after termination of the employment/employment contract he/she will remain subject to the statutory and other regulations relating to the secrecy of Information as well as the sanctions for breach of confidentiality laid down in the regulations;
- no longer has in his/her possession any classified Information that was made available to him/her in the capacity of his/her position.

Place :_____ Date:_____

Signature :_____

Appendix 16

Travelling abroad

Travel for business
International travel for business that is undertaken in the context of an SC, and travel to a foreign military site must be reported in advance to the SO via a Request for Visit (RfV). The SO will sign and forward the RfV to DISS/ISO (RfV department) after inspection of correctness and validity. The RfV department will inform the relevant company or foreign military site of the requested visit. Forms for requesting a visit can be claimed at mivd.requestforvisit.business@mindef.nl.

Travel to countries with a high security risk
As a result of global political developments, the security risks involved in travel to specific countries are subject to constant change. A security risk may, for example, be based on an espionage threat or involvement in an armed conflict (Appendix 6.1). The Ministry of Defence indicates to which countries an increased or limited security risk applies and sets criteria for travel to these countries[9]. DISS/ISO can be contacted for further information in this regard.

Employees holding a Confidential Position (and their partners) at Ministry of Defence suppliers have a duty to report to the SO any proposed travel to these countries, whether in a private or a business capacity. The SO reports to DISS/ISO business travel or a stay in a private capacity of an employee holding a Confidential Position to/in a risk country by means of the form in Appendix 16.1. A security briefing that is specific to the country of destination will be given by the SO prior to the trip. A debriefing will take place on return. The briefing will cover taking IT equipment and the methods of possible actors targeting relevant Information. Personal behavior (dos and dont's) in the country of destination may also be covered during the briefing and debriefing.

Travelling abroad in a private capacity
Employees holding a Confidential Position (and their partners) must also report to the SO travel to countries with a security risk in a private capacity. A briefing and debriefing may be desirable or necessary. The Ministry of Foreign Affairs provides travel advice for travel abroad, including countries to which travel is strongly advised against in connection with risks to personal safety on the internet: www.nederlandwereldwijd.nl (see Appendix 6.1 for more information). In the event of travel or a stay abroad, personnel are advised to adhere to the negative travel advice issued by the Ministry of Foreign Affairs.

Long-term stay abroad
Travel abroad in a business or private capacity for longer than six consecutive months may have consequences for the VNO. This applies to both the employee involved and their partner. If there are insufficient possibilities in the country to gather information about the stay there, the CNO will in principle be denied and/or withdrawn.

[9] A summary of high risk countries can be found on the form of the Security screening

Appendix 16.1

Form to report a visit to an ABDO risk country

PERSONNEL CONFIDENTIAL
(If completed)

Reporting a visit to an ABDO risk country
The following information must be provided to report the upcoming travel of an employee holding a Confidential Position or their partner[10].

Company details	
Company name:	
Chamber of Commerce nº:	
Name of SO/person making the report:	

Travel details	
Date of start of travel:	
Date of end of travel:	
Country of destination:	
Place of destination:	
Name of company/organization of destination:	
Reason for visit/subject:	
Travel in private/business capacity:	

Traveler details	
Surname of traveler:	
Prefixes:	
First name of traveler:	
Citizen service number:	
Position of traveler:	
Field of expertise of traveler:	

[10] See Appendix 6.1 for more information

Appendix 17

Security measures and layered structure

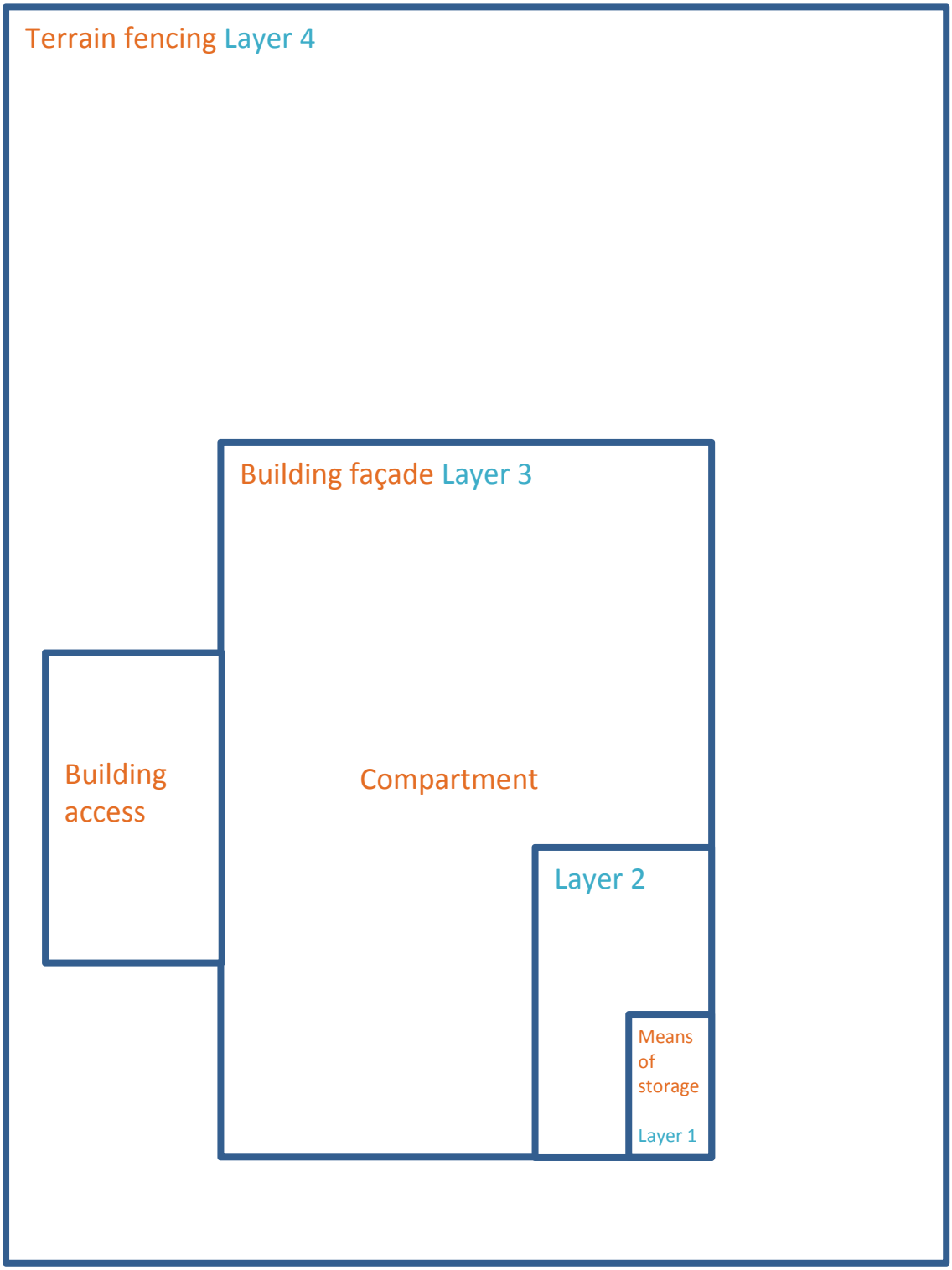
Security measures and layered structure
Security measures are taken to prevent non-authorized persons, particularly those intending to do harm, from accessing a compartment. A thick steel door and bulletproof glass are examples of physical security measures. Optimum security will incorporate several measures that overlap in scope and form several barriers. These barriers can be seen as layers of security around the IBP. A vault, the compartment, the building and the fencing form four different layers of security. If it is not possible to implement a measure prescribed in the ABDO 2017 requirements in a specific layer, the next layer must be made stronger.

The minimum required security measures are laid down in the ABDO 2019.

Examples of layered structures for each IPB category (Appendix 17.2 to 17.5) are classified and therefore only available on request from DISS/ISO.

Appendix 17.1

General situation regarding security measures and layered structure



Appendix 18

Organizational measures

Access control
In Dutch, access control is often referred to using the English term. It is a term that encompasses Identification, Authentication, Authorization, approval or denial of access, and all forms of registration in this regard. Access control is the functionality that grants actual access to a specific compartment on the basis of Authorization or denies access to the person seeking it as the case may be. An adequate access control system, as part of the security as a whole, guarantees that only authorized persons can gain access to an IBP compartment. Authentication is a means of checking whether the person who seeks access to a compartment is authorized for it. Authentication is carried out by people (guards) or by an automated system, based on the use of proof of ID, passwords, tokens, biometric data, digital keys, physical keys, etc. The loss of means of authentication, such as a physical or digital key, is a security incident.

Authorization
Authorizations are granted to persons on the basis of “Need-to-be” and “Need-to-Know”. These indicate to which IBPs the persons are authorized to have access. Authorizations are set up in the access control system by the Security Officer (SO). A distinction is made between authorized and non-authorized persons. Whether a person is authorized depends on a number of conditions referred to in Chapter 2. For the correct and comprehensive management of Authorizations, procedures and instructions must be drawn up. Any lack of clarity regarding who is authorized should be reported.

Access of non-authorized persons to an IBP should be kept to a minimum. As far as possible, tasks such as those of in-house emergency response officers (BHV) should therefore be carried out as a sideline activity by authorized persons. Non-authorized persons include persons such as cleaners, facility staff, maintenance personnel, suppliers and external parties involved in a Special Contract.

If a non-authorized person must nonetheless be granted access to a compartment to carry out duties, this person will be accompanied by authorized personnel at all times and the non-authorized person must be identifiable by means of a pass visibly worn that clearly states “VISITOR” (“BEZOEKER”). They must at all times be accompanied by authorized personnel, who are responsible for protecting the IBP. In addition, visitors that are not Dutch nationals must be registered with DISS/ISO five working days before their visit. This registration form is attached to this appendix.

Only electronic equipment that is essential for executing the contract is permitted in the areas containing an IBP. A list of this equipment is included in the security plan.

When leaving a compartment containing an IBP of level 3 or higher, a security round is completed, during which the door of the means of storage, the compartment and, where possible, the building are locked. Windows and doors are locked and the Intruder Detection and Alarm System (IDAS) is activated. In addition, intrusion checks are carried out and the seals of emergency doors are inspected. In the absence of Authorized personnel, security effectiveness is safeguarded.

Logging
The logging functionality of technical systems that have this functionality must be used. The period of time for which the logs must be kept depends on the IBP category, what the system will be used for and the prevailing statutory restrictions. The minimum logging requirements and retention periods are laid down in the Physical requirements Chapter 3. In the event of a security incident, the Logs will be secured without delay, and a longer retention period applies of up to at least the point in time that the investigation into the security incident has been completed. See Appendix 33 for more information in this regard.

Appendix 18.1

Visitor Authorization form

PERSONNEL CONFIDENTIAL
(If completed)

To be completed by ABDO company

Company name	
Security officer	
Location to be visit	

To be completed by ABDO company or visitor

Surname	
First names (in full)	
Date of birth	
Place of birth	
Nationality	
Citizen service number	
For this application a copy of an identification card is required.	
Company name	
Position	
Point of contact	
Date or period of visit	
Purpose of visit	

Name of SO	**DISS/ISO**
Signature	Signature
Date	Date

Appendix 19

Constructional measures

Constructional measures form the backbone of the mix of OCER measures. It is therefore important to include comprehensive constructional measures at the correct security level in plans for new buildings or changes to buildings in good time, to ensure that it is possible for them to be implemented at an acceptable cost. Examples of constructional measures include:

- robust concrete walls;
- reinforced doors;
- bulletproof glass;
- reinforced fittings on doors and windows;
- fencing and other changes to the terrain.

Constructional measures form a barrier to non-authorized persons who attempt to gain access to an IBP. This may be intrusion, often for the purpose of theft, espionage or sabotage, or the unintentional access of non-authorized employees. The effectiveness of these measures strongly depends on the tools that the intruder has at his/her disposal. This can be seen as an offender profile. See Appendix 25 for more information in this regard. This appendix is classified and can be requested from DISS/ISO.

Delay Time
The Delay Time as a result of the constructional measures is the time needed by an intruder from the time of detection to the time that the constructional security of the IBP is breached. The time needed to breach the range of barriers (constructional layers) is the total time from detection to the IBP being reached. Security is effective if the Intervention Time is shorter than the Delay Time.

Compartmentalization
As far as possible, IBPs of the same level for a single contract must be processed and stored in a single compartment. This principle is called Compartmentalization. Constructional security measures are the most effective if the number and size of compartments in which the IBPs are processed and stored can be limited.

Constructional layers
Surrounding the IBP in three dimensions, the floors, walls, partitions and openings therein for the purpose of access, ventilation, etc., must comply with the security requirements. A weak link may mean that the entire security system is insufficient, which is why a layered structure is often applied. This means that the means of storage forms a layer around the IBP, then the compartment in which the means of storage is located, then the building in which the compartment is located, and then the fenced terrain in which the building is located. The measures become more secure from the outside in.

The highest IBP category present determines the extent of the measures to be taken. It should be noted that the presence of a large number of IBPs of a low category can result in a higher level of security.

It is not only the strength of the floors, walls, ceilings, etc. that determine whether a compartment is sufficiently secured, the location is also important. A safety vault on the fifth floor of a ten-storey block of flats is simpler to secure than a room on the ground floor of a building right next to a busy road. This should be taken into consideration when allocating functionalities to compartments.

Constructional measures should overlap as far as possible in order to create the necessary delays to enable timely intervention. The constructional layers include the following:

- the means of storage in which the IBP is stored;
- a compartment or the part of the building in which the IBP is stored/situated;
- the façade of the building in which the compartment is located;
- the terrain fencing around the building in which the compartment is located.

It should be determined for each security measure whether organizational, constructional, electronic or response measures should be taken, and which ones.

If a security layer is required by the ABDO 2019, but cannot be realized, the next security layers should be reinforced with additional security measures. It is not always possible, for example to install fencing. In that case, the next security layer, which is the façade or compartment, should be secured more heavily.

Terrain
The first security layer of constructional measures is often formed by the terrain. A building in a surveyable location with a view of the roads and cycle paths contributes to increased security. Land and water infrastructure such as plants, ponds and channels can make life more difficult for intruders. Yet, rubbish bins, containers, ladders, bike sheds and smoking sheds can actually make life easier for intruders.

Parking facilities
It is preferable for parking spaces not to be directly next to the building. Delaying measures could be (concrete) plant pots, posts, etc. An enclosed car park enabling supervision of the use of the car park is recommended.

Measures to restrict visuals and acoustics
In addition to compartmentalization, visual security measures (to prevent people from looking in) and acoustic security measures (to reduce the dissemination of sound) are necessary. Security measures such as these are implemented in meeting rooms, briefing rooms and work areas in which an IBP is discussed or handled.

Visual security measures must prevent non-authorized persons from examining an IBP by observing it from outside the work area, whether or not with the help of optical equipment. These measures are necessary regardless of the Classification and/or Marking.

Acoustic security measures must prevent non-authorized persons from taking cognizance of an IBP by listening in from outside the work area, whether or not with the help of audio equipment. These measures are necessary regardless of the Classification and/or Marking.

The acoustic security measures ensure that what is discussed cannot be heard outside the compartment:
- normal speech is not audible;
- a loud voice is barely audible or comprehensible.

Using special equipment to “tap” Information that is processed or stored digitally must also be prevented. Taking such equipment (GSMs, PDAs, tablets, etc.) into compartments in which Special Information is discussed is therefore prohibited. These compartments should be locked when no-one is present and should be checked for the presence of any bugging equipment as often as necessary in consultation with DISS/ISO.

Appendix 19.1

Overview of norms for burglar resistance

NEN-EN 5096	Burglary resistance - Façade elements with doors, windows, shutters and fixed infillings. - Requirements, classification and test methods.
NEN-EN 1143	Secure storage units - Requirements, classification and methods of test for resistance to burglary.
NEN-EN 1627	Pedestrian doorsets, windows, curtain walling, grilles and shutters. - Burglar resistance. - Requirements and classification.
NEN 5087 **NEN 5096**	Security measures to prevent climbing
NEN 8131	Alarm systems - Intrusion and hold-up systems - System and quality requirements and application guidelines based on European standards for intrusion and hold-up alarm systems
NEN-EN 50131	Alarm systems
NEN-EN 50136	Alarm transmission systems and equipment
NEN-EN 50518	Monitoring and alarm receiving centre including all relevant parts

Appendix 19.2

Table of norms regarding intrusion measures

	IBP 1/ NLD TS	IBP 2/ NLD S	IBP 3/ NLD C	IBP 4/ NLD R
Organizational measures	Security policy	Security policy	Security plan	Security plan
	Security plan	Security plan		
	PSI	PSI		
Constructional measures	Customization	Fittings on windows and doors NEN5096, Resistance class 4	Fittings on windows and doors NEN5096, Resistance class 3	Fittings on windows and Doors Lockable
	Customization	Burglar resistance 10 min. NEN-EN 1627, Resistance class 4	Burglar resistance 5 min. NEN 5096, Resistance class 3	Burglar resistance 3 min. NEN 5096, Resistance class 2
Electronic measures	Customization	Burglar alarm system in accordance with NEN 8131; Grade 4	Burglar alarm system in accordance with NEN 8131; Grade 3	Burglar alarm system in accordance with NEN 8131; Grade 2
	Customization	Alarm transmission in accordance with NEN 50136-1 to private-sector emergency centre	Alarm transmission in accordance with NEN 50136-1 to private-sector emergency centre	Alarm transmission in accordance with NEN 50136-1 to private-sector emergency centre
Means of storage				
If response time <15 min	Customized	NEN 1143; Grade 4	NEN 1143; Grade 2	Lockable means of storage
if response time 15-60 min	N/A.	NEN 1143; Grade 5	NEN 1143; Grade 4	Lockable means of storage
if response time 60-240 min	N/A.	N/A.	NEN 1143; Grade 5	
Response measures (alarm response)	Direct intervention	Through private-sector emergency centre to private security service, supplemented by Police (priority 1)	Through private-sector emergency centre to private security service, supplemented by Police (priority 1)	Through public sector emergency centre to private security service
	Alarm transmission according to NEN 8131; DP4(AL3)	Alarm transmission according to NEN 8131; DP4(AL3)	Alarm transmission according to NEN 8131; DP3(AL2)	Alarm transmission according to NEN 8131; SP2(AL1)

Appendix 20

Electronic measures

Electronic security measures are used to secure a compartment, a means of storage or a restricted- access area, to grant access to these, or to verify an alarm. Electronic security measures include all electrotechnical, electronic or optical equipment that has an observation, operation, signaling or alarm function. For example: Camera Systems (CCTV), a wide range of detectors, access control systems, emergency centres, etc. Security personnel have anti-raid measures at their disposal, including the means to sound an alarm.

Electronic systems are divided into three types according to functionality:

- an Intrusion Detection and Signaling System (IDSS);
- an Electronic Access Control System (EAS (in Dutch ETS);
- a Camera System (CCTV).

In a security management system or 'alarm system', these three functionalities can be combined.

IDSS
The IDSS is implemented to contribute to the Security of an IBP. The aim of an IDSS is to detect and signal (sound the alarm) unauthorized access (or attempt) ahead of time, to a compartment containing an IBP. An alarm sounded by IDSS must at all times be responded to within the Intervention Time set. For IBP 3 and higher, the presence of some form of IDSS is obligatory. The IDSS is a security management system (or equivalent) linked to a private-sector emergency centre (PAC), such that IDSS alarms result in intervention.

EACS (ETS)
An EACS is applied from IBP 3 and upwards, possibly in combination with manual access control. The EACS is a means of ensuring that only authorized personnel have access to a compartment, means of storage or a restricted-access area. The EACS also supplies information with which security incidents can be investigated (such as logs).

CCTV
Camera surveillance plays a role in the prevention and processing of incidents. Cameras can act as a deterrent and can be a means of generating and verifying an alarm notification. Just like other recording equipment, cameras are not permitted in compartments where work is carried out using Special Information. It is possible to use a Camera System to secure access to compartments of this kind.

Appendix 21

Response measures

Response measures
For the security of IBPs, the response to security incidents and suspected security incidents is very important. The normal, secure situation must be restored as soon as possible after an incident. The steps that must be taken depend on specific factors. In the case of a response to an IDSS alarm, for example, it is important that the alarm is verified as soon as possible, because the police only takes action in the case of a validated alarm. After the intervention, the normal situation can be returned to if the SO has determined that the IBP has not been compromised and the security measures still function sufficiently.

The task of the SO in the process of responding to the alarm may be assumed by another authorized person by means of a consignment roster. Often employees who live a short distance away are selected for this.

It is important to carry out an accurate timeline analysis for all IBPs in order to determine the effectiveness of security. For IBP 1 and IBP 2, it is the norm that security must be effective. That means that at all times intervention is carried before the perpetrator can compromise the IBP. The total Delay Time that is created by means of the layers of OCER security measures must thus be compared with the time that it takes a perpetrator to compromise the IBP. IBP 3 and IBP 4 do not require the same level of security effectiveness, although intervention must take place within two hours for IBP 3.

Alarm response process
The flow chart included in Appendix 21.1 shows the steps that have to be taken to respond to an alarm in the event of a security incident such as unauthorized access, burglary or intrusion. A distinction is made between the period that personnel are present in the compartment with the IBP and the period that the compartment is locked (and therefore monitored by the alarm system). These periods largely correspond to regular working hours, although it is not unusual for the compartment to be unoccupied on all working days although it is not unusual for the compartment to not be occupied on a routinely basis during working hours.

Personnel present in a compartment when the secure situation is disrupted (for example, if an unknown person walks into the compartment and tries to open the means of storage) are expected to respond adequately. In doing so, his/her own safety comes first. The situation must in any case be reported to the SO as soon as possible and if possible to a connected private-sector emergency centre (PAS). Private-Sector Emergency Centres have judicial recognition and comply with the provisions of the NEN-EN 50518 norm.

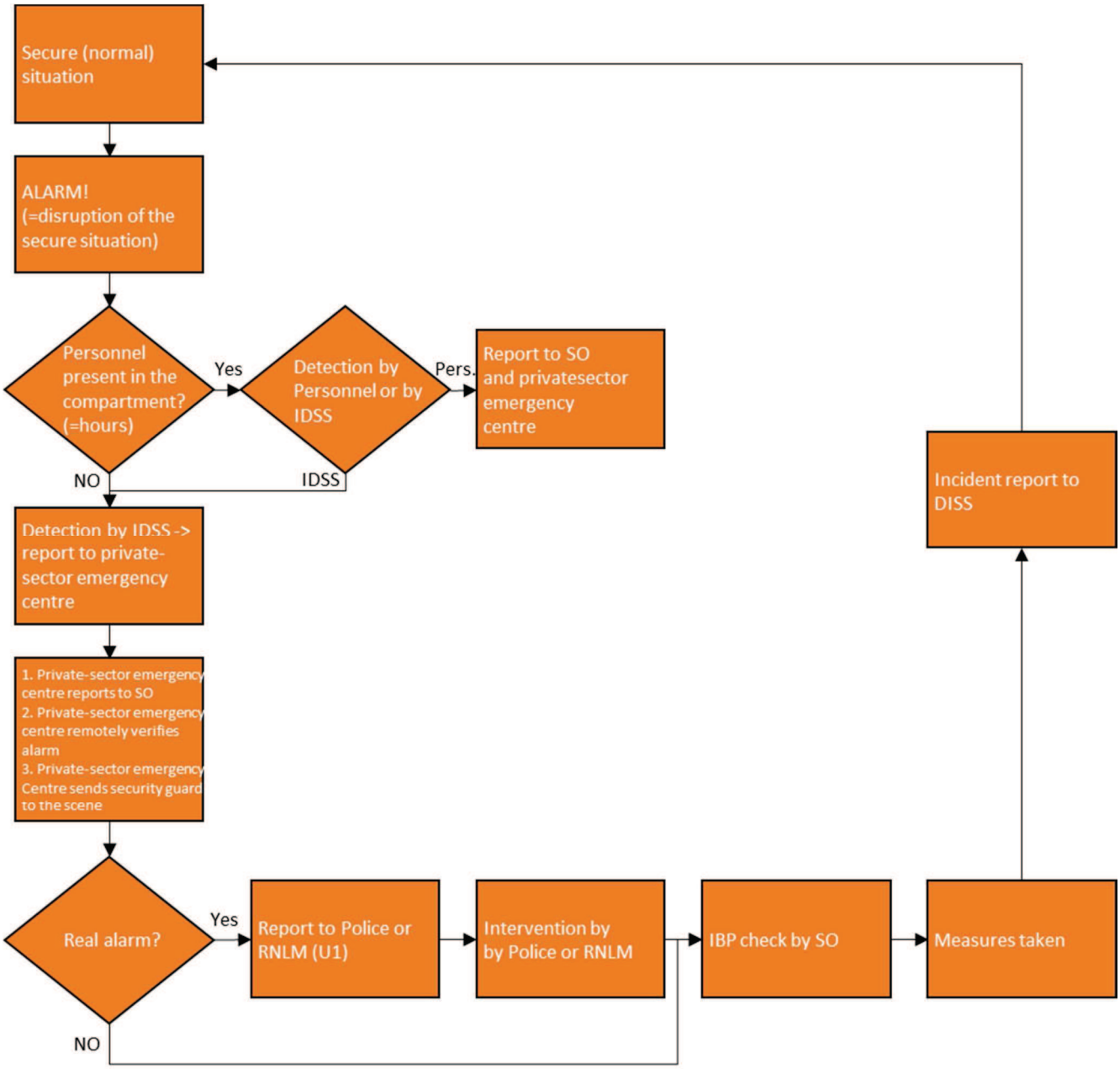
In all cases, it is vital that the intruder (or perpetrator) is detected as soon as possible, so the alarm response can be activated as soon as possible.

Alarm verification
Alarm verification can take place in several ways:
- listening-in using technical equipment connected to the IDSS;
- looking-in using technical equipment connected to the IDSS;
- security personnel on location who look for signs of forced entry;
- a combination of the above.

Alarm verification can also be carried out by authorized personnel who carry out consignment duties and live close to the company. The availability of these persons must be guaranteed and they must have been given clear instructions. With personal safety taken into account, alarm verification by a professional security company is preferred. Technical alarm verification (looking-in/listening-in) in the compartment in which the IBP is located is not permitted. Technical alarm verification is, however, permitted and even preferred in the surrounding areas. A direct link from a private-sector emergency centre to a police control room by means of “Live View”, for example, is also preferable. For personnel charged with alarm response, it is important that they do not have the code and key combination for the storage means of the IBP. Access to the compartment is prohibited to personnel tasked with alarm verification. This is to prevent access being granted to a possible intruder under duress.

Appendix 21.1

Alarm-response procedure



Appendix 22

Transporting and posting a physical IBP

In addition to security measures to protect IBPs within the compartment, it is also necessary for IBPs to be adequately secured during physical transport and postage, whereby transporting and/or posting IBPs should be kept to a minimum.

During transport or postage, IBPs are more vulnerable than when they are at a secure location. After all, it is not possible to fall back on the OCER measures that protect the IBP in the compartment in the normal situation. The increased vulnerability entails a greater risk of the IBP being lost or stolen. In the case of international transport or postage, the vulnerability increases further.

During transport and when being sent by post, the IBP must therefore be packaged in such a way that it is possible to determine whether the IBP has been compromised. In addition, as many measures as possible must be taken to prevent the IBP from being lost or stolen. It is essential that the means of transport can be locked. If a security incident nonetheless occurs, the SO and then DISS/ISO must be informed without delay and an investigation into the incident must be started in accordance with the "Incident Handling" process.

Transportation
Transportation of an IBP refers to the controlled physical transportation thereof, including data carriers (such as USB sticks). The transportation of an IBP must be reported in advance to the SO and, if it concerns State Secrets, to DISS/ISO as well. The SO draws up regulations for the transportation and oversees it. Transport may take place by means of the company's own means of transport and authorized personnel or by engaging a transport or courier company approved by DISS/ISO that is registered with DISS/ISO as a Subcontractor. Transportation of an IBP 1 only occurs through the agency of DISS/ISO.

If international transportation of an IBP is not possible using the company's own means of transport and authorized personnel or by engaging a transport or courier company approved by DISS/ISO, use can be made of the "Government-to-Government" procedure. This entails the IBP being supplied to DISS/ISO for it to be sent on to the foreign government authority in question, which can then deliver it to the addressee if applicable. International transportation of an IBP takes place following approval of the transportation plan by DISS/ISO.

In addition to the requirements and measures for the Security of IBP transport stated in the ABDO 2019, specific bilateral and multilateral agreements have been made for the international transport of Dutch or foreign IBPs. As a rule, these agreements determined in a PSI. DISS/ISO must be informed in advance of the transportation of a foreign IBP.

International transportation of an IBP may only take place following approval of the transportation plan (attached to this Appendix) by DISS/ISO and the security authority or equivalent in the receiving country.

Postage
Postage of an IBP, and SI in particular, refers to it physically being transferred to a postal company for it to be transported to the final destination, as a rule, without being checked. IBPs and, SI in particular, are sent in double packaging in accordance with Appendix 22.4 along with the mass of other pieces of post. When sending SI of level IBP 3 or higher by post, it must be packaged according to Appendix 22.4 and sent by registered post with a track and trace number that makes it possible to find where the item is. The SO must register the details of postage for each item. The party receiving the post must be the Ministry of Defence or a company that has a valid ABDO authorization. Sending an IBP of level 1, and SI in particular, by post is not permitted.

A transportation plan and the requirements regarding the required postage and packaging of IBPs, and SI in particular, are included on the following pages.

Appendix 22.1

Transportation plan

Please approve the following Transportation Plan for the Netherlands:

International transportation plan for the Netherlands (to be submitted in English only)	

A	Consignor and Consignee	
A 1	Consignor [Name, Address, Phone and Fax Number of dispatching Security Officer]	
A 2	Consignee [Name, Address, Phone and Fax Number of receiving Security Officer]	

B	Designated Government Representatives [Name, Address, Phone and Fax Number of authorized Government Point of Contact (PoC) in the dispatching and the receiving country as well]	

C	Description of Consignment	
C 1	Contract or Tender number	
C 2	Export License or other applicable Export Authorization citation	
C 3	Transport License for consignment of hazardous material	
C 4	Consignment Description: [Description of Consignment and Classification level - if possible use abbreviation (C) (S)]	

D	Package description	
D 1	Type of package [e.g. box, card, metal box]	
D 2	Number of packages	
D 3	Number of classified items in each package	
D 4	Package dimensions	
D 5	Package weight	

E	Routing of consignment	
E 1	Date/time of Departure	
E 2	Date/estimated time of Arrival	
E 3	Routes to be used between point of origin, point of export, point of import and ultimate destination [Locations of Transfer - if possible encode locations]	
E 4	Methods of transport for each portion of the consignments [Name and Address of all shipment companies involved - if possible specify Flight, Train or Ship Number]	
E 5	Freight Forwarders/Transportation Agents to be used [Name, Address, Phone and Fax Number of all commercial courier companies involved - The companies have to hold Facility Security Clearances up to the classification and safeguards level necessary]	
E 6	Customs of Port Security Contacts [Name, Phone and Fax Number of PoC's]	

F	Authorized courier	
F 1	Name(s) and identification of authorized Courier [Name, First Name, Date of Birth, Passport-/ID-Card No. and Courier Certificate used]	

G	Security Officer's signature, date and stamp of the requesting facility	

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

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

Appendix 22.2

Posting SI in the Netherlands

(also applies to international SI equivalent).

– : Not permitted
V : Permitted

	NLD TOP SECRET	NLD SECRET	NLD CONFIDENTIAL	NLD RESTRICTED	PERSONNEL CONFIDENTIAL	MEDICAL SECRET	COMMERCIALLY CONFIDENTIAL	UNCLASSIFIED & UNMARKED
Normal post:								
Method of transport (choice from):								
ABDO authorized courier	–	V	V	V				
Registered civilian postal service	–	V	V	V				
Normal civilian postal service	–	–	–	V	V	V	V	V
Transport by own personnel	–	V	V	V	V	V	V	V
Packaging (choice from):								
Security envelope + outer envelope	–	V	V					
Double envelope with the inner envelope sealed.	–	V	V					
Comments:								
Acknowledgement of receipt	–	V	V					

Appendix 22.3

Posting SI to a foreign country

(also applies to international SI equivalent).

– : Not permitted
V : Permitted

	NLD TOP SECRET	NLD SECRET	NLD CONFIDENTIAL	NLD RESTRICTED	PERSONNEL CONFIDENTIAL	MEDICAL SECRET	COMMERCIALLY CONFIDENTIAL	UNCLASSIFIED & UNMARKED
Normal post:								
Method of transport (choice from):								
Escorted diplomatic post	V	V	V					
ABDO authorized courier	–	V	V	V				
Registered civilian postal service	–	–	–	V				
Normal civilian postal service	–	–	–	–	V	V	V	V
Transport by own personnel	–	V	V	V	V	V	V	V
Special delivery due to size:								
Method of transport options								
Dutch/allied transport	V	V	V					
Packaging (choice from):								
Double envelope in which the inner envelope is sealed.	V	V	V					
Security envelope and security case	V	V	V					
Security envelope + outer envelope	V	V	V					
Package packed using packing paper and security tape	V	V	V					
Comments:								
Acknowledgement of receipt	V	V	V	V				

Sending SI to a foreign country is only permitted following consultation with DISS/ISO.

Appendix 22.4

SI packaging

Packaging SI
If SI is sent by post, it must be packaged in carefully addressed envelopes/packages. When sending an IBP of level 2 or higher or internationally classified information of an equivalent level (ATOMAL, SAR, COMINT) or CRYPTO, an acknowledgement of receipt is enclosed.

Packaging SI and classified Information with an international equivalent can take place in two ways, whereby option 1 is preferable:

1. a security envelope as inner envelope with a normal envelope as outer envelope, or:
2. double envelopes with inner envelope sealed with security tape.

Regardless of the packaging method, the inner envelope must at all times bear the classification and marking, if relevant, that apply as a whole to the SI enclosed.

The addressee and the sender must be stated on the inner envelope. If the inner envelope contains CRYPTO, the following must be stated on the inner envelope: UITSLUITEND TE OPENEN DOOR DE CRYPTOBEHEERDER or ONLY TO BE OPENED BY THE CRYPTOCUSTODIAN. The addressee and the sender must be stated on the outer envelope, but not the Classification.

If the SI does not fit in a security envelope, a mailing box must be used or a postal tube for drawings etc. The highest Classification of the contents as a whole must be stated on the mailing box/postal tube. The package must be sealed in such a way that it is not possible to open it without breaking the seal. Ministry of Defence security tape and/or cable security seals are used for this purpose. The addressee and the sender must be stated on the package. If the package contains CRYPTO, the following must be stated on the inner package: UITSLUITEND TE OPENEN DOOR DE CRYPTOBEHEERDER of ONLY TO BE OPENED BY THE CRYPTOCUSTODIAN. The whole package is then wrapped in packaging paper, on which the addressee and sender are stated.

In the event that a steel case is used, it must be sealed using a cable security seal (steel cable with security seal).

SI will not be sent in the event that:

- parts of the address are crossed out or written over;
- the address is written in pencil
- the inner (security) envelope and or packaging show signs of having been opened and closed again.

If SI post is not deliverable at the address stated, it is not allowed to forward it to the addressee if he/she no longer works at the address.

If a delivery includes Crypto resources, the Crypto Custodian is contacted. The Crypto Custodian then gives instructions regarding how to proceed.

Acknowledgement of receipt
If SI classified to IBP level 2 or higher or Information with the equivalent classification (ATOMOL, SAR, COMINT) or Crypto is sent, an acknowledgement of receipt is enclosed (in the inner envelope).

This acknowledgement of receipt states the reference and, if applicable, the copy number of the document and any appendices.

The recipient (who has the correct screening level) signs and dates the acknowledgement of receipt and sends it back to the sender. The sender ensures that he receives the acknowledgement of receipt and makes enquiries if it has not been received within a reasonable period of time. If this does not have the desired effect, the sender informs his/her SO. The SO enquires about the delivery. If the delivery has not arrived, this should be treated as a security incident.

A reasonable period is understood to mean:

- within the Netherlands: 2 weeks;
- within Europe: 3 weeks;
- outside Europe: 1 month.

Appendix 23

Physical storage, processing, development and destruction

Registration
Special Information (BI), of level IBP 3 and higher, and the physical and/or digital access thereto must be registered. This applies both to the SI received from the Ministry of Defence and the products AND documents that have been generated on the basis of the aforementioned SI. The SRC, the PSI and/or special contractual terms are guiding.

The SO or a person designated and authorized to do so must have an up-to-date list available of the SI from IBP level 3 and higher, with details of where it is located and who is managing it. The SO or person designated and authorized to do so has an up-to-date list on file of all SCs above IBP level 4. For IBPs of level 3 and higher, a log must be kept of who has had access to, performed work on, or taken cognizance of the SI. It is essential to Security that the SO keeps a careful log of this kind and that it is accessible. On this basis it is possible to check whether the SI is still present and sufficiently secure.

Labelling
It is important that SI bears the correct (unique) references, Classification and Labelling that indicate how the SI should be handled and stored. More information about the correct application of references, Classifications and Markings is included in Appendix 23.1.

Reproduction of SI
For the continuation of the SC, it may be necessary for reproductions to be made of SI. It goes without saying that this must be limited to what is absolutely necessary. After all, the greater the number of reproductions, the greater the risk of the SI being compromised. Strict norms therefore apply to the reproduction of SI. The reproduction of SI is not permitted without prior permission from the Commissioning Party.

It goes without saying that the same security norms apply to reproductions of an SI or parts thereof as to the original. Documents containing SI are preferably classified per paragraph, to prevent uncertainty occurring. In addition to the original, reproductions must be registered and given unique characteristics, Classifications and Markings if State Secrets are involved.

The means that are used for reproductions, such as printers, scanners and photocopiers, must be secured in the same way and are therefore located in the compartment. This equipment must meet the requirements as laid out in Chapter 4. A security policy for the multifunctional printer can also be requested from DISS/ISO. It provides more information about handling the multifunctional printer in the context of SI.

Destruction of SI
If SI is no longer needed for the SC or if the SC is terminated, it must be destroyed or returned to the Contracting Party. The unnecessary storage of SI leads to an increased risk of compromise and requires efforts for Security to remain in place, which may no longer be necessary.

Requirements apply to the destruction of SI. It is essential in this regard that Information is no longer traceable after destruction.

Destruction is carried out according to a process set up by the SO. To destroy SI (physically or digitally), the SO or authorized person, strictly needs permission from the Commissioning Party. Destruction always occurs under the supervision of an authorized person, whereby functional separation is required. An official report of the destruction must be drawn up at all times and be registered and managed by the SO. See Appendix 23.2 for more information about the destruction and the associated forms.

Appendix 23.1

Labelling an IBP

Information	Classification	Classification text	Method of application	Place of Classification/Marking
Document	Whole document is classified and/or marked.	Classification and/or Marking in capital letters (only on front page or in details of the publication: person who determined the Classification, date on which the Classification was determined and period of validity.	- Handwritten. - Printed. - Stamped.	Top and bottom of every page. On cover. On appendices. (For information about numbering copies and pages, see Chapter 4).
Document	Appendix has a higher classification and/or marking than main document.	Highest Classification and/or Marking in capital letters. (In details of the publication: person who determined the Classification, date on which the Classification was determined and period of validity).	- Handwritten. - Printed. - Stamped.	On the cover of the main document: <highest Classification/Marking> with extension without appendix (x) <Classification/Marking> or <unclassified/unmarked>. On the appendix/appendices at the top and bottom of each page. (For information about numbering copies and pages, see Chapter 4).
Document	Different Classifications in one document.	(SZG): paragraph with Stg. ZEER GEHEIM (NLD TOP SECRET) classified Information (SG): paragraph with Stg. GEHEIM (NLD SECRET) classified Information (SC): paragraph with Stg. CONFIDENTIAL (NLD CONFIDENTIAL) Classified Information (DV) paragraph with Departementaal VERTROUWELIJK (NLD RESTRICTED) Classified Information	- Handwritten. - Printed. - Stamped.	Highest Classification at the top and bottom of each page. Abbreviation of the Classification at the start of each paragraph. (For information about numbering copies and pages, see Chapter 4).
Electronic media (incl. Removable hard drives)	All Classifications and/or Markings.	Highest level of Classifications and/or Markings in capital letters.	Engrave or burn the Classification /Marking onto the data carrier or use a permanent marker to write it on, or use a sticker stating the Classification/Marking, color or a ribbon/label.	Stickers/engraving/text must be visible. If possible, put sticker/engraving/text on both sides.
Workstations	All Classifications and/or Markings.	Highest level of Classifications and/or Markings in capital letters.	Sticker stating Classification / Marking.	Apply stickers visible to system unit and top of screen.
Laptops	All Classifications and/or Markings.	Highest level of Classifications and/or Markings in capital letters.	Sticker with Classification / Marking.	Apply stickers visibly to outside of screen/lid.

Appendix 23.2

Destruction of an IBP

	IBP 1 ZG/NLD TS	IBP 2 G/NLD S	IBP 3 C/NLD C	IBP 4 DV/NLD R
Paper	If IBP 2, burn as well	Shred L<25mm W<3mm	Shred L<25mm W<3mm	Shred L<30mm W<5mm
CD/DVD	Shred AND burn	Shred	Shred	Break
Diskette	Shred AND burn	Shred	Shred	Break
Hard disc	Shred AND burn	Shred	Shred	Drill
USB stick	Shred AND burn	Shred	Shred	Drill
Other	Shred AND burn	Shred	Shred	Destroy

Appendix 23.2.1

Proof of transfer of Information to be destroyed

PROOF OF TRANSFER OF INFORMATION TO BE DESTROYED

The undersigned:_____ Employee ID: _____ Position: _____

requests that the security officer/crypto custodian of: _____(unit)

destroys the following information from the archives of: _____(unit)

Number	Sender	Date	Copy no.	Classification incl. marking	No. of pages	Medium[11]	Comments

Handed over

Taken on

Date: _____

Signature_____

Signature_____

[11] For example: paper, hard disk, DVD, USB stick, etc.

Appendix 23.2.2

Official report of destruction

Ministry of Defence

OFFICIAL REPORT OF DESTRUCTION

On this day, _____ 20_____ , in the presence of

1. _____rank and position_____

2. _____rank and position_____

the information stated on the reverse or in the appendix was destroyed by means of:

_____[1]

In_____

Signature_____ Signature_____

Upon the destruction of classified information, careful attention must be paid to ensuring that no information can be reconstructed from the remains.

_____

[1] Indicate the method by which destruction took place

- burning
- pulverizing/fragmentation
- burning followed by pulverizing
- shredding
- shredding followed by burning
- solution using chemicals
- removal by means of deletion or overwriting

Appendix 24

The tasks and responsibilities of the Cyber Security Officer/Deputy Cyber Security Officer

The Cyber Security Officer and Deputy Cyber Security Officer
The Cyber Security Officer (Cyber SO) is charged with the daily responsibility for cyber security and can be supported in these activities by one or more designated Deputy Cyber Security Officers. The Deputy Cyber Security Officer(s) can, for example, substitute for the Cyber SO in his / her absence, or one could be designated to do so for each location of the company or on the basis of specific specializations within the digital field. The executive board recommends to DISS / ISO a suitable Cyber SO / Deputy Cyber SO candidate in accordance with the requirements, tasks and responsibilities as laid out in the ABDO. The Cyber SO has direct and independent access to the executive board of the organization regarding Cyber security. (For the Cyber SO and Deputy Cyber SO application form, see Appendix 24.1)

Minimum requirements for the appointment of a Cyber Security Officer/Deputy Cyber Security Officer
As a minimum, the Cyber Security Officer / Deputy Cyber Security Officer must:

- have the Dutch nationality and be employed by the company in question;
- have sufficient autonomy, authority, power and seniority;
- have been screened for the highest level applicable to the Special Contracts that the company performs;
- have direct and independent access to the CEO, senior management or executive board;
- have expertise with regard to cyber security and IT infrastructures at the level of Certified Information Systems Security Professional (CISSP).

Tasks and responsibilities
With regard to ABDO Authorization, the Cyber SO / Deputy Cyber SO is responsible for:

- being the first point of contact on behalf of the Contractor for DISS and representing the Contractor for all digital security aspects, and being authorized to take the required measures and decisions;
- setting up the cyber security section of the Security Plan in relation to the Special Contracts and IBP in accordance with the requirements of the ABDO 2019;
- implementing necessary changes to the Security Plan within the set timeframe following an increased threat level or an incident;
- regularly updating the cyber security section of the Security Plan (approved by DISS / ISO) based on the progress of the Special Contracts and having an IBP on site;
- periodically testing the cyber security section of the Security Plan in practice and reporting this in writing to the executive board and DISS / ISO. For a full assessment of the security, the Cyber SO draws up a self-inspection report at least once a year (see Appendix 37) and sends this to the executive board and DISS / ISO;
- giving full cooperation during inspections, audits and investigations at the Contractor by DISS / ISO;
- reporting, investigating and taking measures regarding incidents. This is carried out according to the Incident Handling process (see Appendix 9);
- in the context of Security Awareness, providing information to employees holding confidential positions at the start of a new Special Contract and periodically during Special Contracts regarding ABDO procedures and the related responsibilities;
- regularly keeping the Deputy Cyber SO up to date regarding procedures and incidents so that these tasks can be carried out by the Deputy Cyber SO in the absence of the Cyber SO;
- having the IT administrator take security measures that guarantee the availability, integrity and confidentiality of the IBP;
- being informed periodically by IT management about the set-up of the digital infrastructure within the company with regard to availability, integrity and exclusivity.
- overseeing, by means of a log, the location, issue, intake and origin of all digital IBPs received by or put under control of the organization;
- periodically inspecting the implementation of the security requirements determined the ABDO;
- on behalf of the board of directors, taking appropriate security measures in the Cyber Security domain, or arranging for them to be taken;
- checking the accuracy of the Authorizations issued;
- periodically having insight into unauthorized equipment and software within the digital infrastructure and the measures taken;
- analyzing logging issues relevant to security and monitoring activities that have an impact on security;
- unblocking blocked accounts;

- granting permission for the screen lock to be disabled/delayed;
- maintaining a log of when the screen lock of a workstation/workstation session was disabled/delayed and the reason why it was necessary to grant permission to do so;
- granting permission for the lock out of a user/administration account to be lifted and for the password to be reset;
- granting permission for a group account to be put into use;
- granting permission for company equipment, information and software to be taken off site;
- granting approval for changes to IBP systems;
- having insight into all external links in the case of remote management;
- arranging for IT management to take security measures to guarantee the Availability, Integrity and Confidentiality of the IBP.

Appendix 24.1

Appointment of Cyber Security Officer / Deputy Cyber Security Officer

Appointment of Cyber Security Officer / Deputy Cyber Security Officer and assigning of responsibilities		
To:	Industrial Security Office Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands	T: +31-70-4419463 E: indussec@mindef.nl

Appointment of Cyber Security Officer / Deputy Cyber Security Officer

I, _____ of _____
(highest administrative body, executive board and/or owner) *(Company/Organization)*

appoint, following approval from DISS/ISO, the following employee as (Deputy) Cyber Security Officer (CSO) in accordance with the provisions laid out in the ABDO 2019.

_____
(full name of ((D)CSO)

Date _____

Signature_____
(Signature of highest administrative body, executive board and/or owner)

I, _____
(full name of appointed ((D)CSO)

Employee of _____

Position _____

Appointed establishment _____

hereby declare to understand and accept the tasks and responsibilities of the (D)CSO as described in Appendix 4 of the ABDO 2019 and to comply with them.

Signature_____
(signature of the ((D)CSO)

Details(D)CSO (mandatory)	
Gender:	
First Name:	
Last Name:	
identity card number:	
Telephone number:	
E-mail address:	

Solely when DISS/ISO refuses the appointed (D)CSO, the applicant will be notified.

Appendix 25

Approval for the use of equipment

In a number of cases, equipment may only be used that has been approved by DISS/ISO, such as crypto equipment or specific software to secure connections.

The equipment approved by the National Communication Security Agency (Nationaal Bureau voor Verbindingsveiligheid) (NVB) of GISS will automatically be approved by DISS/ISO. The list of equipment approved by the NBV is available online on the website of GISS.

In addition, the approval of DISS/ISO also automatically applies to the equipment approved by the Security Authority (SA) of the Ministry of Defence.

Equipment that meets FIPS level 2 or higher are approved for use in combination with an IBP level 4.

Finally, DISS/ISO can also approve equipment itself.

Appendix 26

The Cyber-security awareness training course

The Cyber-security awareness training course covers at least the following:

- the classified contract including the classification;
- the importance of the contract for the Ministry of Defence and the organization and the damage that would occur if the contract is compromised;
- who within the organization is involved in the security of the classified contract of the Ministry of Defence (incl. Project team, Cyber SO, IT management);
- the ABDO as a set of requirements to secure the contract;
- the security plan of the organization to protect against threats;
- general and specific threats in the digital domain (incl. phishing);
- explanation of the measures and the use thereof;
- explanation of the use of security measures;
- reporting incidents and how to act in the event of an incident.

More information and security advice is available from the National Cyber Security Centre (www.ncsc.nl) and the General Intelligence and Security Service (www.aivd.nl).

Appendix 27

Registration of company resources

The proper and accurate registration of company resources is essential. A Configuration Management Database (CMDB) is often used for this purpose. The CMDB contains information about all company resources in the infrastructure of a company or organization that are used for the classified contract. The scope of the mandatory registration of company resources is in principle limited to assets used for the classified contract, including the measures referred to chapter 3 physical and chapter 4 cyber.

When setting up the register of company resources for the classified contract of the Ministry of Defence, the use of existing systems and processes with the organization is preferable. A spreadsheet suffices in cases that involve only a very small network or system.

Company resources include things such as:

- hardware;
- software;
- data sets;
- services.

At least the following details of the company resources must be registered:

- a unique identifier (“ID”);
- description of the company resource;
- brand, model, manufacturer and supplier;
- date put into operation;
- physical location;
- user (if assigned to another user “under the name of”);
- classification for the organization for the purpose of determining the value (e.g. assigned to project X or Y);
- IBP level;
- maintenance details. (status, history, schedule);
- particulars;
- configuration, software.

The connections between the ICT business resources are mapped out in a network drawing. Possible elements for a network drawing include:

- networks;
- network segmentation;
- management segment;
- DMZ;
- user environment;
- guest network;
- data storage;
- hardware;
- software;
- external and internal connections;
- location;
- Encryption.

Appendix 28

Mobile equipment and BYOD/CYOD

Mobile equipment includes all devices that do not have a static location. A workstation has a static, registered location. Laptops, smartphones, tablets, etc. do not have a fixed location and are therefore mobile devices. In this context, a 'mobile device' is a device with its own processor capacity. For example, a USB stick is therefore not a mobile device, but a Raspberry-Pi is.

Bring-Your-Own-Device (BYOD) is a term for the equipment that is usually purchased (in a private capacity) by the user him/herself and used in a professional capacity. As a result, the Contractor does not have full control or management of the device.

Choose-Your-Own-Device (CYOD) is a variant of BYOD whereby the user has the choice from devices chosen in advance by the organization.

As the Contractor does not have full control of the device, this goes against the principle that only controlled access is permitted for the security of the IBP.

There are software solutions that claim to provide the answer to this problem. The use of these solutions is permitted in special cases. If this applies, the solution is described in the security plan and the application is approved by DISS/ISO.

Appendix 29

System documentation

System documentation (incl. an Operations Manual) is a document or set of documents that describe the implementation of a system to enable management to be carried out. A proper document is important to be able to take well-founded security measures, in order to restore the system after a disruption, in order to investigate incidents and as a basis for change management. The nature of the documentation is such that it includes descriptions of security measures and information that an attacker could use in the case of an advanced attack. This part of the system documentation must be secured, so that non-authorized persons cannot inspect it or use it.

The scope of the system documentation is in principle limited to the company resources that are used for the classified contract of the Ministry of Defence.

System documentation describes at least the following:

- purpose and use;
- account management;
- changes with regard to factory settings;
- screenshots of management interfaces;
- coherence between systems;
- build-up of systems;
- technical description of hardware;
- which services/processes launch under which account;
- system names;
- file names and locations.

Appendix 30

Labelling data carriers

The purpose of labelling data carriers is to clearly and directly indicate to the person working with the data carriers that the classified data carrier should be handled differently; for example, the data carrier must not be taken elsewhere and USB sticks must not be put into an arbitrary workstation.

If, with a view to attracting unwanted attention, it is not possible to label a data carrier, the colour code below may be used (on a keycord, for example). This must then be described in the security plan and included in the user instructions.

	Red	IBP 1	STG. ZEER GEHEIM, NLD TOP SECRET, COSMIC TOP SECRET, TRÈS SECRET UE/EU TOP SECRET, ATOMAL, SAR, BOHEMIA, COMINT
	Blue	IBP 2	STG GEHEIM, NLD SECRET, NATO SECRET, SECRET UE/EU SECRET, UN STRICTLY CONFIDENTIAL
	Green	IBP 3	CLASSIFIED: CONFIDENTIEEL, NLD CONFIDENTIAL, NATO CONFIDENTIAL, CONFIDENTIEL UE/EU CONFIDENTIAL, UN CONFIDENTIAL
	Yellow	IBP 4	DEPARTEMENTAAL VERTROUWELIJK, NLD RESTRICTED, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED, PERSONEELSVERTROUWELIJK, COMMERCIEEL VERTROUWELIJK, MEDISCH GEHEIM, INTERN BERAAD
	White	UNCLASSIFIED	ONGERUBRICEERD, NATO UNCLASSIFIED, NLD UNCLASSIFIED, UN UNCLASSIFIED

Appendix 31

Users, IT administrators and accounts

An authorized user is someone who by agency of the Cyber SO is authorized to work with special information on an IT system. There must be a reason why the system must be used to perform the classified contract. All other users at the organization are unauthorized users and they must not work on the system. Where the ABDO refers to “users”, this refers solely to “authorized” users.

IT administrators are a special group of authorized users. They have at their disposal the accounts with which the system is managed. The rights of these accounts is often “root” or “administrator” level, which means that it is not possible to technically restrict the information to which the account has access. It may also be possible for IT administrators to make changes to systems without being detected. Extra security requirements are therefore set for the administrator accounts and the administrators themselves.

An account in an IT system is a set of data that determines to which sources the account has access. For user accounts it is determined what the user, as a natural person, has access to. In the context of ABDO, the user account of an IT administrator is called an administrator account. The requirements that apply to user accounts therefore also apply to administrator accounts. In addition to user accounts, there may also be system accounts. System accounts include functional accounts, machine accounts and service accounts.

A group account is a user account that is used by several natural persons. This type of account is only used in special cases. In these cases, a log must be kept of who used the account and when.

Some organizations have what are referred to as “privileged” and “unprivileged” accounts. Administrator accounts can be seen as “privileged” and user accounts usually as “unprivileged”.

As there is a risk that he or she may give preferential treatment to him or herself or others, or damage the organization, users or IT administrators do not have the rights to manage a full cycle of actions in critical information systems.

Administrator activities are only performed when logged in as administrator and normal user tasks only when logged in as a user.

Appendix 32

Large concentration of IBPs

Reference is made in a number of norms to a large concentration of IBPs, to which stricter measures apply.

Below are a number of examples of situations in which these norms apply:

1. **Personnel data**
   The personal details of a single employee of the Ministry of Defence is marked as Personnel Confidential and should be handled as NLD RESTRICTED. If this were to be compromised, the damage would, in principle, be limited to this employee only. The effectiveness of the Ministry of Defence as a whole would not be affected. If, however, all personnel details of part of the organization were to become public knowledge, the effectiveness of the Ministry of Defence as a whole could be jeopardized. Where relevant, sets of personnel data must therefore be secured more tightly. This is always a case of customization.

2. **Several contracts to one Contractor**
   If a Contractor performs several classified contracts and the relevant data is processed on the same infrastructure, a large concentration of IBPs may apply. If compromised, the damage to the Ministry of Defence would be significantly greater. This may lead to data sets such as this having to be secured more tightly. This is always a case of customization.

It is determined per contract whether there is a “large concentration” of IBPs. This is then included in the Security Requirements Checklist (RAL). DISS/ISO can also mark a collection of IBPs as a “large concentration”.

Appendix 33

Logging and Monitoring

Logging and Monitoring are means for determining whether a system has been compromised. The Logging functionality is used to record events. This makes it possible, for example, for a data leak to be signaled on the basis of deviations from the standard. Monitoring makes it possible, for example, to gain an indication of whether malware (including Advanced Persistent Threats; APTs) is present on a system or network on the basis of Indicators of Compromise (IOCs). Once an incident has been observed or is suspected, the Logging and Monitoring functionalities can be used to investigate the incident. Logging and Monitoring can also be used to identify Command & Control (C2) traffic.

At least the following information is saved in log files:

- use of technical management functionalities, such as changes to configurations, settings or updates;
- execution of a system command, starting and stopping, execution of back-up or restore;
- use of functional management functions, such as changes to configurations or settings, the release of new functionality, intervention in data sets (including databases);
- security management actions such as promoting and demoting users, assigning and withdrawing rights, resetting passwords, issuing and retracting crypto keys;
- security incidents (such as the presence of Malware, testing for Vulnerabilities, erroneous attempts to log in, breach of authorization powers, refused log-in attempts, use of non-operational system services, the starting and stopping of security services);
- disruptions to the production processes (such as overload, system errors, interruption during execution of software, unavailability of programme parts or systems that are called up);
- actions of users and system administrators, such as system access, online transactions, and access to files.

A log entry contains:

- a user name or ID that can be traced back to a natural person;
- the event;
- if possible the identity of the workstation or the location;
- the object on which the action was carried out;
- the result of the action;
- the date and time of the event.

In large or complex systems it is advisable to arrange for Logging to be managed by a Security Information and Event Management System (SIEM). The systems that generate log messages are connected to it. An SIEM then generates notifications and alarm signals for the management organization.

Appendix 34

Virtualization and VLAN

When implementing/installing a virtualized infrastructure, the following should be taken into account:

- only the necessary Operating System (OS) components and services are activated;
- connections from Virtual Machines (VMs) with unnecessary physical equipment is prohibited;
- file sharing between the host and guest OS is deactivated;
- the use of resources by a VM is limited;
- physical switch ports connected with a virtual trunk port are always configured statically;
- a virtual switch is not connected with other virtual switches or physical switches;
- VM production and test environments are separate;
- a firewall has been installed and activated to protect the host;
- The guest and host OS's must be patched regularly.

Important points for safeguarding proper control where virtualization applies:

- a monthly inspection of the virtual environment;
- individual log-in attempts will be checked for irregularities on a weekly basis;
- Central Logging takes place on the guest OS;
- VM 'sprawl' as a result of creating and distributing VM's is not possible;
- migrations from VMs are logged and supervised;
- the use of Introspective Capacity such as Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) is recommended.

Important points regarding the traceability to individual users and system functions are:

- no administrators are permitted to log in as "administrator" or "root";
- administrators must log in to personally allocated accounts;
- network access to the host is limited to administrators for management tasks;
- network management is separate from operational traffic of the guest OS;
- the use of Two-factor Authentication for access to the host system;
- the use of passwords for access to the Basic Input/Output System (BIOS) and "boot loaders";
- management of "hypervisors" is limited to administrators and is centralized;
- the use of Encrypted communication for the management of the OS host;
- guest OSs are excluded from access to the administration network.

VLANs make it possible to realize logically separate networks on physical separated hardware. As a result separate network segments can be assigned specific functions, for example. When implementing VLANs, take the following into account:

- drawing up a VLAN number plan/implementing a process for registering the issue and revocation of VLANs;
- ensuring correct and up-to-date documentation of the configuration;
- checking on a monthly basis that the VLAN separation in the configuration is still correct;
- arranging patch management.

Appendix 35

Demilitarized Zone (DMZ)

A DMZ is a network segment between an untrusted environment (such as the internet) and the network on which the IBP is located. Servers can be placed in this segment that inspect the traffic on the basis of the content of the traffic.

There are Network Perimeter Devices in the DMZ, and incoming and outgoing traffic is checked and/or terminated for example by a proxy and malware scanner. The Network Perimeter Devices must have a span port. The proxy logs individual TCP sessions, and blocks specific URLs, domain names and IP addresses in accordance with a blacklist. There are also servers in the DMZ which permit connectivity from the internet and the trusted network.

Appendix 36

TEMPEST

TEMPEST
Electronic devices emit electromagnetic radiation. When processing Information on these devices, there is the risk that processed Information can be traced from the electromagnetic radiation emitted. This phenomenon (compromising emissions) and the measures that can be taken to minimize this, are referred to as: Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST).

Three types of compromising emissions should be taken into consideration:
- direct electromagnetic emissions;
- transition, if there is irradiation on an electric conductor (for example a heating pipe or water pipe);
- variations in the power supply as a result of data processing.

TEMPEST requirements are set for IBP processing. Physical measures and changes to digital equipment can counteract the above-mentioned vulnerabilities. The measures required depend on the situation.

Threat
A threat arises as a result of the above-mentioned compromising emissions if a non-authorized person is able to intercept and save an electronic/electromagnetic signal and reconstruct the processed images/Information from it.

Measures
The measures to counter the above-mentioned threat are divided into four categories:

1. **Separating systems and networks**
   When implementing the measures, the following must be taken into consideration:
   - separation of unclassified Information and Classified Information;
   - separation of classified Information by dividing against itself (e.g. NLD SECRET and NATO SECRET).

2. **Distance**
Measures that fall into the distance category focus on creating an inspectable and controllable area around the source of radiation. The distance (in metres, in three dimensions, based on the shortest distance) from the source of radiation to the edge of the controllable area determines the “area zone”. The inspectable area is the area over which the owner has control and can carry out independent inspections. The controllable area is the area around the inspectable area for which measures have been taken to exercise control over the personnel and vehicles that are in it.

3. **Equipment**
Measures that fall into the equipment category are intended to minimize the amount of radiation emitted.

4. **Installation**
Measures that fall into the installation category are intended to minimize the risk of transition or variations in the powers supply. In order to combat compromising emissions of this kind, measures have been determined with regard to cabling, installation distances and filtering.

Method
The necessary measures for processing classified information are determined in collaboration with DISS/ISO. To this end, it may be necessary to take measurements of the proposed areas. The process and regulations concerning TEMPEST measures are based on classified NATO regulations.

Appendix 37

Self-inspection

Organizations must periodically inspect the prescribed security measures on the basis of the ABDO with regard to their currency and effectiveness. The self-inspection report can act as a guide for these inspections.

In the self-inspection report each security requirement relevant to the contract will be assessed and any comments will be included. An indication will also be given of what action is needed. A self-inspection report template is available on request.

Each deviation from a requirement in the ABDO results in a risk. In the report, a distinction is made between low risk, medium risk and high risk.

Risk is quantified as the product of the likelihood and the damage that the deviation (the finding) could do (risk = likelihood x damage).

Appendix 38

Identification of workstations

Only workstations that are managed by the organization and are specifically deployed for the purpose of the contract to which the ABDO applies are part of the IT infrastructure. Specific security measures apply to these workstations. To prevent non-approved equipment being connected to the network, a form of automatic identification of the workstations must take place. Various technologies can be applied, for example:

- MAC authentication;
- use of the 802.1X protocol;
- application of the RADIUS server;
- application of domain-member check in the Active Directory.

A combination of technologies is preferable. Which technology should be used in a specific situation is dependent on the size and complexity of the network, the classification and on whether other compensatory measures have been taken.

Appendix 39

Offender profile

NLD RESTRICTED

Appendix 40

Crypto Officer

The Crypto Officer is charged with responsibility for the Crypto resources.

The Crypto Custodian is responsible for:

- the authorization of users of crypto resources;
- the registration of crypto resources in use;
- the implementation of cryptographic techniques in accordance with the prevailing legislation and regulations AND the guidelines of the Ministry of Defence;
- the management of CCI equipment;
- the issue of CCI equipment;
- the periodic inspection and counting of CCI equipment;
- the supervision of and reporting on CCI equipment;
- the storage of CCI equipment;
- the packaging of CCI equipment;
- the transportation of CCI equipment;
- the disposal and destruction of CCI equipment.

The forms in this appendix are for the appointment and release of crypto officers.

Appendix 40.1

Statement of non-disclosure for the duty of secrecy of employees holding a Confidential Position in the context of a CRYPTO position

The undersigned:

Name :_____

Date of Birth :_____

Place of Birth :_____

Appointed position :_____

Hereby declares that he/she:

- with a view to the CRYPTO duties, including the application of resources and the handling and examination of CRYPTO, CRYPTO SECURITY or CCI-marked materiel with which I shall be charged;
- has taken cognizance of the security measures prescribed for the CRYPTO company, as described in the Communication Security Regulations for Physical Security (Verbindingsbeveiligingsvoorschrift Fysieke Beveiliging; VBV 41000 B);
- with attention drawn in particular to the content of Sections 2, 3, 4, 5, 23, 98, 98a, 98b, 98c, 272, 273 and 463 of the Criminal Code;
- full duty of secrecy has been imposed on him/her with regard to the CRYPTO activities carried out by him/her.
- has been informed that, in the event that I have taken any oath and/or signed any declaration, as a result of which I have a duty to report in certain circumstances, or a duty to report pursuant to a relationship I have or will have with others, I will NEVER mention, whether directly or indirectly anything regarding my activities as mentioned above and the knowledge resulting from it;
- have been informed that the above-mentioned duty to secrecy imposed on me does not apply, if this is necessary to carry out my duty, with regard to persons who are authorized to perform the same CRYPTO activities or who are expressly authorized to take cognizance thereof.

Place :_____ Date:_____

Signature :_____

Appendix 40.2

Appointment of Crypto Security Officer

Appointment of Crypto Security Officer and assigning responsibilities		
To:	**Industrial Security Office** Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands	T: +31-70-4419463 E: indussec@mindef.nl

Appointment of the Crypto Security Officer

I, _____ of _____
(highest administrative body, executive board and/or owner) *(Company/Organization)*

appoint, following approval from DISS/ISO, the following employee as Crypto Security Officer (CSO) in accordance with the provisions laid out in the ABDO 2019.

_____
(full name of CSO)

Date _____

Signature_____
(Signature of highest administrative body, executive board and/or owner)

I, _____
(full name of appointed CSO)

Employee of _____

Position _____

Appointed establishment _____

hereby declare to understand and accept the tasks and responsibilities of the CSO as described in Appendix 40 of the ABDO 2019 and to comply with them.

Signature_____
(signature of the CSO)

Details CSO (mandatory)	
Gender:	
First Name:	
Last Name:	
identity card number:	
Telephone number:	
E-mail address:	

Solely when DISS/ISO refuses the appointed CSO, the applicant will be notified.

Appendix 40.3

Declaration of release from crypto position

To:	**Industrial Security Office** Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands	T: +31-70-4419463 E: indussec@mindef.nl

The undersigned:

Name :_____

Date of Birth :_____

Place of Birth :_____

Appointed position :_____

Hereby declares:

- that he/she will not reveal to non-authorized persons the classified and/or CRYPTO-SECURITY or CCI-marked information that he/she has taken cognizance of while performing my duties;
- that he/she understand that after termination of the employment/employment contract he/she will remain subject to the statutory and other regulations relating to the secrecy of Information as well as the sanctions for breach of confidentiality laid down in the regulations.
- that he/she no longer has in his/her possession any classified and/or CRYPTO, CRYPTO SECURITY or CCI-marked documents or materiel that were available to him/her in the capacity of his/her position.

Place :_____ Date:_____

Signature :_____

Appendix 41

Details ABDO Company

Form technical details ABDO company		
To:	**Industrial Security Office** Counter-Intelligence and Security Division Defence Intelligence and Security Service MPC 58B PO Box 90701 2500 ES The Hague Netherlands	T: +31-70-4419463 E: indussec@mindef.nl

ABDO company	
Name:	
Address:	
Post code / Place:	
Contact:	
Telephone number:	
E-mail:	

Signature
Name of SO
Date
Signature

Establishment	
Name:	
Address:	
Post code / Place:	
ISP (Internet Service Provider)	

IP address's

Names Domain

Hardware (used for SC)

Software (used for SC)