Ministerie van Defensie

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 and the knowledge institutes and companies. Unlawful practices and covert means are not shunned in an attempt to lay hands on this or gather information regarding it. Proper security is therefore vital.

Your organisation also has valuable property that it does not want to reveal to unauthorized persons. Unfortunately, not everyone is sufficiently aware about that. That, in combination with a low/too low level of security, makes an organisation vulnerable. The security of knowledge, information, materiel and goods, as well as other objects 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 securing information/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 there has been a security incident. For each ministry, these rules have been further detailed in security policy. In the case of the Ministry of Defence, this 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 nececessary 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 organisations and companies with regard to the security of an IBP.
The ABDO 2019 is derived from the abovementioned 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 June 2019.

On behalf of the Minister of Defence,

Brigadier General W.S. Rietdijk
Principal Director of Business
Management / National Security Authority
MOD NL

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 the 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. On the basis of 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 cognisance by non-authorised persons could damage those interests. Non-State Secret SI applies if cognisance by non-authorised 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]

[2] For example, 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.

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

Information may also have a Marking (whether or not in combination with a Classification). A Marking is intended to limit the set of persons authorised to take cognisance 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 deployability 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 damages security 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

The Netherlands Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017; Wiv 2017), Section 10, lays down the measures designated by the Defence Intelligence and Security Service (DISS) 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 authorisation: 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 authorised to award the contract. The company is thus authorised for IBP storage and processing. With only a few exceptions,

this authorisation is awarded per contract and is therefore not a general authorisation[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 taken 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 DISS director;
- 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.

In the context of a NATO or EU SC, these organisations 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 organisations 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 laid down 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 recognisable 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

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

used as a guideline for the intended security regime if the contract is issued by the Ministry of Defence, the ABDO 2019 does apply, 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 authorisation 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, giving an IBP to a non-authorised person, and making available an IBP to a n o n - authorised 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 coming into effect 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 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 the 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 organisation, 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 Organisation

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 organisation, 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 organisation 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 authorisations, 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 organisation**		**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 organisational, 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 organisation 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 specialisations 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 ighest applicable level of classification of the SC; - direct and independent access to all administrative bodies within the organisation.	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 laid down 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 authorisation.	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 recognisable company/part of company that can be legally and organisationally 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, organisations, or personnel involved in EU and/or NATO programmes, barring exceptions laid down 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 centralised 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 authorisation 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 laid down 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 realise 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 Cytographic Item (CCI-marked) 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 tocompromise 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 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 Twofactor 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 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 Virtualisation.

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	**Organising Information Security**		**IBP 1/ NLD TS**	**IBP 2/ NLD S**	**IBP 3/ NLD C**	**IBP 4/ NLD DV**
4.2	Internal organisation		-	-	-	-
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 organisation. The Cyber SO can have third parties within the organisation carry out subtasks.	Appendix 24	●	●	●	●
2	On behalf of the board of directors, the Cyber SO has been authorised 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 organisation.	Appendix 24	●	●	●	●
4	Each year and at the request of DISS/ISO, the Cyber SO provides DISS/ISO with the organisation's 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 organisation.	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 laid down 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 cognisance of them. The rules are laid down 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 authorised users have access.	Appendix 31	●	●	●	●
2	The system prevents unauthorised 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 authorised in advance.		●	●	●	●
4.5	Access to networks and network services		–	–	–	–
6	Remote administration is not permitted.		●	●	●	
7	A procedure has been laid down whereby remote maintenance is only accessible if it is strictly necessary and a connection can only be activated by an authorised 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	Authorisations and user roles are issued per user in accordance with a fixed authorisation 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 unauthorised 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 authorisations 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 authorisations, 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 authorised use is permitted for purposes explicitly determined by the organisation.		●	●	●	●
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 authorisation 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 authorised 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 laid down 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 minimised.		●	●	●	●

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 organisation.		●	●	●	●
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 organisation 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 laid down 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 jeopardise 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 organisation.		●	●	●	●
20	Measures have been taken to combat the spread of Malware and thus limit the damage (e.g. quarantine and Compartmentalisation)		●	●	●	●
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 reestablish 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 authorised 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 synchronisation		–	–	–	–
41	System clocks are synchronised 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 authorised 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	Unauthorised 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 authorised 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 unauthorised 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 (Compartmentalised) 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 unauthorised 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/ISOapproved 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	Virtualisation		–	–	–	–
32	A risk analysis is carried out when applying Virtualisation. The following conditions apply in this regard: - security functions run on physically separate virtualisation 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 Authorisation 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 Authorisation 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.
Authorisation	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 realised 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 organisations 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 cognisance 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 organisation 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 todirect 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 realised 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.
Compartmentalisation	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 cognisance of an IBP.
Compromise	The unauthorised access to or cognisance 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).
Confidentiality	The safeguard that information is only accessible to those authorised.
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 Contract or 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 organisation on the ground of actual or legal circumstances. Having relevant influence on the policy of an organisation can arise from financial, organisational 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 cognisance 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 Authorisation	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	Demilitarised zone. A physical or logical part of the network that contains the external services of an organisation 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 Enryption
Encryption	Changing information using an algorithm so it becomes illegible and incomprehensible to nonauthorised 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 Signalling (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 orfrom 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 Authorisation 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 minimisation 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 Organisation.
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 cognisance of Special Informationif 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.
Provisional Authorisation	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.
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 authorised to access or take cognisance of an IBP and SI in particular.
PSI	Project Security Instruction. A Document in which further security requirements are laid down, usually in the context of a foreign contract.
Reliability	The extent to which the organisation 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 organisation.
Remote Maintenance	Maintenance activities performed externally on equipment internal to the organisation.
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 laid down, 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 cognisance by non-authorisedparties.
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 laid down.
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 recognised.

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 cognisance by non-authorised 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 systemsfor 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 unauthorised 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
Virtualisation	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.