Government of the Netherlands

# ABRO 2026
# Security Requirements

General Security Requirements for
Central Government Contracts 2026

# INTRODUCTION

Geopolitical developments and events such as acts of sabotage in Europe and espionage by state actors stress the need to protect national security interests. The government-wide approach to economic security has further reinforced the attention for this issue. When the Central Government and the police procure products and/or services from a supplier, this may trigger risks to national security. The General Security Requirements for Central Government Contracts (ABRO) 2026 have been prepared to mitigate these risks.

The Central Government and the police are in the possession of information, systems, equipment and objects, also known as Interests to be Protected. In many cases they are important to our national security and malicious parties must be prevented from accessing them or taking cognisance of them at all times. If you are a supplier for the Central Government or the police and you gain access to an Interest to be Protected that affects national security, it is important that sufficient safeguards are in place to guarantee the security level of the Interest to be Protected. In these cases, you must comply with the ABRO 2026 in your role of supplier.

The ABRO 2026 represents the continued development of ABDO 2019, the General Security Requirements for Defence Contracts. With the coming into force of the ABRO 2026, the entire Central Government and the police subject suppliers to the same security requirements where contracts involving Interests to be Protected are concerned. Existing Defence contracts to which ABDO applies, are still subject to ABDO for the term of the contract.
This document is a translation of the original Dutch ABRO 2026. In the event of any conflict or inconsistency between this English translation and the original Dutch text, the Dutch text shall prevail.

ABRO 2026 is adopted to implement article 2 of the 'Kaderbesluit ABRO Rijksdienst', as published in the Government Gazette in The Hague on December 3, 2025.

| | |
|---|---|
| The Minister of Defence | The Minister of the Interior and Kingdom Relations |
| R.P. Brekelmans | F. Rijkaart |

# TABLE OF CONTENTS


| | |
|---|---|
| General | 4 |
| 1. Management and Organisation | 10 |
| 2. Personnel | 18 |
| 3. Physical | 22 |
| 4. Cyber | 32 |
| 5. Cloud | 51 |
| 6. Abbreviations and terms | 56 |
| Appendix overview | 68 |
| • **Appendix 1:** Setting up the security organisation | 69 |
| • **Appendix 2**: Security Officer | 71 |
| • **Appendix 3:** Crypto Custodian | 73 |
| • **Appendix 4:** List of Interests to be Protected | 74 |
| • **Appendix 5:** Physical security | 75 |
| • **Appendix 6:** Constructional measures | 79 |
| • **Appendix 7:** Transport and Sending | 81 |
| • **Appendix 8:** Labelling and destruction of Data Carriers | 83 |
| • **Appendix 9:** Approved Means | 86 |
| • **Appendix 10:** Scrubber | 87 |
| • **Appendix 11:** Cloud | 88 |

## 1. Introduction

The *Central Government* and the police depend on the business community for certain processes, services and products. When the *Central Government* and/or the police procure supplies, services and products they act in the capacity of *Contracting Authority*. When a *Supplier*, hereinafter referred to as *Contractor*, is directly or indirectly involved in *Central Government* contracts that affect national security, the *General Security Requirements for Central Government Contracts (ABRO)* 2026 may apply. *ABRO* 2026 sets requirements for *Contractors* to guarantee the *Confidentiality, Availability* and *Integrity* of *Interests to be Protected* as part of national security. If the proper execution of a purchase order requires a *Contractor* to have access to or come into contact with an *Interest to be Protected* (ITBP), this is referred to as a *Special Contract*. Work on a *Special Contract* requires an *ABRO Declaration*, for which the *National Office for Industrial Security (NOIS)* is the contact point. *NOIS* is also responsible for all aspects of the *ABRO Declaration*.

## 2. Interest to be Protected

All information, *Systems*, materiel, goods and objects requiring some degree of protection are classified as *Interests to be Protected*. There are four categories of *Interests to be Protected*, ITBP 1 to ITBP 4, with ITBP 1 being the most heavily protected category. When an *Interest to be Protected* involves or contains information, *Classifications* or *Markings* are used as well; also see sections 3 and 4.

*Interests to be Protected* are constantly exposed to threats such as crime, extremism, sabotage, terrorism and espionage. The requirements stipulated for the various ITBP categories and *Classification Levels* contribute to resistance to these threats. The level of security measures depends on the nature of the *Interest to be Protected* in relation to the specific threat. Before starting a procurement process, the *Contracting Authority* determines whether it involves an *Interest to be Protected* and what security level is required.

## 3. Special Information

Information that could adversely affect the interests of the State, its allies or one or more ministries if non-authorised persons were to take cognisance of such information, is referred to as *Special Information*. *Special Information* is given a *Classification Level* that is distinguished into *State Secret* and non-State *Secret Special Information*. *State Secret Special Information* is involved when *vital* interests of the State or its allies are at stake, which could lead to (very serious) damage to these interests if non authorised persons were to take cognisance of such information. Non-*State Secret Special Information* is involved if it could lead to damage to the interests of one or more ministries if non-authorised persons were to take cognisance of such information. Also see the summary in the following table.

As part of a *Special Contract*, a *Contractor* may also come into contact with *Special Information* carrying a police or international *Classification*. An overview of the corresponding police, *NATO* and *EU Classifications*, as well as the most common foreign national *Classifications*, can be found on the website.

Depending on the *Classification Level*, *Special Information* falls into an ITBP category. It should be noted that, unlike *Special Information*, an *Interest to be Protected* need not be classified. *Special Information* is always an *Interest to be Protected*, but an *Interest to be Protected* is not always classified.

It is emphasised that *ABRO* 2026 applies to a contract whose *Classification Level* is NLD RESTRICTED when it has been determined by the *Contracting Authority* that the contract involved both affects national security and the relevant *Interest to be Protected* may be transferred to the *Contractor*.

| Interest to be Protected* | Classification | Applicable when: |
|---|---|---|
| ITBP 4 | NLD RESTRICTED | The interest of one or more ministries may be harmed if non-authorised persons take cognisance of this. |
| ITBP 3 | NLD CONFIDENTIAL | The interest of the State or its allies may be damaged if non-authorised persons take cognisance of this. |
| ITBP 2 | NLD SECRET | The interest of the State and its allies may be seriously damaged if non-authorised persons take cognisance of this. |
| ITBP 1 | NLD TOP SECRET | The interest of the State or its allies may be very seriously damaged if non-authorised persons take cognisance of this. |

* *Special Information* is always an *Interest to be Protected*, but an *Interest to be Protected* is not always classified.

## 4. Marking information

Information may also bear a *Marking* (whether or not combined with a *Classification*). A *Marking* aims to restrict the circle of authorised persons taking cognisance by limiting it to a specific group. A *Marking* may also have the objective to implement a specific treatment and security level. If information is only provided with a *Marking*, this may give reason to protect information as NLD RESTRICTED.

## 5. Special Contract

If proper execution of a contract requires a *Contractor* to access or come into contact with an *Interest to be Protected*, this is referred to as a *Special Contract*. Depending on the nature of the *Special Contract*, different chapters or sections of *ABRO* 2026 are applicable. This is determined in advance by *NOIS*. Also see a number of examples in the following table.

| Application of ITBP | Notes | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|---|
| Access-to-site | Work for the *Special Contract* takes place only at a *Contracting Authority's* site | ● | ● | | | |
| Physical storage | Physical storage and processing of *Interest to be Protected* at a *Contractor*'s site | ● | ● | ● | | |
| Digital storage | Digital storage and processing of *Special Information* in a *Contractor*'s digital environment | ● | ● | ● | ● | |
| Cloud service | Use of public *Cloud* solutions | ● | ● | ○ | ○ | ● |

Under a *Special Contract*, the *Contractor* has the contractual obligation to implement security requirements as described in *ABRO 2026*, in line with the ITBP category. Considering not all situations are fully predictable, it can in exceptional cases be necessary to interpret certain security requirements alternatively. In this case, alternative or additional security measures ensuring that the required security level is realised are looked for in coordination with *NOIS* and the *Contracting Authority*.

## 6. International contracts

Companies may also qualify for a *Special Contract* from *NATO*, *EU*, *ESA*, or a foreign government. Thus, in addition to national *Interests to be Protected*, there may be a *NATO*, *EU*, *ESA*, or foreign *Interest to be Protected*. The *Contracting Authority* involved may impose different or additional requirements. The *ABRO Declaration* is then a *Facility Security Clearance (FSC)* and must be interpreted as such in this document. On behalf of these organisations and countries, *NOIS* acts as an intermediary for the company involved. Often, one of the conditions is that agreements are laid down in a *Security Agreement* or a *Memorandum of Understanding (MoU)*.

## 7. Roles and responsibilities within the chain

Securing an *Interest to be Protected* requires safeguarding security within the chain of parties involved. This starts with the service provided by the *Contractor* to the *Contracting Authority*, but also concerns any *Suppliers* of the *Contractor*. Depending on a *Supplier's* involvement, this can be designated as a *Subcontractor* and thus *ABRO 2026* also applies to this party. Hence, *Subcontractors* must have an *ABRO Declaration* for the provision of services or goods under a *Special Contract*.

In applying *ABRO 2026* to a *Subcontractor*, the following principles apply:

- At all times, the *Contracting Authority* continues to be responsible for an *Interest to be Protected* and the associated security risks;
- The *Contracting Authority* is the only party that can give approval where 'approval by the *Contracting Authority*' is stipulated in a requirement;
- The *Contracting Authority* is the only party permitted to accept any residual risks in respect of an *Interest to be Protected*;
- For other requirements where the intended security purpose relates to the cooperation between the *Contractor* and the *Subcontractor* under the *Special Contract*, the following applies:
  - For the term *Contracting Authority* this is assumed to be the *Contractor*;
  - For the term *Contractor* this is assumed to be the *Subcontractor*.

At all times, *NOIS* is responsible for getting approval from and communicating with the *Contracting Authority* as part of *ABRO 2026*.

## 8. Interim change of the security level

Situations may arise where (possibly on the instructions of *NOIS*) a changed threat landscape or a *Security Incident* leads to the need to adjust the security level during the execution of the contract and to implement further security measures. Any consequences will be agreed in specific consultations between the *Contractor*, the *Contracting Authority* and *NOIS*.

## 9. Certificate of No Objection and equivalents

If, under the *Special Contract*, one of the employees of the *Contractor* has access to or comes into contact with an *Interest to be Protected*, in most cases an employee will need a *Certificate of No Objection*. If it involves an international contract, for example provided by *NATO*, *EU* or *ESA*, a *Personnel Security Clearance (PSC)* may be required.

In both cases, a *Security Screening* is carried out by the Security Screenings Unit of the *General Intelligence and Security Service (GISS)* and the *Military Intelligence and Security Service (DISS)*. Where *ABRO* 2026 refers to a *Certificate of No Objection* this may also also be read as referring to its national or international equivalents.

For some *Special Contracts*, for example when only working with ITBP 4 or NLD RESTRICTED, a *Certificate of Conduct* will suffice. This is applied for with and issued by Justis of the Ministry of Justice and Security.

## 10. ABRO Declaration

Before starting the execution of the *Special Contract*, a *Contractor* must have an *ABRO Declaration* at the required level. This can be issued by *NOIS*, provided that *Contractor* meets all *ABRO* requirements at the required level. This explicitly involves an *ABRO Declaration* under a *Special Contract* and not a *Certification*. The *Contractor* is not permitted to publicly announce that it has an *ABRO Declaration*.

An *ABRO Declaration* is issued for each single *Special Contract*. Situations may arise where a *Contractor* works on multiple *Special Contracts* and thus has multiple *ABRO Declarations*. Depending on the nature of the *Special Contract*, different *ABRO* 2026 chapters may apply. This is why an *ABRO Declaration* issued for one *Special Contract* cannot simply be copied for another *Special Contract*

*ABRO* 2026 forms an integral part of the contract between the *Contracting Authority* and the *Contractor*. Changes in the execution of the *Special Contract* or failure to comply with the security requirements or instructions of *NOIS* set out in *ABRO* 2026, are therefore considered a breach of contract. This may lead to suspension or revocation of the granted *ABRO Declaration*, which may result in termination of the contract. Upon termination of the contract, the *Interest to be Protected* must be handed in or destroyed, in accordance with the applicable procedures .

## 11. Use of existing Certifications

Some of the requirements stipulated in *ABRO* 2026 are based on or align with other government and industry standards, such as Government Information Security Baseline and ISO27002. If a *Contractor* has *Certification(s)* or *Assurance Reports*, this can help make the process of obtaining an *ABRO Declaration* more efficient. Ultimately, *NOIS* itself must be able to determine whether the design, existence and operation of security measures are adequate. A *Certification* does not guarantee the issuance of an *ABRO Declaration*.

## 12. Risk Analysis

Prior to the *Special Contract*, a *Contractor* performs a *Risk Analysis*, taking account of the results of the *Risk Analysis* performed by the *Contracting Authority*, relating to the relevant *Interest to be Protected*. This analysis forms the basis for correctly identifying and implementing security measures appropriate to the ITBP category and must continually be taken into account in the *Contractor's* overall risk management.

## 13. Advice and control

*NOIS* is the point of contact relating to and in respect of monitoring the *ABRO Declaration* under the *Special Contract*. To this end, *NOIS* may visit the *Contractor*, for example for:

- **Advice**: During the process of obtaining an *ABRO Declaration* and the *Special Contract*, *NOIS* advises on the measures to be taken to meet the security requirements of *ABRO* 2026 appropriate to the threats and risks of the *Special Contract*. In addition, *NOIS* can proactively approach the *Contractor*, for example to give presentations on security awareness, map out additional threats, or notify potential victims of a *Security Incident*, so as to increase resilience.

- **Compliance check**: *NOIS* carries out a formal, integral compliance check on the implementation and adequacy of the security measures, which is announced in advance. The results are recorded in a report. Failure to address findings in a timely manner may result in the previously issued *ABRO Declaration* being revoked.

- *Security Incident*: After notification of an actual or possible *Security Incident*, *NOIS* conducts investigations into possible *Compromise* of an *Interest to be Protected* and advises on possible additional security measures with the aim of limiting the damage and preventing any recurrence.

## 14. Transitional arrangement (ABDO to ABRO)

*ABRO* 2026 represents the continued development of *General Security Requirements for Defence Contracts (ABDO)* 2019 to address a government-wide need to safeguard a supplier chain's *Confidentiality, Integrity and Availability*, where it touches on national security. In doing so, adjustments were made to meet different needs within the *Central Government* and police and the security requirements were updated to align with current legislation, technological developments and the current threat landscape

With the coming into force of *ABRO* 2026, *ABDO* 2019 will be fully replaced. Hence, for new contracts, sub-contracts, projects, sub-projects, international contracts, contracts under framework contracts, etc., *ABRO* 2026 will apply. For existing contracts, the version of *ABDO* in force at the time will continue to apply. In this case the use of the current *ABRO* is encouraged.

## 15. Citation to ABRO 2026

These security requirements may be cited as *General Security Requirements for Central Government Contracts* 2026, abbreviated *ABRO* 2026.

## 16. Reading guide

*ABRO* 2026 is divided into five chapters based on the categories: 1) Management and Organisation, 2) Personnel, 3) Physical, 4) Cyber and 5) Cloud. Some requirements are specified in more detail in an appendix. If so, the requirement involved explicitly refers to the related appendix. The abbreviations and terms used in *ABRO* 2026 are in italics and included in the list of abbreviations and terms.

Forms referenced in the requirements and appendices have been made available on the website. In addition, the website includes guidance on various topics to support the *Contractor* in correctly implementing *ABRO* 2026. The guidance is regularly adjusted and updated.

# 1. MANAGEMENT AND ORGANISATION

## Introduction

Adequate security of a *Special Contract* starts with a widely supported, implemented and structurally enforced security policy, endorsed by the *Highest Executive Authority* of a *Contractor*. The *Security Plan*, the Self-Inspection List and the security organisation form the basis for the security of the *Special Contract*.

This chapter includes corporate structure, ownership, *Significant Influence* and *Control*, as these may trigger undesirable influence on a *Contractor* and accordingly the execution of the *Special Contract*.

*ABRO 2026* requires the *Contractor* to nominate an employee for the role of *Security Officer*. The *Security Officer* coordinates the security of the *Special Contract*. Considering the size of the *Special Contract* or the specialisms required, the *Security Officer* may opt to be supported by one or more *Deputy Security Officers* or, for example, by a *Cyber Security Officer*; also see appendix 2

In executing the *Special Contract*, it is important for the entirety of *Suppliers* and *Subcontractors* to be transparent. Even the delivery of in itself 'innocuous' components or services may trigger influence on the *Special Contract*.

If a *Security Incident* occurs or is suspected to have occurred, this must be reported to *NOIS*. The *Contractor* must set up an *Incident Response Procedure (IRP)* to deal with *Security Incidents*.

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **1.1** | **Setting up the security organisation** | | | | |
| 1.1.1 | The *Contractor* must have an integral security policy in place, endorsed by the *Contractor's Highest Executive Authority*. This describes organisational, personnel, physical and cybersecurity aspects. This policy has no impediments to meeting the requirements laid down in ABRO 2026. | • | • | • | • |
| 1.1.2 | The *Contractor* must perform a *Risk Analysis* for the *Special Contract(s)*, taking into account the results of the *Risk Analysis* conducted by *Contracting Authority*. At least once a year, the *Risk Analysis* must be reviewed by the *Contractor* and revised as necessary. It includes at least:<br>• a more detailed description of the type of threats that the *Contractor* must take into account when executing the *Special Contract(s)*;<br>• the identification, analysis and evaluation of the risks involved in executing the *Special Contract(s)*, including the *Interest to be Protected*. | • | • | • | • |
| 1.1.3 | The *Contractor* must establish and implement a risk management process related to the *Special Contract(s)* and the *Interest to be Protected*. | • | • | • | • |
| 1.1.4 | The *Contractor* must nominate an employee to *NOIS* for the role of *Security Officer*, in accordance with the 'Appointment of Security Officer' form. Upon approval, the *Security Officer* will be appointed by *NOIS*. Depending on the nature and size of the *Special Contract(s)*, the number of sites, and the specialisms involved, one or more *Deputy Security Officers* may be appointed, if necessary. | • | • | • | • |
| 1.1.5 | Depending on the nature and scope of the *Special Contract(s)*, the *Contractor* may nominate an employee to *NOIS* for the role of *Cyber Security Officer*, in accordance with the 'Appointment of Security Officer' form. Upon approval, the *Cyber Security Officer* will be appointed by *NOIS*. If necessary, one or more *Deputy Cyber Security Officers* may be appointed; also see appendix 2. | • | • | • | • |
| 1.1.6 | The *Security Officer* acts as the primary contact for *NOIS*. The *Security Officer*:<br>• is employed by the company involved;<br>• has a direct reporting line to the *Highest Executive Authority* of the *Contractor*;<br>• has a sufficient mandate, seniority, execution capability and control over relevant executive staff to carry out responsibilities without interference from superiors;<br>• holds a *Certificate of Conduct* or a *Certificate of No Objection* at the highest applicable *Classification Level* of the *Special Contract(s)*. | • | • | • | • |
| 1.1.7 | If the *Special Contract* involves the use of *Cryptographic Security Solutions*, the *Contractor* must nominate an employee to *NOIS* for the role of *Crypto Custodian*, in accordance with the 'Appointment of Crypto Custodian' form. Upon approval, the *Crypto Custodian* will be appointed by *NOIS*. If necessary, multiple *Crypto Custodians* may be appointed; also see appendix 3. | • | • | • | • |

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 1.1.8 | The *Contractor* must have a *Security Plan* in place, prepared by the *Security Officer*, in accordance with appendix 1. The *Security Plan* is approved by the *Highest Executive Authority* of the *Contractor*, agreed by *NOIS* and uniformly implemented. | ● | ● | ● | ● |
| 1.1.9 | The *Security Plan* must only be accessed by *Authorised Employees* and in preparing and handling the *Security Plan* measures have been taken to safeguard *Integrity* and *Confidentiality*, including the application of *Need to-Be* and *Need-to-Know*. | ● | ● | ● | ● |
| 1.1.10 | To obtain an *ABRO Declaration* the *Contractor* must perform, at the request of *NOIS*, a *Self-Inspection* to estimate the extent to which the *Contractor* complies with the measures required under *ABRO* 2026 and provide it to *NOIS*. To this end, the *Contractor* must use the Self-Inspection List. | ● | ● | ● | ● |
| 1.1.11 | As soon as possible, the *Contractor* must submit an up-to-date record of the *Company Resources* used for the *Special Contract(s)*. The *Contractor* must do so no later than 48 hours after *NOIS*'s request to that effect. | ● | ● | ● | ● |
| 1.1.12 | At least once a year and upon *NOIS*'s request, the *Security Officer* must provide *NOIS* with an overview of all external *IP Addresses*, Internet Service Provider(s) and domain names used by the *Contractor* in accordance with the 'IP addresses and domain names' form. | ● | ● | ● | ● |
| 1.1.13 | When designing security measures, the *Contractor* must take into account prevailing legislation to ensure that the well-being and safety of employees is not compromised. If prevailing legislation, such as the Occupational Health and Safety Act, means that certain security measures cannot be fully implemented, the *Contractor* must take appropriate mitigating measures in coordination with *NOIS*. | ● | ● | ● | ● |
| 1.1.14 | The *Contractor* must fully cooperate with compliance checks and investigations at the *Contractor*, performed by *NOIS* and related to the *Special Contract*. | ● | ● | ● | ● |
| 1.1.15 | Access to an *Interest to be Protected* or *System* pursuant to checks or audits by others than statutory regulators or other bodies mandated by law, is subject to prior approval by *NOIS*. | ● | ● | ● | ● |
| 1.1.16 | In case of inspections, audits and investigations related to the *Special Contract* by third parties (such as *NATO*, *EU* or *ESA*), the *Contractor* must coordinate with *NOIS* in advance | ● | ● | ● | ● |
| 1.1.17 | On termination of the *Special Contract*, the *Contractor* must return all *Interests to be Protected* provided by the *Contracting Authority* or generated during the *Special Contract*, in accordance with a process established together with the *Contracting Authority*, unless the *Contracting Authority*, in coordination with *NOIS*, has given prior written approval to destroy the *Interests to be Protected* through approved procedures and methods. | ● | ● | ● | ● |

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **1.2** | **Security Officer** | | | | |
| 1.2.1 | At the very least, the *Security Officer* is responsible for the tasks described in appendix 2. | • | • | • | • |
| 1.2.2 | The *Security Officer* is charged with taking care of daily security, exercises supervision and performs an annual *Self Inspection* using the Self-Inspection List. The results and follow-up of findings must be recorded in writing and reported to the *Highest Executive Authority* of the *Contractor*. | • | • | • | • |
| 1.2.3 | Every year and if changes occur, the *Security Officer* compares the *Security Plan* and underlying security measures with practice. At the very least, the Self-Inspection List is used for this purpose. The results are recorded in writing and reported to the *Highest Executive Authority* of the *Contractor*, with a copy to *NOIS*. If changes occur, the *Security Plan* must be updated. | • | • | • | • |
| 1.2.4 | Changes to security measures and (policy) changes affecting the security measures related to the *Special Contract(s)* must be provided to *NOIS* for review and incorporated into the *Security Plan*. | • | • | • | • |
| 1.2.5 | Changes to security measures, for example in response to a changed threat landscape or a *Security Incident*, must be recorded in the *Security Plan* within the deadline set by *NOIS*. | • | • | • | • |
| 1.2.6 | The *Security Officer* must keep an up-to-date record of all employees who have a *Certificate of No Objection*, *Certificate of Conduct* and signed *Non-Disclosure Agreement(s)*. | • | • | • | • |
| 1.2.7 | The *Security Officer* must have an up-to-date overview of all *Interests to be Protected* that are managed by the *Contractor*. | • | • | • | • |
| 1.2.8 | The *Security Officer* must keep an up-to-date record of who has performed activities on the *Special Contract* or who has access to an *Interest to be Protected*. | | • | • | • |
| 1.2.9 | The *Security Officer* must keep an up-to-date record of who has which *Special Information* in their possession. | • | • | • | • |
| **1.3** | **Control and corporate structure** | | | | |
| 1.3.1 | For the purpose of the *ABRO Declaration* the *Contractor* must prepare a declaration of 'ownership, *Control* and corporate structure', in accordance with the 'declaration of ownership, *Control* and corporate structure' form and provide it to *NOIS*. | • | • | • | • |
| 1.3.2 | For the purpose of approval the *Contractor* must immediately notify *NOIS*, in writing, of any intended change in ownership, *Control* (including directors), corporate structure or shareholding (including changes as a result of any intended (re)financing) of the *Contractor*, in accordance with the 'Change of ownership, Control and corporate structure' form, such that *NOIS* can review the intended change in a timely manner. | • | • | • | • |
| 1.3.3 | The *Contractor* must immediately notify *NOIS*, in writing, of any intended cooperation with foreign companies or governments. | • | • | • | • |

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 1.3.4 | The *Contractor* must immediately notify *NOIS*, in writing, of each of the following events, in accordance with the 'Change of ownership, Control and corporate structure' form: intended demergers, strategic collaborations, *Outsourcings*, sourcings, mergers, changes in *Significant Influence*, impending partial or full acquisitions (including binding and non-binding offers), business cessations, suspensions of payment, or bankruptcies. | • | • | • | • |
| 1.3.5 | Management decisions relating to intended demergers, strategic cooperations, *Outsourcings*, sourcings, mergers, changes in *Significant Influence* and impending partial or full acquisitions (including binding and non-binding offers) must be immediately submitted in writing to *NOIS* for approval, in accordance with the 'Change of ownership, Control and corporate structure' form, such that *NOIS* can review the intended changes in a timely manner. | • | • | • | • |
| 1.3.6 | The *Contractor* must immediately report to *NOIS*, in writing, any intended change of business operations, sites or changing environmental factors around existing sites that directly or indirectly relate to a *Special Contract*, in accordance with the 'Change of ownership, Control and corporate structure' form. | • | • | • | • |
| 1.3.7 | Relocation of an *Interest to be Protected* or activities under a *Special Contract* other than included in the *Security Plan* only takes place with the written approval of *NOIS* and in coordination with the *Contracting Authority*. | • | • | • | • |
| 1.3.8 | The *Contractor* must clearly state to which (part of the) company and to which site the *Special Contract* will be allocated. As much as possible it must strive to outsource all *Special Contracts* to a single, clearly recognisable and legally and organisationally separated (part of the) company. | • | • | • | • |
| 1.3.9 | Based on a *Risk Analysis*, the *Contracting Authority* may determine, in coordination with *NOIS*, that there are additional risks for which additional security measures must be implemented by the *Contractor*. Examples of additional security measures are mandatory processing or handling by a Dutch based legal entity, on Dutch territory. | • | • | • | • |
| **1.4** | **Classification and additional security arrangements** | | | | |
| 1.4.1 | The *Contractor* must have an up-to-date, contract-specific list of *Interests to be Protected*, completed and approved by the *Contracting Authority*; see appendix 4. | • | • | • | • |
| 1.4.2 | If the *Special Contract* with a foreign *Contracting Authority* requires additional or deviating specific security measures, the *Contractor* must have an up-to-date *Project Security Instruction (PSI)* or *Security Aspect Letter (SAL)*. | • | • | • | • |
| 1.4.3 | Email traffic between the *Contracting Authority* and the *Contractor*, even when it does not contain *Special Information*, must be secured (for instance through Forced TLS) such that *Confidentiality* and *Integrity* is safeguarded. | • | • | • | • |

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 1.4.4 | The *Contractor* must take measures to ensure that *Special Information* with different *Classification Domains* and *Levels* is processed and stored separately. | • | • | • | • |
| 1.4.5 | Prior to generating information under the *Special Contract* to which a *Classification* is reasonably applicable, the *Security Officer* must submit a request for *Classification* to the *Contracting Authority*. Following determination by the *Contracting Authority*, this information must be generated, recorded and handled as such by the *Contractor*. | • | • | • | • |
| 1.4.6 | Any unforeseen situations, for example due to a changed threat landscape, new attack methods, execution of multiple *Special Contracts* at a site or *System*, or knowledge aggregation, may require the stipulation of additional organisational, personnel, physical or *Cyber* security measures, within reasonable limits. The *Contractor* must implement these security measures. | • | • | • | • |
| **1.5** | **Subcontractors and Suppliers** | | | | |
| 1.5.1 | The *Contractor* must submit any intended *Outsourcing* of activities under a *Special Contract* to a *Subcontractor* for prior approval to the *Contracting Authority* and *NOIS*, in accordance with the 'Subcontractor Application' form. | • | • | • | • |
| 1.5.2 | In coordination with the *Contracting Authority* and *NOIS*, the *Contractor* must prepare a contract-specific list of *Interests to be Protected* for each *Subcontractor* and any underlying *Subcontractors* involved in the *Special Contract*, such that it is clear to the *Contracting Authority* and *NOIS* which *Subcontractor* has access to which *Interests to be Protected*; also see appendix 4. | • | • | • | • |
| 1.5.3 | After the *Contracting Authority* and *NOIS* have granted their approval to *Outsource*, the *Contractor* must stipulate the prevailing *ABRO* in the contract with the *Subcontractor* that comes into contact with an *Interest to be Protected* in any way whatsoever. | • | • | • | • |
| 1.5.4 | Following approval by *NOIS* based on a *Facility Security Clearance* provided by a *Foreign Partner*, in the contract with the foreign *Subcontractor(s)* the *Contractor* must stipulate the security requirements applicable in the country involved. In this respect *NOIS* must be provided with a completed list of *Interests to be Protected*. | • | • | • | • |
| 1.5.5 | In coordination with the *Contracting Authority* and based on a *Risk Analysis*, the *Contractor* must determine whether the products and/or services provided by *Supplier(s)* pose a risk to the *Special Contract*. If this is the case, the *Supplier* is considered to be a *Subcontractor* and the *Contractor* must contractually stipulate the applicable *ABRO*. | • | • | • | • |
| 1.5.6 | The *Contractor* is responsible for compliance with *ABRO 2026* requirements by the *Subcontractor*(s). | • | • | • | • |
| 1.5.7 | The *Contractor* must establish and implement a process to continually manage, monitor and review changes to and compliance with security arrangements entered into with *Subcontractor(s)*. If any deficiencies are identified that affect an *Interest to be Protected*, the *Contractor* must inform *NOIS* in accordance with the *Incident Response Procedure*. | • | • | • | • |

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 1.5.8 | When working on the *Special Contract* within a partnership with other companies, the activities related to an *Interest to be Protected* are centralised as much as possible. | ● | ● | ● | ● |
| 1.5.9 | The *Contractor* must provide *NOIS* with an overview of the entire chain of *Subcontractor(s)* and *Supplier(s)* and the countries in which they are located, for all business operations applicable to the *Special Contract(s)* and activities involved in an *Interest to be Protected*. | ● | ● | ● | ● |
| 1.5.10 | When an *Interest to be Protected* is placed with an *Escrow Agent* chosen by the *Contractor*, the prevailing *ABRO* must be contractually stipulated and the *Escrow* Agent must have an *ABRO Declaration* for the *Special Contract* before an *Interest to be Protected* is transferred. | ● | ● | ● | ● |
| **1.6** | **Recordings and publications** | | | | |
| 1.6.1 | The *Contractor* is not permitted in any way to disclose the existence of, or knowledge gained during, the *Special Contract* outside the authorised persons or organisations. This applies to all information whose confidential nature the *Contractor* knows about or can reasonably suspect. Only after prior, express and written approval by the *Contracting Authority* or organisation to which the information belongs, may disclosures about the *Special Contract* be made outside the authorised persons or organisations. | ● | ● | ● | ● |
| 1.6.2 | It is not permitted to make *Recordings* of an *Interest to be Protected* and/or the *Compartment*, other than necessary for the execution of the *Special Contract*, unless prior written approval is obtained from the *Contracting Authority*, in coordination with *NOIS*. | ● | ● | ● | ● |
| 1.6.3 | The *Contractor* is not permitted in any way to (publicly) disclose contact details of, and agreements with, *NOIS*. | ● | ● | ● | ● |
| **1.7** | **Security Incidents** | | | | |
| 1.7.1 | The *Contractor* must establish and implement an *Incident Response Procedure* for handling and evaluating *Security Incidents*. All employees who work on or have access to an *Interest to be Protected* must be familiar with this procedure. | ● | ● | ● | ● |
| 1.7.2 | In case of detection of a *Compromise* of an *Interest to be Protected*, the *Security Officer* must be informed immediately. | ● | ● | ● | ● |
| 1.7.3 | *Security Incidents* must be verified after detection and reported directly to *NOIS* in accordance with the 'Security Incident Report' form. | ● | ● | ● | ● |
| 1.7.4 | Data relating to access to and insight into an *Interest to be Protected* must be recorded and retained for 3 months to enable subsequent investigation of suspected *Security Incidents*. | ● | ● | | |
| 1.7.5 | Data relating to access to and insight into an *Interest to be Protected* must be recorded and retained for 6 months to enable subsequent investigations into suspected *Security Incidents*. | | | ● | ● |

## Chapter 1: Management and Organisation

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 1.7.6 | After *Reporting*, all available information directly related to a *Security Incident* must be retained for a period determined in coordination with *NOIS*. | • | • | • | • |
| 1.7.7 | An evaluation mechanism must be defined that identifies specific lessons learned, for example following a *Security Incident*, and where necessary improvements must be incorporated into the security policy and implemented. | • | • | • | • |
| 1.7.8 | In case of gross negligence or deliberate *Compromise* of an *Interest to be Protected* by an employee, the *Security Officer* must inform *NOIS* directly. | • | • | • | • |
| 1.7.9 | In its security policy the *Contractor* must define how employees who knowingly or unknowingly cause a *Security Incident* are dealt with, what disciplinary measures are available, and that a report will be filed in case of criminal offences. | • | • | • | • |

# 2. PERSONNEL

## Introduction

Personnel security refers to measures aimed at obtaining a degree of assurance that a *Contractor's* employee does not harm the *Confidentiality, Integrity and Availability* of the *Special Contract*. This does not include physical security of personnel or personal protection.

In this section, *Reliability* requirements are imposed on the *Contractor's* employees who perform work on a *Special Contract*. The security awareness of employees is crucial in this respect and employees must be made aware of the potential security risks, for example when travelling abroad for business, and the usefulness and necessity of the security measures taken.

In most cases, having access to or coming into contact with an *Interest to be Protected* under a *Special Contract* requires a *Certificate of No Objection*. If it involves an international contract, for example provided by *NATO*, *EU* or *ESA*, a *PSC* may be required. In both cases, a *Security Screening* is carried out by the Security Screenings Unit of the *GISS* and *DISS*. In various cases, for example if it involves a change of position, or a termination of the *Special Contract*, an employee may be discharged of their role and/or *Position of Confidentiality*. If non-compliance with ABRO 2026 can be traced back to an individual, this may result in the revocation of their *Certificate of No Objection*.

For some *Special Contracts*, for example when only working with ITBP 4 or NLD RESTRICTED, a *Certificate of Conduct* will suffice. This is applied for with and issued by Justis, of the Ministry of Justice and Security.

In case a *Special Contract* involves the police, with activities that may pose a risk to police integrity, a *Background Investigation (BO and BO+)* is carried out by the police.

## Chapter 2: Personnel

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **2.1** | **Security Screening, Certificate of No Objection and Certificate of Conduct** | | | | |
| 2.1.1 | *Employees Involved* must have a *Certificate of Conduct* based on the screening profile set by the *Contracting Authority* for performing the function involved. A *Certificate of Conduct* must not be older than the period specified by the *Contracting Authority*. | • | | | |
| 2.1.2 | *Employees Involved* have a valid *Certificate of No Objection* for fulfilling a *Position of Confidentiality* at the level set by the *Contracting Authority*. A *Certificate of No Objection* must not be older than 5 years. | | • | • | • |
| 2.1.3 | The *Contractor* must keep an up-to-date record of the *Special Contract(s)* and *Employee(s) Involved*, including the *Certificate of Conduct* or *Certificate of No Objection* and the date of issue. | • | • | • | • |
| 2.1.4 | If nationality requirements are set by the *Contracting Authority* in an international contract, they must be complied with by the *Contractor*. | • | • | • | • |
| 2.1.5 | The *Contractor*, in coordination with *NOIS*, has identified whether any employees have *Elevated Privileges or Access Rights* (such as *Administrators*) for the performance of their duties and thus pose an above-average risk to an *Interest to be Protected*. | • | • | • | • |
| 2.1.6 | For *Employees Involved* who have *Elevated Privileges or Access Rights*, such as *Administrators*, facility staff, service desk staff and security analysts, the *Contractor* has put in place additional security measures, in coordination with the *Contracting Authority* and *NOIS*. | • | • | • | • |
| 2.1.7 | If the *Contracting Authority* requires periodic renewal of a *Certificate of Conduct* of *Employees Involved*, the *Security Officer* must apply for a new *Certificate of Conduct* at least 1 month before the expiry of the agreed term. | • | | | |
| 2.1.8 | At least 3 months before the expiry of the deadline for re-examination of a *Certificate of No Objection* of *Employees Involved*, the *Security Officer* must request a renewed *Security Screening*. | | • | • | • |
| **2.2** | **Non-Disclosure Agreement** | | | | |
| 2.2.1 | *Employees Involved* must sign a *Non-Disclosure Agreement*, in accordance with the 'Non-Disclosure Agreement' form. These declarations are kept by the *Security Officer* and specific *Non-Disclosure Agreements* are provided to *NOIS* upon request. | • | • | • | • |
| 2.2.2 | The *Crypto Custodian* is designated as an *Employee holding a Position of Confidentiality* and must sign a *Non Disclosure Agreement*, in accordance with the 'Non Disclosure Agreement *Crypto Custodian*' form. This agreement must be kept by the *Security Officer* and specific agreements are provided to *NOIS* upon request. | • | • | • | • |

## Chapter 2: Personnel

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **2.3** | **Discharge from a Position of Confidentiality** | | | | |
| 2.3.1 | When an employee is discharged by the *Contractor* in the capacity of *Employee holding a Position of Confidentiality*, the *Security Officer* must notify *NOIS*. This includes situations where the following occurs:<br>• change of position of an *Employee holding a Position of Confidentiality*;<br>• dismissal of an *Employee holding a Position of Confidentiality*;<br>• revocation of the *Certificate of No Objection*;<br>• breach of security rules by an *Employee holding a Position of Confidentiality*. | • | • | • | • |
| 2.3.2 | The *Security Officer* must explain the declaration of discharge to the employee, must update the records in which *Certificates of Conduct* and *Certificates of No Objection* are kept, and must ensure that the employee no longer has access to or possession of an *Interest to be Protected*. Upon discharge from a *Position of Confidentiality*, *NOIS* receives from the *Security Officer* a declaration of discharge signed by the employee, in accordance with the 'Discharge from Position of Confidentiality' form. | • | • | • | • |
| 2.3.3 | A procedure is in place for changes at staff level (including changes or terminations of positions or employment contracts) or in the contractual relationship between the *Contractor* and the *Contracting Authority*. At the very least this includes:<br>• revocation of access rights;<br>• repossession of *ICT Resources*;<br>• the responsibilities and duties relating to security of the *Special Contract*, which remain in force even after the termination of employment, such as confidentiality;<br>• how to record actions performed in response to the change or termination. | • | • | • | • |
| **2.4** | **Change of the security organisation** | | | | |
| 2.4.1 | The *Contractor* must cooperate in discharging a *(Cyber) Security Officer* or *Crypto Custodian* at the direction of *NOIS*. This includes situations after or concurrent with the following causes:<br>• violating security rules or policies;<br>• acting in breach of *ABRO 2026*;<br>• failing to comply with instructions from *NOIS*;<br>• failing to comply with legislation relating to the *Special Contract*. | • | • | • | • |
| 2.4.2 | If the *(Cyber) Security Officer* is discharged, *NOIS* must be sent a declaration of discharge signed by the employee, in accordance with the 'Security Officer Discharge' form. | • | • | • | • |
| 2.4.3 | Upon discharge of the *Crypto Custodian*, *NOIS* must be sent a declaration of discharge signed by the employee, in accordance with the '*Crypto Custodian* Discharge' form. | • | • | • | • |
| **2.5** | **Training and awareness** | | | | |
| 2.5.1 | Prior to working on a new *Special Contract* and after that at least once a year, *Employees Involved* must demonstrably complete the relevant course(s). Such course(s) explain the policies and procedures for handling an *Interest to be Protected* and discusses (discuss) relevant threats. | • | • | • | • |

## Chapter 2: Personnel

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 2.5.2 | At least once a year, the *Contractor* must demonstrably inform all *Employees Involved* that they must immediately report security weaknesses to the *Security Officer*. | ● | ● | ● | ● |
| 2.5.3 | At least once a year, *Employees Involved* and internal *Security Personnel* must be trained in carrying out security measures. | ● | ● | ● | ● |
| 2.5.4 | At least once a year, the *Security Officer*, in cooperation with relevant *Employees Involved* and internal *Security Personnel*, must test the operational effectiveness of security measures in practice. To this end, realistic scenarios for *Compromise* must be used, focusing both on potential external and internal threats. | | ● | ● | ● |
| 2.5.5 | The *Security Officer* must make each *Employee holding a Position of Confidentiality* aware of the responsibilities ensuing from holding a *Position of Confidentiality*. | ● | ● | ● | ● |
| 2.5.6 | The *Security Officer* must make every *Employee holding a Position of Confidentiality* aware of possible reasons for a renewed *Security Screening* and advises to *Report* it if such a reason arises. | ● | ● | ● | ● |
| 2.5.7 | The *Security Officer* must provide individual advice and guidance to *Employees Involved* who work on a *Special Contract*, for example on having foreign contacts or taking business trips to a *High-Risk Country*. | ● | ● | ● | ● |
| 2.5.8 | Within a *Compartment*, the *Clear Desk* and *Clear Screen* principles are followed. An *Interest to be Protected* is never left unattended and a *Compact Interest to be Protected* is stored away after use. | ● | ● | ● | ● |
| **2.6** | **Travelling abroad** | | | | |
| 2.6.1 | When an *Employee holding a Position of Confidentiality* takes a business trip to a *High-Risk Country*, the *Security Officer* must report this to *NOIS*, in accordance with the 'Notification of visit to High-Risk Country' form. | ● | ● | ● | ● |
| 2.6.2 | If a business trip under the *Special Contract* requires a *Request for Visit (RfV)*, the *Employee holding a Position of Confidentiality* must submit an *RfV* to *NOIS* for approval in a timely manner, through the *Security Officer*. Without an approved *RfV*, the trip cannot take place. | ● | ● | ● | ● |
| 2.6.3 | The *Security Officer* must brief and debrief the *Employee holding a Position of Confidentiality* on any business trip to a *High-Risk Country*. A debriefing report is prepared and handed over to *NOIS* upon request. | ● | ● | ● | ● |
| 2.6.4 | For a business trip by an *Employee Involved* to a *High-Risk Country* dedicated *Mobile Equipment* must be used, which may only be deployed for this trip and must be wiped upon return. | ● | ● | ● | ● |

# 3. PHYSICAL

## Introduction

In defining the physical security requirements, *Security Effectiveness* is leading and sufficient security measures must therefore be taken to generate the required delaying effect (*Delay Time*). *Compromise* is considered to be the moment when an intruder has unauthorised access to, knowledge of and the opportunity to damage an *Interest to be Protected*, or has the opportunity to take cognisance of or gain access to an *Interest to be Protected*. In preventing *Compromise*, both Organisational, Constructional, Electronic and Reactive measures can be taken.

Based on a *Risk Analysis*, the *Contractor* maps out the physical threats relating to the *Special Contract*. The required *Security Effectiveness* and *Intervention Time* can then be used to determine, in coordination with *NOIS*, which security measures are required. This is based on an inside-out reasoning with the *Interest to be Protected* as the starting point, where the required *Security Effectiveness* is realised based on various security measures. *NOIS* can advise in selecting the required security measures; also see appendix 5.

In addition to the required Organisational, Constructional, Electronic and Reactive measures, this chapter sets out requirements for the physical storage of an *Interest to be Protected* at the *Contractor's* site. This includes processing, development and destruction of an *Interest to be Protected*. When an *Interest to be Protected* is transported or sent it is more vulnerable than when it is located at a secure site. This is why appropriate security measures must be taken to ensure *Integrity* and *Confidentiality* of the *Interest to be Protected* during *Transport* and *Sending*; also see appendix 7.

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **3.1** | **Organisational measures** | | | | |
| 3.1.1 | In its *Risk Analysis* for the *Special Contract(s)*, the *Contractor* must include the methods and tools available to potential intruders to physically compromise the *Interest to be Protected*. | ● | ● | ● | ● |
| 3.1.2 | The *Contractor*, on the basis of the *Risk Analysis* and in coordination with *NOIS*, has established the required *Security Effectiveness*. Based on the *Security Effectiveness* and the *Intervention Time*, the necessary measures (Organisational, Constructional, Electronic, Reactive) must be taken to achieve the required delay effect (*Delay Time*). To this end, the NEN standard referred to in appendix 6.1 must be applied. | ● | ● | ● | ● |
| 3.1.3 | The measures related to the *Intervention Time* must demonstrably safeguard (through certified components) that *Intervention* must take place at the latest 120 minutes after *Compromise* of an *Interest to be Protected*. | | ● | | |
| 3.1.4 | The measures related to the *Intervention Time* must demonstrably safeguard (through certified components) that *Intervention* must take place before *Compromise* of an *Interest to be Protected* (a positive *Security Effectiveness*). | | | ● | ● |
| 3.1.5 | Detection measures must ensure that *Compromise* of an *Interest to be Protected* or attempts to do so are detected within the required time to achieve *Security Effectiveness*; also see appendix 5. | ● | ● | ● | ● |
| 3.1.6 | The physical security measures must be built up according to a layered structure, applying '*Need-to-Know*' and '*Need-to-Be*' principles. | ● | ● | ● | ● |
| 3.1.7 | Access to a *Compartment* with an *Interest to be Protected* must be registered, to safeguard that only *Authorised Employees* have access. | ● | ● | ● | ● |
| 3.1.8 | The access registration for a *Compartment* must at least register the person's name, date and time of arrival, and departure. If it involves a non-digital registration, it must include a signature. | ● | ● | ● | ● |
| 3.1.9 | Access to a *Compartment* requires *Multi Factor Authentication*. | | ● | ● | ● |
| 3.1.10 | Only *Authorised Employees* have independent access to a *Compartment*. | ● | ● | ● | ● |
| 3.1.11 | *Employees* only have access to an *Interest to be Protected* after *Authorisation* by the *Security Officer*. *Authorised Employees* have a *Certificate of Conduct* or, if required, a valid *Certificate of No Objection* of the prescribed level. | ● | ● | ● | ● |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.1.12 | In the event that a *Visitor* is granted access to a *Compartment*:<br>• the visit must be in the direct interest of the *Special Contract*;<br>• the *Visitor* must be registered with the *Security Officer* in advance;<br>• the identity of the *Visitor* must be established in advance;<br>• the *Visitor* must be registered and at the very least the name of the *Visitor* and the date, time of arrival, and departure must be recorded;<br>• throughout the visit, the *Visitor* must constantly be accompanied by an *Authorised Employee*;<br>• the *Visitor* must wear a clearly recognisable and visible visitor's pass;<br>• the employees present must be informed in advance. In response, the employees must take measures to avoid *Compromise*. | • | • | • | • |
| 3.1.13 | Access registration to a *Compartment* must be retained for a minimum of 6 months and provided to *NOIS* upon request. | • | • | • | • |
| 3.1.14 | Within a *Compartment*, the access pass must be worn visibly. The pass must at least bear the person's name. | • | • | • | • |
| 3.1.15 | The intended access to a *Compartment* by a *Visitor* must be submitted to *NOIS* for approval at least 5 working days before the visit, using the 'Visitor Authorisation' form. | | • | • | • |
| 3.1.16 | The security instructions applicable to the *Compartment* must be attached to the outside of the *Compartment*. | | • | • | • |
| 3.1.17 | Issuing *Physical Access Authentication Devices* for a *Compartment* is subject to the following:<br>• on issuing *Authentication Means* for *Physical Access*, it must be verified that the receiving employee has the appropriate *Authorisation*;<br>• issuing *Physical Access Authentication Devices* must be registered;<br>• the registration must be updated at least once a year. | • | • | • | • |
| 3.1.18 | When using *Biometrics*, the equipment must be fitted with security measures to prevent unauthorised physical access to the equipment's content and to prevent unauthorised modification or replacement of the equipment. | • | • | • | • |
| 3.1.19 | When using *Biometric* equipment, *Cryptographic Security Solutions* must be applied to ensure the authenticity, *Confidentiality* and *Integrity* of *Biometric* information. | • | • | • | • |
| 3.1.20 | When using *Biometrics*, the equipment must be demonstrably resistant to known methods used to deceive or bypass *Biometric* equipment. | • | • | • | • |
| 3.1.21 | *Authentication Means for Physical Access* must be certified, in accordance with relevant NEN standards; also see appendix 6.1. | | • | • | • |
| 3.1.22 | Physical keys and spare keys giving access to a *Compartment* must remain at the *Contractor's* site at all times and are only left in a designated *Storage Unit*. Spare keys are never kept in the same *Storage Unit* as the original. | | • | • | • |
| 3.1.23 | *Authentication Means for Physical Access*, digit combinations and *Certificates* are administered by the *Security Officer*. | | • | • | • |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.1.24 | If they are not being used, *Authentication Means for Physical Access* and digit combinations for *Compartments* and *Storage Units* must be stored in a *Storage Unit*, in accordance with appendix 6.1. | | ● | ● | ● |
| 3.1.25 | Digit combinations of *Storage Unit* locks must be changed at the very least every 6 months. They must be changed immediately if:<br>• a new *Storage Unit* or lock is being used;<br>• the *Authorisation* of an employee who knows the digit combination is revoked or changed;<br>• maintenance has taken place on the lock;<br>• *Compromise* is suspected or established.<br><br>When the digit combination is revised, no previously used combination must be chosen. | | ● | ● | ● |
| 3.1.26 | The loss or theft of *Authentication Means for Physical Access* must be treated as a *Security Incident*. | ● | ● | ● | ● |
| 3.1.27 | Physical equipment, security components and *Security Systems* must be administered and maintained to keep them functioning permanently. | ● | ● | ● | ● |
| 3.1.28 | When *Cloud Solutions* are used for the administration and maintenance of physical equipment, security components or *Security Systems*, the supplier of such *Cloud Solutions* must be registered with *NOIS* as a *Subcontractor*. | ● | | | |
| 3.1.29 | It is not permitted to use *Cloud Solutions* for the administration and maintenance of physical equipment, security components or *Security Systems*. | | ● | ● | ● |
| 3.1.30 | *Security Personnel* must have alarm devices at their disposal. | | ● | ● | ● |
| 3.1.31 | When the last employee leaves a *Compartment*, a closing round must be made, during which it must at least be checked that:<br>• the *Storage Unit*, the *Compartment* and, if possible, the floor and/or the building are locked;<br>• windows and doors are locked<br>• everyone has left;<br>• the seals on the emergency doors are intact;<br>• any security measures have been activated (such as an Intruder Detection and Alerting *System*, *IDAS*).<br><br>The closing procedure must be included in the *Security Plan*. | ● | ● | ● | ● |
| 3.1.32 | A *Prohibited Area* must meet ITBP 1 security requirements in all security areas (organisational, personnel, physical and cyber security). | | ● | ● | ● |
| 3.1.33 | The *Security Officer* liaises with the municipality and the local police to stay updated on relevant local developments and any threats regarding the security of an *Interest to be Protected*. If necessary, the *Security Officer* takes additional measures. | | ● | ● | ● |
| **3.2** | **Constructional measures** | | | | |
| 3.2.1 | A *Compact Interest to be Protected* must be stored in a lockable *Storage Unit* that complies with the standards stipulated in appendix 6.1. | ● | ● | ● | ● |
| 3.2.2 | An *Interest to be Protected* must be placed in a *Compartment*. | ● | ● | ● | ● |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.2.3 | The specifications of a *Storage Unit* and/or *Compartment* used to store a *(Compact) Interest to be Protected* must be coordinated with *NOIS*. | | | | ● |
| 3.2.4 | A *Compartment* in which an *Interest to be Protected* is stored must be locked with a certified mechanism, preventing unauthorised access without traces of forced entry; see appendix 6.1. | | ● | ● | ● |
| 3.2.5 | Access doors to a *Compartment* must be fitted with a door closer on the inside and an electronic and audible alarm that goes off when a door is left open for longer than necessary. | | ● | ● | ● |
| 3.2.6 | Emergency doors in a *Compartment* can only be opened outwards. On top of this, emergency doors must be sealed, equipped with an electronic and audible alarm, and alarms are triggered when the doors are opened. | | ● | ● | ● |
| 3.2.7 | *Storage Units* of up to 1000 kilograms must be anchored. | | ● | | |
| 3.2.8 | *Storage Units* of up to 1000 kilograms must be *Chemically Anchored*. | | | ● | ● |
| 3.2.9 | Any *Storage Unit* fixing points that can be accessed from the outside must be physically secured. | | ● | ● | ● |
| 3.2.10 | *Storage Units* must have *Multi Factor Authentication*. | | ● | ● | ● |
| 3.2.11 | *Security Lighting* must be installed around buildings and/or grounds that include an *Interest to be Protected*. | | ● | ● | ● |
| 3.2.12 | When constructing infrastructure such as paving, vegetation or watercourses, burglary prevention must be taken into account. | | ● | ● | ● |
| 3.2.13 | All elements of a *Compartment* must be equipped with measures to restrict visibility. | | ● | ● | ● |
| 3.2.14 | The building in which an *Interest to be Protected* is located is secured against climbing. Loose climbing aids, such as (waste) containers and ladders, must be removed. Rainwater downpipes, low walls and similar features must be equiped with anti-climb protection. | | ● | ● | ● |
| **3.3** | **Electronic measures** | | | | |
| 3.3.1 | It is not permitted to have *Security Systems* for the purpose of securing the *Special Contract* that originate from a country that has an *Offensive Cyber Programme* against Dutch interests. | ● | ● | ● | ● |
| 3.3.2 | *Security Systems* must be installed in accordance with the standards stipulated in appendix 6.1. Maintenance and inspection must be carried out by a certified company (such as with a BORG Certificate), at least once a year. | | ● | ● | ● |
| 3.3.3 | Any unauthorised access, sabotage of *Security Systems*, or any attempts to do so, must trigger an alert and lead to *Intervention* within the required time, to achieve the required *Security Effectiveness*. | | ● | ● | ● |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.3.4 | System clocks of *Security Systems* must use the same time synchronisation and must be protected against changes such that they cannot be modified or manipulated without being detected. | | ● | ● | ● |
| 3.3.5 | It is not permitted to link a *Security System* to a central building administration system or other *Systems* that allow a security system to be administered remotely. | | ● | ● | ● |
| 3.3.6 | Wireless connectivity of *Security Systems* must be disabled and all components must be protected against digital *(Cyber) Compromise*. | | ● | ● | ● |
| 3.3.7 | The only manner in which *Security Systems*, including underlying administration systems, can be connected is through a dedicated and protected administration network. | | ● | ● | ● |
| 3.3.8 | Motion detectors must be equipped with anti-masking measures. | | ● | ● | ● |
| 3.3.9 | In accordance with appendix 6.1, facilities must be implemented outside a *Compartment* to visually recognise persons before they enter the *Compartment*. | | ● | ● | ● |
| 3.3.10 | Camera images must be retained for 28 days. Camera images related to an actual or possible *Security Incident* are retained for as long as necessary for the investigation and handling of the *Security Incident*. In coordination with *NOIS* and the *Contracting Authority*, it may be decided to retain camera images for a longer period. | | ● | ● | ● |
| 3.3.11 | Access to a *Compartment* must be secured through an electronic or mechanical access control system. | | ● | ● | ● |
| 3.3.12 | Where an *Electronic Access Management System (EAMS)* is used, measures are in place to detect situations where access has been gained 'through force'. | | | ● | ● |
| 3.3.13 | An *EAMS* is equipped with an Anti Pass Back *System*. | | ● | ● | ● |
| 3.3.14 | An *EAMS* is equipped with *Logging* and logs must be retained for a minimum of 6 months. The logs must be checked for notable anomalies by the *Security Officer* every month. | | ● | ● | ● |
| 3.3.15 | An *EAMS* is implemented such that when the *System* shuts down or fails, all entrances to the *Compartment* are locked and/or remain locked. | | ● | ● | ● |
| 3.3.16 | A *Compartment* has an emergency button or mechanical panic release for calamities. The procedure around its use must be described in the *Security Plan* | | ● | ● | ● |
| 3.3.17 | An *Interest to be Protected* is equipped with an *IDAS*. The *IDAS* may be installed on the *Compartment*, the *Storage Unit* or the *Interest to be Protected* itself. | | ● | ● | ● |
| 3.3.18 | *IDAS components* are positioned such that *Compromise* of an *Interest to be Protected* or attempts to do so are detected and trigger an alarm. | | ● | ● | ● |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.3.19 | The *Compartment* with an *Interest to be Protected* must be included within the *IDAS* as a separate zone. When no *Authorised Employee* is present in the relevant room, this zone must be activated. | | • | • | • |
| 3.3.20 | Unless *Authorised Employees* are present in the *Compartment*, the *IDAS* is always activated. | | • | • | • |
| 3.3.21 | An *IDAS* can only be deactivated by a designated person, through *Multi Factor Authentication*. | | • | • | • |
| 3.3.22 | The *IDAS* must operate at all times and under all possible conditions. | | • | • | • |
| 3.3.23 | Automatic *IDAS* signalling complies with the standards stipulated in appendix 6.1. | | • | • | |
| 3.3.24 | An automatic *IDAS* alarm must be implemented in coordination with *NOIS*. | | | | • |
| 3.3.25 | The *IDAS* must have a guaranteed power supply that safeguards its operation until at least the maximum *Intervention Time*. | | • | • | • |
| 3.3.26 | The *IDAS* must identify and record any power failure of an *IDAS*. The response to a power failure must be the same as if an alarm has been triggered. | | • | • | • |
| 3.3.27 | Only *Electronic Equipment* strictly necessary for carrying out the activities is permitted in a *Compartment*. The permission to place *Electronic Equipment* in a *Compartment* must be based on a *Risk Analysis*. In this respect, *Electronic Equipment* originating from a country with an *Offensive Cyber Programme* must be excluded. A list of equipment and the accompanying *Risk Analysis* must be approved in advance by the *Contracting Authority*, in coordination with *NOIS*, and must be included in the *Security Plan*. | | • | • | • |
| 3.3.28 | Procedural and other measures must be taken to keep *Electronic Equipment* that is not strictly necessary for carrying out activities outside the *Compartment*. | | • | • | • |
| 3.3.29 | *Electronic Equipment* applied in the security or the buildings management (including *BMS* and connected devices (IOT)) are considered to be *Systems* and are only permitted in a *Compartment* when this is secured at the security level set for the *Special Contract*. | • | • | • | • |
| 3.3.30 | No cameras, smart devices, microphones or other equipment with recording or communication functionality are present in a *Compartment*. | | • | • | • |
| 3.3.31 | Both before a *Compartment* is put into use and if *Means* are added or changed, an *Electronic Security Screening* and *Sound Reduction Measurement* must be carried out, in coordination with *NOIS*. Any measures must be coordinated with *NOIS* prior to implementation. | | | • | • |
| 3.3.32 | Both before a *Compartment* is put into use and if *Means* are added or changed, *TEMPEST* measures must be implemented, in coordination with *NOIS*. The instructions for the required measures can be requested through *NOIS*. | | • | | |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.3.33 | Both before a *Compartment* is put into use and if *Means* are added or changed, a *Zoning Measurement (TEMPEST)* must be carried out, in coordination with *NOIS*. Prior to implementation, any required measures must be coordinated with *NOIS*. The instructions for the required measures can be requested through *NOIS*. | | | • | • |
| **3.4** | **Reactive measures** | | | | |
| 3.4.1 | Alarms from an *IDAS* and *EAMS* must lead to *Intervention* within the required time to achieve the established *Security Effectiveness*. | | • | • | • |
| 3.4.2 | Intervention is carried out by designated and trained *Security Personnel*. | | • | • | • |
| 3.4.3 | In the event of technical or other failures, mitigating security measures are taken to ensure *Security Effectiveness*. | | • | • | • |
| 3.4.4 | Initially, alarm verification must take place on the outside of the *Compartment*. This involves checking all entrances, wall openings, roofs, etc. | | • | • | • |
| 3.4.5 | During alarm verification, *Employees* or *Security Personnel* carrying out alarm verification do not have access to *Authentication Means for Physical Access* that provide access to the *Interest to be Protected*. | | • | • | • |
| 3.4.6 | An *External ARC* has a statutory accreditation and meets the standards set in appendix 6.1. | | • | • | • |
| 3.4.7 | An *Internal ARC* must be secured as a *Compartment* at the security level applicable to ITBP 4. | | • | • | • |
| 3.4.8 | Following an alarm or notification, the *Security Officer* checks the *Interest to be Protected* involved and, if necessary, takes measures to restore the required *Security Effectiveness*. | • | • | • | • |
| **3.5** | **Transport and Sending - general** | | | | |
| 3.5.1 | An *Interest to be Protected* will be taken outside the *Compartment* only if absolutely necessary for the execution of the work. | • | • | • | • |
| 3.5.2 | An *Interest to be Protected* and related equipment, information and software of the *Contractor* used in a *Special Contract* may not leave the *Contractor's Compartment* without prior consent of the *Security Officer*. | • | • | • | • |
| 3.5.3 | In the *Security Plan*, the *Security Officer* must describe how to handle the *Transport* and *Sending* of an *Interest to be Protected* under the *Special Contract*, in accordance with appendix 7. This description must be submitted to the *Contracting Authority* for approval, in coordination with *NOIS*. | • | • | • | • |
| 3.5.4 | Prior to any *Transport* or *Sending* of an *Interest to be Protected*, the *Security Officer* must determine that the receiving party can handle the *Interest to be Protected* in accordance with the established security level and is authorised to have the *Interest to be Protected* at its disposal. | • | • | • | • |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **3.6** | **Physical Sending** | | | | |
| 3.6.1 | Prior to *Sending*, the *Interest to be Protected* must be packaged such that the contents are not visible and not discernible, and detection of intrusion must be possible. | • | | | |
| 3.6.2 | *Sending* an *Interest to be Protected* is only permitted when it is sent by registered mail, with a track and trace number and with immediate acknowledgement of receipt | • | | | |
| 3.6.3 | *Sending* an *Interest to be Protected* by mail is not permitted. | | • | • | • |
| **3.7** | **Physical Transport of Interest to be Protected** | | | | |
| 3.7.1 | The physical *Transport* of an *Interest to be Protected* (such as goods and materiel) is carried out in accordance with the security measures established by the *Contracting Authority*. | • | • | • | • |
| **3.8** | **Physical Transport of Special Information** | | | | |
| 3.8.1 | Prior to *Transport* of *Special Information*, a transport plan must be prepared in accordance with the 'Transport plan' form and submitted to *NOIS* for approval. | | • | • | • |
| 3.8.2 | The transport plan for *Transport* of *Special Information* outside the Netherlands must be submitted to the *Contracting Authority* for approval at least 10 working days prior to *Transport*, in coordination with *NOIS*. | | • | • | • |
| 3.8.3 | *Special Information* is transported in a lockable *Means of Transport* such that the contents are not visible and not discernible, and detection of intrusion must be possible. | • | | | |
| 3.8.4 | *Special Information* must be transported in a *Means of Transport* approved in advance by the *Contracting Authority*. | | • | • | • |
| 3.8.5 | *Transport* of an *Interest to be Protected* must be carried out without unnecessary and unplanned interruptions. The *Interest to be Protected* must always be supervised. | | • | • | • |
| 3.8.6 | *Transport* of *Special Information* must take place in one of the following ways:<br>• hand-carried, either with or without private transport, by an *Authorised Employee*;<br>• by a courier company. | • | | | |
| 3.8.7 | *Transport* of *Special Information* must take place in one of the following ways:<br>• hand-carried, either with or without private transport, by an *Authorised Employee*;<br>• by a courier company approved by a *Contracting Authority*;<br>• the courier company must be registered as a *Subcontractor*. | | • | | |
| 3.8.8 | *Transport* of *Special Information* must take place in one of the following ways:<br>• hand-carried, either with or without private transport, by at least two *Authorised Employees*;<br>• by a courier company approved by a *Contracting Authority*;<br>• the courier company must be registered as a *Subcontractor*. | | | • | |

## Chapter 3: Physical

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 3.8.9 | *Transport* of *Special Information* must only carried out in coordination with, and with the prior approval of, the *Contracting Authority*. | | | | • |
| **3.9** | **Physical storage, processing, development and destruction** | | | | |
| 3.9.1 | An *Interest to be Protected* received or administered by the *Contractor* must be included in an up-to-date registration, showing the site, issue, intake and origin of the *Interest to be Protected*. This registration must be administered by the *Security Officer* and *NOIS* must have the possibility to immediately retrieve it, at all times. | | • | • | • |
| 3.9.2 | *Data Carriers* on which *Special Information* is processed or stored are marked (through labelling), in accordance with appendix 8, with the various *Classification Domains* and *levels* being clearly distinguishable. | • | • | • | • |
| 3.9.3 | Reproduction of *Special Information* may only be done with the approval of the *Contracting Authority*. | | • | • | • |
| 3.9.4 | It is not permitted to make more reproductions than those needed to execute the *Special Contract*. | • | • | • | • |
| 3.9.5 | Reproductions have the same *Classification* as the original, even if only parts of the original have been used. | • | • | • | • |
| 3.9.6 | *Special Information* and any related reproductions must be registered and given a unique copy number. | | • | • | • |
| 3.9.7 | Only designated *Authorised Employees* are permitted to make reproductions. They are also responsible for registering any reproductions. | | • | • | • |
| 3.9.8 | Security measures for reproduction means must be determined in coordination with *NOIS*. | • | • | • | • |
| 3.9.9 | Destruction of *Special Information* must be carried out by an *Authorised Employee*, in accordance with the method of destruction specified in appendix 8, after having obtained permission from the *Contracting Authority*. | • | | | |
| 3.9.10 | Destruction of *Special Information* must be carried out in accordance with the method of destruction specified in appendix 8, by an *Authorised Employee*, under the supervision of a second *Authorised Employee*, and after having obtained permission from the *Contracting Authority*. | | • | • | • |
| 3.9.11 | A confirmation of destruction is prepared by the *Security Officer*, in accordance with the 'Confirmation of destruction' form. | | • | • | • |
| 3.9.12 | The *Contractor* must prepare an *Emergency Destruction Plan*, in coordination with the *Contracting Authority*. The *Emergency Destruction Plan* must be included in the *Security Plan* and must contain procedures and instructions relating to the destruction of an *Interest to be Protected* in an emergency situation. | | • | • | • |

# 4. CYBER

## Introduction

In a *Special Contract*, ICT facilities of the *Contractor* may be important for the execution of the work. The term *Cyber* is not only used to describe the IT infrastructure (the hardware and software) but also includes the associated processes and the human actions involved. Taken together, this must ensure the security of an *Interest to be Protected*. Cyber security is based on a thorough *Risk Analysis* related to processing and storing *Special Information*, setting up both technical measures and the system of activities as a whole, in accordance with the *ABRO* requirements. The security requirements set out in this chapter are structured in accordance with a selection of domains from the Secure Controls Framework (SCF).

*ABRO* 2026 sets requirements for a wide range of cybersecurity measures, explicitly taking into account state actors and their capabilities. Among other things, a *Contractor* must have a clear overview of all IT infrastructure components used to process *Special Information*. On top of that, they should know the whereabouts of *Special Information* and who has access to what. The IT infrastructure must be set up according to modern standards, be up-to-date and be separated from untrusted environments. A multitude of security measures must be taken to have sufficient overview of *Network* and system activities and to detect *Malware*. The use of specific *Cryptographic Security Solutions* also plays an important role in securing *Special Information* at the right security level.

A specific risk to be considered, the requirements for which are included in chapter 3, is the leakage of electromagnetic radiation. Moreover, software development and the implementation of changes must be done in a safe and reliable way, in which business continuity has a major role. The role of employees and the risks involved in human actions are central to all these aspects. This involves both access control and adequately instructing employees in the correct use of *ICT Resources*.

In the field of *Cyber*, a *Cyber Security Officer* may also be appointed in addition to a *Security Officer*; also see appendix 2. The *Cyber Security Officer* supports the *Security Officer* with *Cyber*-related security issues.

Chapter 5 specifically addresses the additional requirements regarding the use of *Cloud Solutions*.

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **4.1** | **Management of ICT Resources** | | | | |
| 4.1.1 | Digital *Special Information* received or administered by the *Contractor* must be included in an up-to-date record, indicating the site, issue, intake and origin of the *Special Information*. This record must be administered by the *(Cyber) Security Officer* and must be immediately retrievable by *NOIS* at any time. | | • | • | • |
| 4.1.2 | *ICT Resources* and the associated software, processes and data collections must be kept updated in a record, including an owner, an *Administrator*, the related *Special Contract* and the interrelationship with other components of the record, including the transfer of data. | • | • | • | • |
| 4.1.3 | System and network components related to a *Special Contract* must be kept up to date in a detailed network diagram. | • | • | • | • |
| 4.1.4 | *Systems* on which *Special Information* is processed and stored must be deployed only within the part of the IT infrastructure set up for the relevant *Classification Domain* and *Level*. | • | • | • | • |
| 4.1.5 | The use of a *KVM switch* to switch between *Systems* of different *Classification Levels* is only permitted when this occurs within the same *Classification Domain* and using *Approved Means*. | • | • | • | • |
| 4.1.6 | *Cloud Solutions* must not be used for the administration and maintenance of physical equipment, security components or *Security Systems*. | • | • | • | • |
| 4.1.7 | The reuse of *ICT Resources* for the execution of a *Special Contract* is permitted under the following conditions:<br>• the *ICT Resource* has previously been used for the same *Classification Domain* and *Level*;<br>• the *ICT Resource* has been wiped for use through *Approved Means*. | | • | • | • |
| 4.1.8 | Before they are used, *Removable Data Carriers* must be checked with a dedicated *Scrubber*, in accordance with appendix 10. | • | • | • | • |
| 4.1.9 | Procedures must be established for the disposal of *ICT Resources*. These procedures must be approved by *NOIS*. | • | • | • | • |
| 4.1.10 | Upon termination of the *Special Contract* or upon disposal of hardware (whether defective or not), the hardware must be wiped through *Approved Means*, using a procedure approved by *NOIS*. If clearance is not possible (or only partially), the hardware must be destroyed in accordance with the methods specified in appendix 8. | • | | | |
| 4.1.11 | Upon termination of the *Special Contract* or upon disposal of hardware (whether defective or not), the hardware must be destroyed in accordance with the methods specified in appendix 8. To this end, a confirmation of destruction must be prepared in accordance with the 'Confirmation of Destruction' form, which is to be provided to the *Contracting Authority* and/or *NOIS* upon request. | | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **4.2** | **Data classification and processing** | | | | |
| 4.2.1 | Prior to any transfer or exchange of *Special Information*, the *Security Officer* must determine that the receiving party is able to handle the *Special Information* in accordance with the established security level and is authorised to have the *Special Information* at its disposal. | • | • | • | • |
| 4.2.2 | *Removable Data Carriers* must only be used as part of an established data exchange procedure. This procedure stipulates, among other things, the specific *Removable Data Carrier* to be used and how it is to be secured, retained, wiped or destroyed. | • | • | • | • |
| 4.2.3 | *Removable Data Carriers* must be provided with a physical label in accordance with appendix 8, based on the highest *Classification* of what is stored on the related *Removable Data Carrier*. | • | • | • | • |
| 4.2.4 | *Data Carriers* containing *Special Information* must be encrypted through *Approved Means*. | • | • | • | • |
| 4.2.5 | Only *Approved Means* must be used to clear *(Removable) Data Carriers* containing *Special Information*. | • | • | • | • |
| 4.2.6 | Data Leak Prevention (DLP) measures must be implemented in *Systems*, *Networks* and other devices on or with which *Special Information* is generated, processed or stored to prevent unintended sharing (such as by email) of *Special Information*. | • | • | • | • |
| 4.2.7 | *Special Information* originating from *NATO* and the *EU*, if established by the *Contracting Authority*, must be processed on a *System* accredited for that purpose. | | • | • | • |
| 4.2.8 | The use of *Artificial Intelligence (AI)* systems is only permitted if these systems meet the requirements for the relevant ITBP category and after approval from the *Contracting Authority*. | • | • | • | • |
| 4.2.9 | When using *AI systems*, data from different *Classification Domains*, *Classification levels* or the *Contracting Authorities* must be separated at all times. | • | • | • | • |
| 4.2.10 | *AI systems* must operate entirely within the *Trusted Network* and must not have any links to untrusted *Networks* or *Systems*. | • | • | • | • |
| 4.2.11 | Upon termination of a *Special Contract*, all data (training data and otherwise), generated outcomes and developed *AI* models that were created on the basis of *Special Information* or are traceable to *Special Information* must be transferred back or destroyed in consultation with *NOIS*, unless otherwise agreed with the *Contracting Authority*. | • | • | • | • |
| **4.3** | **Identification and Authentication** | | | | |
| 4.3.1 | Rules regarding the use of *ICT Resources* (including the use of passwords) must be established, documented and made known to *Users*. | • | • | • | • |
| 4.3.2 | Access to a *System* must be restricted to specifically *Authorised Users*. This must be enforced automatically by the *System* prior to and during a user session. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.3.3 | *Authentication Data* of *Users* must be kept in an up-to-date record, based on which *Users* are *identified* and authorised. | • | • | • | • |
| 4.3.4 | It must be determined on the basis of a *Risk Analysis* where and how segregation of duties is applied and which access *Rights* are granted. The risk assessment, results and measures must be included in an authorisation matrix in the *Security Plan*. | • | • | • | • |
| 4.3.5 | Accounts must not include any indication of the privilege levels of *Users*. | • | • | • | • |
| 4.3.6 | When an authentication token is issued, the *User's* identity and their right to the relevant authentication token must be established. | • | • | • | • |
| 4.3.7 | Accounts must be assigned *Rights* that are necessary for the execution of the *User's* tasks ('*Need-to-Know*', '*Need-to-Use*'). When assigning *Rights*, a distinction must at least be made between reading and writing *Rights* and the applications and commands a *User* has access to. | • | • | • | • |
| 4.3.8 | A *User's Rights* must not include an entire cycle of actions in a critical *System* to secure or execute the *Special Contract*. | • | • | • | • |
| 4.3.9 | *Administrator Rights* must be restricted to *Administrator Accounts*. Administration activities are performed only from *Administrator Accounts*. | • | • | • | • |
| 4.3.10 | General *User* activities, such as use of business applications, email and internet, must be performed using regular *User Accounts*. | • | • | • | • |
| 4.3.11 | *Rights* of *Administrators* must be granted to a restricted group only by means of a *Privileged Access Management (PAM)* solution. Records must be kept of this. | • | • | • | • |
| 4.3.12 | *Rights* granted to *Administrator Accounts* must be reviewed periodically, at least quarterly. | • | • | | |
| 4.3.13 | *Rights* granted to *Administrator Accounts* must be reviewed periodically, at least monthly. | | | • | • |
| 4.3.14 | Activities from an *Administrator Account* must be logged and be traceable to an individual. | • | • | • | • |
| 4.3.15 | Only specifically authorised *Administrators* are permitted to (un) install or (de)activate features and software. | • | • | • | • |
| 4.3.16 | *Service Accounts* must be maintained in an up-to-date record, indicating the owner, the purpose and the date when the *Service Account* was last assessed. The need for a *Service Account* must be assessed at least quarterly. | • | • | • | • |
| 4.3.17 | *System* processes must be performed by unique *Service Accounts*, which are not linked to individuals. IT management, under the supervision of the *(Cyber) Security Officer*, maintains an up-to-date record of *Service Accounts* and associated *Rights*. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.3.18 | If the use of a *Service Account* is necessary for the functionality of a *System*, *NOIS* must approve this exception in advance. The following conditions apply to the use of a *Service Account*:<br>• processing of personal or non-work-related information is not permitted;<br>• any required external access for a *Service Account* must be documented in the *Security Plan*;<br>• using a *Service Account* to log into a *System* is not permitted;<br>• using a *Service Account* via external access is not permitted. | • | • | • | • |
| 4.3.19 | Default or automatically created accounts and other pre-configured accounts must be provided with a new password and disabled by an *Administrator* under the supervision of the *(Cyber) Security Officer*. | • | • | • | • |
| 4.3.20 | A dedicated emergency or 'break glass' account is available that can only be accessed through an 'envelope procedure'. The procedure specifies how a password is released, who authorises it, how its use is recorded and that the password must be changed after use. When these accounts are used, an immediate (automatic) alert occurs and the *(Cyber) Security Officer* is informed. The *(Cyber) Security Officer* records the use of these accounts. | • | • | • | • |
| 4.3.21 | *Rights* of *Users* must be reviewed periodically, at least semi-annually. | • | | | |
| 4.3.22 | *Rights* of *Users* must be reviewed periodically, at least quarterly. | | • | • | |
| 4.3.23 | *Rights* of *Users* must be reviewed periodically, at least monthly. | | | | • |
| 4.3.24 | Accounts that have not been used for 40 days must be automatically blocked. | • | • | • | • |
| 4.3.25 | If a *User* enters an incorrect password five times, the *User Account* must be blocked. | • | | | |
| 4.3.26 | If a *User* enters an incorrect password three times, the *User Account* must be blocked. | | • | • | • |
| 4.3.27 | If an *Administrator* enters an incorrect password three times, the *Administrator Account* is blocked. The *Administrator Account* must only be released after approval by the *(Cyber) Security Officer*. | • | • | • | • |
| 4.3.28 | A blocked account must be unblocked according to a procedure approved by the *(Cyber) Security Officer*. | • | | | |
| 4.3.29 | A blocked account must only be unblocked after approval from the *(Cyber) Security Officer*. | | • | • | • |
| 4.3.30 | Passwords must meet the following characteristics as a minimum:<br>• passwords must consist of at least 15 characters;<br>• obvious patterns (such as '1234' and 'qaz') are not permitted;<br>• passwords must contain at least three of the following categories: uppercase, lowercase, numbers and punctuation. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.3.31 | Use of passwords is subject to the following requirements:<br>• a new password must be set at least once a year;<br>• initial passwords and passwords that have been reset have a maximum validity period of 24 hours and must be changed on first use;<br>• initial passwords and passwords that have been reset must be unique and must not be reused;<br>• initial passwords must comply with all regular password requirements;<br>• passwords must be issued in a secure manner, in which at least the *User's* identity and their right to use the authentication device must be verified;<br>• passwords must not be issued through the same channel as *User Accounts*. | ● | ● | ● | ● |
| 4.3.32 | The rules regarding use of an *Interest to be Protected* and *ICT Resources* (including the use of passwords), include at least the following requirements:<br>• passwords must not be written down;<br>• *Users* must never share their password with others;<br>• passwords must be changed immediately if there is a suspicion that they have become known to other persons;<br>• passwords must not be reused;<br>• passwords must not be used in automatic login procedures (such as stored under a function key or in a macro). | ● | ● | ● | ● |
| 4.3.33 | Personalised *Multi Factor Authentication* must be used to log in to a *User Account*, with SMS not counting as a factor. | ● | | | |
| 4.3.34 | To log in to a *User Account*, personalised *Multi Factor Authentication* must be used, of which one of the factors is a *Hardware Token*, with SMS not counting as a factor. | | ● | ● | ● |
| 4.3.35 | To log in to an *Administrator Account*, personalised *Multi Factor Authentication* is used, of which one of the factors is a *Hardware Token*, with SMS not counting as a factor. | ● | ● | ● | ● |
| 4.3.36 | When using *Biometrics* as an authentication factor for *Multi Factor Authentication*, PIN-based *Authentication* is excluded as an alternative option. | ● | ● | ● | ● |
| 4.3.37 | If *Hardware Tokens*, *Biometric* applications or *Multi Factor Authentication* are being used, they cannot be disabled by *Users*. The *(Cyber) Security Officer* must keep an up-to-date record of *Hardware Tokens* used. | ● | ● | ● | ● |
| 4.3.38 | Prior to using a *System*, a notification must be shown to the *User* that only authorised use is permitted for the purposes explicitly defined by the organisation. | ● | ● | ● | ● |
| 4.3.39 | A maximum of three active workplace (sessions) is permitted per account. | ● | | | |
| 4.3.40 | A maximum of one active workplace (session) is permitted per account. | | ● | ● | ● |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.3.41 | If there is an operational need for the use of a group account, this exception must be approved in advance by *NOIS*. The following conditions apply to the use of a group account:<br>• the *(Cyber) Security Officer* must authorise its use;<br>• the use of a group account must be traceable to an individual;<br>• it is not possible to use a group account via external access;<br>• it is not possible to access external *Systems* (such as the internet) using a group account;<br>• it is not possible to process personal or non-work-related information using a group account. | • | | | |
| 4.3.42 | The use of group accounts is not permitted. | | • | • | • |
| 4.3.43 | Passwords must not be displayed on screen during entry and information traceable to the *Authentication Data* must not be displayed. | • | • | • | • |
| 4.3.44 | *Users* can choose and change their own passwords. This is subject to the following minimum requirements:<br>• *Users* must be re-authenticated before they can change their passwords;<br>• a confirmation procedure must be applied to prevent typing errors in the newly chosen password. | • | • | • | • |
| 4.3.45 | Passwords must not be stored or transmitted in their original form (plain text), unless they are being used for the purpose of an 'envelope procedure'. | • | • | • | • |
| 4.3.46 | On successful login, the date and time of the previous login or login attempt must be displayed to the *User*. | | • | • | • |
| **4.4** | **Configuration management** | | | | |
| 4.4.1 | All hardware and software functionality (such as settings, network ports, USB ports, services, accounts, system tools) not required for the *Special Contract* must be disabled. | • | • | • | • |
| 4.4.2 | An exception can be made for activating hardware and software functionalities, such as *Data Carriers*, based on a *Risk Analysis* when this is strictly necessary for the execution of the *Special Contract*. This is subject to the approval of the *(Cyber) Security Officer*. The *(Cyber) Security Officer* must keep an up-to-date record of these exceptions. | • | • | • | • |
| 4.4.3 | For all equipment used as part of the *Special Contract* or located within the *Compartment*, all *Wireless Communication* components (such as Wi-Fi, Bluetooth, NFC and 5G) as well as all cameras and microphones must be removed or disabled in hardware settings. If specific functionality is required for the execution of a *Special Contract*, exceptions may be made. Exceptions must be approved in advance by *NOIS*. | | • | • | • |
| 4.4.4 | *Hardening* must be applied to hardware and software, including authentication protocols and mechanisms, in line with the manufacturer's stipulated and recommended security measures and supplemented based on recent industry standards. | • | • | • | • |
| 4.4.5 | Internal and external data traffic must be restricted to necessary protocols and sessions based on a *Risk Analysis*. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.4.6 | Software, servers, *User-*, *Network-* and storage devices must be provided with secure configurations through an established process. These configurations must be established, reviewed at least once a year, updated where necessary and shared with *NOIS* upon request. | ● | ● | ● | ● |
| 4.4.7 | A mechanism must be in place that checks the settings of information security functions (such as security software) on the *Interface* between different *Networks* for unauthorised changes. | ● | ● | ● | ● |
| 4.4.8 | The settings of logging mechanisms must be protected so that they cannot be modified or manipulated without being detected. Changes must be checked based on the four-eyes principle. | ● | ● | ● | ● |
| 4.4.9 | *System* clocks must use the same time synchronisation and must be protected against changes such that they cannot be modified or manipulated without being detected. | ● | ● | ● | ● |
| 4.4.10 | Only actively maintained hardware and software is to be used. | ● | ● | ● | ● |
| 4.4.11 | When *System Documentation* contains sensitive information about security measures of an *Interest to be Protected* located on the *System*, it must be protected at the same level as the *Interest to be Protected*. | ● | ● | ● | ● |
| 4.4.12 | For the purpose of performing management tasks, *System* configurations, including hardware, software, services, *Networks* and security, must be documented. | ● | ● | ● | ● |
| **4.5** | **Network security** | | | | |
| 4.5.1 | *Networks*, *Systems* and applications must be monitored and managed so that attacks, failures and/or errors can be detected and repaired and *Availability* does not fall below the agreed minimum level. This minimum must be included in the *Security Plan*. | ● | ● | ● | ● |
| 4.5.2 | Continuous real-time *Monitoring* and *Logging* of all incoming and outgoing *Network* traffic and *Network* links must be in place, paying attention to deviations from the normal pattern and intervening (automatically) where necessary. | ● | ● | ● | ● |
| 4.5.3 | All *Wireless Communication* must be treated as an *External (Network) Connection*. | ● | | | |
| 4.5.4 | The use of *Wireless Communication* is not permitted. | | ● | ● | ● |
| 4.5.5 | A *DMZ* must be applied in case of an *External (Network) Connection*. | ● | | | |
| 4.5.6 | For inbound and outbound data traffic to and from an untrusted environment, both internal and external, security measures such as a *DMZ*, *Proxy server* and/or sandbox must be in place. | ● | | | |
| 4.5.7 | All security mechanisms must use up-to-date indicators, such as virus definitions and *Signatures*. | ● | ● | ● | ● |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.5.8 | Security mechanisms for the purpose of the *Special Contract* must not originate from a country that has an *Offensive Cyber Programme* against Dutch interests. | ● | ● | ● | ● |
| 4.5.9 | At least once a year, the implemented security measures on an *Interface* must be tested to verify their operational effectiveness. Findings must be addressed and documented. | ● | ● | ● | ● |
| 4.5.10 | At the very least every six months, the implemented security mechanisms of *Networks*, *Systems* and applications must be tested to verify their operational effectiveness. Findings must be addressed and documented. | | ● | ● | ● |
| 4.5.11 | *Remote Access* to an *Interest to be Protected* (via a remote login facility) must only take place through *Approved Means* and procedures approved by *NOIS*. The equipment used must meet the relevant security requirements for the relevant *Classification Level*. | ● | | | |
| 4.5.12 | In *Interfaces* with external or untrusted *Networks*, measures must be in place to identify and respond to possible attacks that adversely affect the *Confidentiality*, *Integrity* and *Availability* of information provision (such as *DoS* and *DDoS attacks*). | ● | ● | ● | ● |
| 4.5.13 | *Systems* that use a connection to an external service for their functionality (such as licence servers and Device Management solutions) must be pre-approved by *NOIS*. To do so, mechanisms must be implemented to:<br>• limit data exchange to what is strictly necessary;<br>• prevent (information traceable to) *Special Information*, *Positions of Confidentiality* and unique characteristics of the *Technical Infrastructure* from leaving the *Trusted Network*;<br>• monitor, log and frequently review all interactions with an external service to detect suspicious activity early. | ● | | | |
| 4.5.14 | *Networks* must feature routing management measures based on mechanisms to verify source and destination addresses. | ● | ● | ● | ● |
| 4.5.15 | Technical measures must be taken to prevent internal network addresses from routing outwards, such as applying Outbound Traffic Filtering. | ● | ● | ● | ● |
| 4.5.16 | *Special Information* is only permitted to be sent over an untrusted connection if the *Special Information* is encrypted using *Approved Means*. | ● | ● | | |
| 4.5.17 | Technical and procedural measures must be in place to ensure that only identified and authenticated equipment can connect to the *Network*. When unknown equipment is connected, alerting takes place. | ● | ● | ● | ● |
| 4.5.18 | TOR (The Onion Router)/Darknet traffic must be blocked. | ● | ● | ● | ● |
| 4.5.19 | At the request of *NOIS*, the *Contractor* must cooperate in:<br>• installing a detection device;<br>• monitoring network traffic and hosts by using a detection mechanism;<br>• performing and delivering specific *Logging* requests for the local and *Cloud* environments (including telemetry);<br>• installing host-based detection;<br>• using a *DNS* service provided by the *Central Government*. | ● | ● | ● | ● |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.5.20 | The encryption protocols used must be the most recent protocols according to national and international security standards. Newly published standards must be implemented within the minimum feasible deadline. The connection conditions of the *Contracting Authority* must prevail and deviations must be reported to *NOIS*. | • | • | • | • |
| 4.5.21 | *Networks* for different *Classification Domains* must be separated and access must be secured using *Approved Means*. | • | | | |
| 4.5.22 | *Networks* for different *Classification Domains* must be physically separated and access must be secured using *Approved Means*. | | • | • | • |
| 4.5.23 | *International Network Connections* must use products and procedures approved by *NOIS*. | • | • | • | • |
| 4.5.24 | *Networks* of the same legal entity on which an *Interest to be Protected* is stored must be connected only through *Approved Means* and procedures approved by *NOIS*. | • | • | • | • |
| 4.5.25 | *Networks* of different legal entities on which an *Interest to be Protected* is stored must be connected only with the approval of the *Contracting Authority*. All entities must have the required *ABRO Declaration*, the connection must take place using *Approved Means* and based on procedures approved by *NOIS*, and the connection requirements of the relevant *Networks* must be met. | • | • | • | • |
| 4.5.26 | Information exchange for *Interfaces* between *Networks* of different *Classification Levels* must take place only from a *Network* with a lower *Classification Level* to a *Network* with a higher *Classification Level*. The interface must use *Approved Means*. Information exchanged must be handled according to the *Classification Level* of the *Segment* on which the information resides. | • | • | • | • |
| 4.5.27 | For *Interfaces* between *Networks* of different *Classification Levels*, information exchange from a *Network* with a higher *Classification Level* to a *Network* with a lower *Classification Level* is not possible. | | • | • | • |
| 4.5.28 | Unlocking an *Interest to be Protected* on a *Network* between different sites of the *Contractor (WAN)* is not permitted. | | | | • |
| 4.5.29 | The *Technical Infrastructure* is divided into *Segments*. The *Contractor* must ensure that *Special Information* of the same *Classification Domain* and *Classification Level* is processed within one *Segment* only. The *Contractor* must evaluate this at least once a year and revise *Segments* if necessary. | • | • | • | • |
| 4.5.30 | Each *Segment* must have a defined *Classification Domain* and *Classification Level*. *Interfaces* between *Segments* must be subject to controls on protocol, content and direction of communication. | • | • | • | • |
| 4.5.31 | *Segments* must be equipped exclusively with features strictly necessary for the required functionality. Management and auditing of *Segments* must take place from a logically separated *Segment*. | • | | | |
| 4.5.32 | *Segments* must be equipped exclusively with features strictly necessary for functionality. Management and auditing of *Segments* must take place from within a *Segment*. | | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.5.33 | Segmentation must be applied to separate groups of *Systems*, services and *Users* in the *Network*. For example, through a firewall or *DMZ*. | ● | ● | ● | ● |
| 4.5.34 | When applying *Virtualisation* within the framework of the *Special Contract*, a *Risk Analysis* must be carried out by the *(Cyber) Security Officer* and an *Administrator*. The following minimum conditions apply:<br>• security functionalities must run on physically separate virtualisation platforms;<br>• only system components with the same *Classification Domain* and *Classification Level* can be combined;<br>• *NOIS* must pre-approve the design and implementation;<br>• the management interface must be accessible only from the management segment;<br>• the *Virtualisation* platform must be hardened in accordance with the *Supplier's* instructions. | ● | ● | ● | ● |
| 4.5.35 | The deployment of VLANs is only permitted in *Networks* with the same *Classification Domain* and *Classification Level*. *NOIS* must pre-approve the design and implementation. The following minimum conditions apply:<br>• a firewall must be used to filter unwanted traffic;<br>• industry standards for the configuration of VLANs must be followed;<br>• network ports must be assigned to a VLAN either statically or based on a certificate. | ● | ● | ● | ● |
| **4.6** | **Endpoint security** | | | | |
| 4.6.1 | Facilities for *Remote Access* must be designed in such a way that no information from a *Trusted Network* is stored on the workstation or *Mobile Device (Zero Footprint)*. The workstation or *Mobile Device* must be encrypted with a hard disk encryption module available within the *System*, using Firmware TPM, Secure boot and Pre-boot authentication. | ● | | | |
| 4.6.2 | Provisions for *Remote Access* must be designed in such a way that possible *Malware* from the workstation or *Mobile device* cannot enter the part where *Special Information* is stored. | ● | | | |
| 4.6.3 | It is not possible to install or run unauthorised software or scripts on a workstation or *Mobile Device*. This must be technically enforced, with deviations being detected and addressed. Exceptions must be approved in writing and recorded by the *(Cyber) Security Officer*. | ● | ● | ● | ● |
| 4.6.4 | If a *User* is logged in to a workplace (session), the *Administrator* is only permitted to take over the workplace (session) with the *User's* permission. An option must be available to terminate takeover of the workplace (session) itself and a *Report* must appear that the workplace (session) has been terminated. The *User* must supervise that the *Administrator* does not gain knowledge of an *Interest to be Protected*. | ● | ● | ● | ● |
| 4.6.5 | Devices providing access to an *Interest to be Protected* must be checked automatically for compliance with a predefined security policy prior to providing access. | ● | ● | ● | ● |
| 4.6.6 | A workplace (session) must be automatically locked (*Clear Screen*) after 10 minutes of inactivity. | ● | ● | | |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.6.7 | A workplace (session) must be automatically locked (*Clear Screen*) after 5 minutes of inactivity. | | | • | • |
| 4.6.8 | When using a *Hardware Token*, the workplace (session) must be automatically locked when the *Hardware Token* is removed. | • | • | • | • |
| 4.6.9 | Disabling/deferring automatic locking at a particular workplace (session) is subject to the following conditions:<br>• automatic locking must only be turned off or postponed in the event of an operational need;<br>• the *(Cyber) Security Officer* must approve before automatic locking is turned off or postponed;<br>• the *(Cyber) Security Officer* must maintain an up-to-date record of the workplace (session) for which such permission was granted and why it was necessary to grant permission;<br>• each approval must be reviewed annually. | • | • | • | • |
| 4.6.10 | Anti-*Malware* software must periodically, at least daily, scan *Systems* and must perform direct scans on files, emails and other information when they are downloaded, opened, saved or executed. Any *Malware* identified must be quarantined. | • | | | |
| 4.6.11 | Anti-*Malware* software must periodically, at least daily, scan *Systems* and perform direct scans on files and other information when opened, saved or executed. Any *Malware* identified must be quarantined. | | • | • | • |
| 4.6.12 | Updating the detection definitions must take place at least daily. If online/*Cloud*-based anti-*Malware* services are used for this purpose, this must be submitted to *NOIS* in advance for approval and described in the *Security Plan*. | • | • | • | • |
| **4.7** | **Management of Mobile Equipment** | | | | |
| 4.7.1 | An *Interest to be Protected* may be stored or processed on *Mobile Devices* only to the extent strictly necessary for the *Special Contract*, subject to the following conditions:<br>• *Approved Means* must be used for encryption;<br>• only the strictly necessary amount of information must be stored;<br>• the relevant *Mobile Equipment* must be used only where and when cognisance by unauthorised persons is not possible;<br>• the relevant security requirements for the relevant *Classification Level* must be met. | • | • | • | • |
| 4.7.2 | *Mobile Equipment* outside the *Compartment* must not contain any features that are directly traceable to the *Contracting Authority* or the *Contractor* (whether physically on the *Mobile Equipment* or displayed on the screen of the *Mobile Equipment*). | • | • | • | • |
| 4.7.3 | *Mobile devices* on which an *Interest to be Protected* is generated, stored or processed may only use an *External Connection* when approved by *NOIS*. | • | | | |
| 4.7.4 | With *Remote Access*, all traffic to and from the equipment must be routed over an encrypted connection using *Approved Means*. Based on a *Risk Analysis*, exceptions can be made with prior approval from *NOIS*, such as for the purpose of Mobile Device Management, updates or data deletion. | • | | | |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.7.5 | Operating instructions must be drawn up for the use of *Mobile Devices* and *Remote Access*. | • | | | |
| 4.7.6 | After loss or theft of *Mobile devices*, the communication capability with the central applications must be closed, the *Authentication* mechanism must be reset and associated *Certificates* must be revoked immediately. Data must be wiped remotely as soon as possible. | • | | | |
| 4.7.7 | *Mobile Equipment* that is located outside the *Compartment* must be locked within 2 minutes if it is not used. | • | | | |
| 4.7.8 | Measures to restrict visibility (such as screen filters) must be applied for *Mobile Equipment* located outside the *Compartment*. | • | | | |
| 4.7.9 | Measures to restrict visibility (such as screen filters) must be applied to all equipment. | | • | • | • |
| **4.8** | **Cryptography** | | | | |
| 4.8.1 | *Cryptographic Security Solutions* must be deployed and managed in accordance with the documentation obtained through *NOIS*. In addition, the following advice and conditions must be complied with and documented in the *Security Plan*:<br>• the *Contracting Authority*'s connection conditions;<br>• the deployment advice, as obtained through *NOIS*;<br>• the manufacturer's advice.<br><br>Insofar as the advice and conditions conflict, the connection conditions prevail over the deployment advice, which prevail over the manufacturer's advice. | • | • | • | • |
| 4.8.2 | The process, roles, officers and their responsibilities regarding the management of *Cryptographic Security Solutions* must be set out in the cryptography policy (*RASCI*), as part of the *Security Plan*. | • | • | • | • |
| 4.8.3 | If the *Contractor* is provided with cryptographic keys through the National Distribution Authority or the *Contracting Authority*, at least two *Crypto Custodians* must be appointed, unless otherwise agreed with *NOIS*. The *Crypto Custodian* must further perform the duties as described in appendix 3. | • | • | • | • |
| 4.8.4 | The validity period of cryptographic keys is determined by the supplier or in the deployment advice and must be set out in the cryptography policy, as part of the *Security Plan*. | • | • | • | • |
| 4.8.5 | The administration of *Cryptographic Security Solutions* must take place based on the four-eyes principle. | • | • | • | • |
| 4.8.6 | *Administrators* must be trained in the management of *Cryptographic Security Solutions*, and administrator instructions must be provided to *Administrators*. | • | • | • | • |
| 4.8.7 | Before using *Cryptographic Security Solutions*, *User* instructions must be provided to *Users*. | • | • | • | • |
| 4.8.8 | *Users* of *Cryptographic Security Solutions* must be trained for this purpose by the *Contractor*. | | • | • | • |
| 4.8.9 | *Cryptographic Security Solutions* must be applied only if *Approved Means* are used. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.8.10 | The agreements, laws and regulations (such as export restrictions) with which *Cryptographic Security Solutions* must comply must be established. This must be set out in the *Security Plan*. The *Security Officer* monitors this. | • | • | • | • |
| 4.8.11 | Cryptographic keys, equipment and documentation must be secured throughout their lifecycle at least at the same level as the *Interests to be Protected* encrypted with the related key, unless deployment advice dictates otherwise. | • | • | • | • |
| 4.8.12 | Cryptographic keys that have expired must not be used and must be destroyed or dealt with in accordance with the deployment advice. Expired keys for which deployment advice is not available must be destroyed or dealt with in coordination with *NOIS*. | • | • | • | • |
| 4.8.13 | The *Crypto Custodian* must keep an up-to-date record of all cryptographic keys that have been or will be used. This record must include the recipient, site, use and destruction of the keys, in accordance with the terms and conditions of the key owner. | • | • | • | • |
| 4.8.14 | Prior to loading a new cryptographic key, *Cryptographic Security Solutions* must be checked for *Compromise*, as described in the administrator instructions. This includes checking physical seals, *Logging* and software validation. Records must be kept by the *Crypto Custodian* or, if not appointed, by the *(Cyber) Security Officer*. | • | • | • | • |
| 4.8.15 | A procedure has been established for dealing with compromised or potentially compromised *Cryptographic Security Solutions*. In the event of a *Compromise*, this must immediately be reported to the owner of the key and *NOIS*. | • | • | • | • |
| 4.8.16 | Management of *Cryptographic Security Solutions* must take place from a management segment without access to external or untrusted *Networks*, with the exception of file encryption using *Approved Means*. | • | | | |
| 4.8.17 | Management of *Cryptographic Security Solutions* must take place from a management segment specifically set up for this purpose, in accordance with the *Classification Level*. | | • | • | • |
| 4.8.18 | A procedure must be established for the entire life cycle of digital *Certificates* used within the organisation relating to IT facilities to be used for a *Special Contract*. | • | • | • | • |
| 4.8.19 | An externally verifiable *Certificate* must be provided by a *Supplier* certified to do so (such as WebTrust or ETSI). | • | | | |
| 4.8.20 | A Root Certificate Authority key must be stored in a FIPS 140-3 compliant standalone *Hardware Security Module (HSM)*. | • | • | • | • |
| 4.8.21 | An *HSM* on which a Root Certificate Authority key is stored must be physically secured at least at the security level applicable to ITBP 3, strictly applying the principles of *Need-to-Know* and *Need-to-Be*. | • | | | |
| 4.8.22 | An *HSM* on which a Root Certificate Authority key is stored must be physically secured at least at the *Special Contract* security level, strictly applying the principles of *Need-to-Know* and *Need-to-Be*. | | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **4.9** | **Physical and environmental security** | | | | |
| 4.9.1 | Equipment and cabling must be positioned and protected in such a way that risks of external damage and interference are reduced to an acceptable level, based on a *Risk Analysis*. | • | • | • | • |
| 4.9.2 | To prevent conduction and emission, unused voltage,data cables or loose metal conductors must be removed. | | • | • | • |
| 4.9.3 | Printers must use a 'secure printing' function by default (such as through PIN code authentication). | • | • | • | • |
| 4.9.4 | All *Special Information* located outside the designated physical *Compartment* must be encrypted using *Approved Means*. | • | • | • | • |
| **4.10** | **Vulnerability and patch management** | | | | |
| 4.10.1 | A process must be in place to identify and *Mitigate* technical vulnerabilities. This includes detection of technical vulnerabilities (at least quarterly) and periodic *Penetration Tests* (at least once a year). The results of these procedures must be shared with *NOIS* upon request. *Penetration Tests* must be performed only on *Networks* with a connection to another (external) *Network*. | • | • | • | • |
| 4.10.2 | A process must be in place to identify and implement new updates and *Patches* in a timely manner. Before an update or *Patch* can be implemented, it must first be verified. | • | • | • | • |
| 4.10.3 | Critical updates and *Patches* must be implemented as soon as possible. | • | • | • | • |
| 4.10.4 | In the event of a known vulnerability with a *CVSS* score of 4.0 or higher for a *System* with an *External Connection*, the *External Connection* to the *System* must be severed in coordination with the *Contracting Authority* and the *System* must be taken out of service until the vulnerability is patched or demonstrably mitigated. The *Contractor* must inform *NOIS* during this process. | • | • | • | • |
| **4.11** | **Change management** | | | | |
| 4.11.1 | Changes to an *Interest to be Protected* must be made through an established change management process that allows changes to be traceable and provides insight into possible negative effects. Changes must only be implemented with the prior approval of the *(Cyber) Security Officer*. | • | • | • | • |
| 4.11.2 | Changes to the configuration of *Systems* must be made only after demonstrable verification and acceptance by another designated *Authorised Employee*. A log must be kept of the acceptance. | • | • | • | • |
| **4.12** | **Maintenance** | | | | |
| 4.12.1 | Equipment, software and *Data Carriers* must be installed, used and maintained in accordance with the manufacturer's instructions, insofar as this does not conflict but aligns with the *Contractor*'s use and maintenance plan. Any deviations must be reported to *NOIS*. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.12.2 | Procedures (including roles and responsibilities) for the management of the IT facilities used to process *Special Information* (such as relating to backup and recovery, error handling and emergency procedures) must be established and made available to *Administrators*. Procedures must be evaluated at least once a year and updated where necessary. | • | • | • | • |
| 4.12.3 | *Remote Administration* of *Systems* must be limited to situations where it is strictly necessary and must be done using an established procedure and through a connection that can only be activated by an *Authorised Employee*. | • | | | |
| 4.12.4 | Only *Approved Means* must be used for *Maintenance* and *Remote Administration*. | • | | | |
| 4.12.5 | *Suppliers* must only be granted access for *Remote Maintenance* on the basis of a change request or fault report with prior approval of the *(Cyber) Security Officer*. An up-to-date record must be kept of this. | • | | | |
| 4.12.6 | *Remote Maintenance* and *Administration* of *Systems* is not permitted. | | • | • | • |
| 4.12.7 | Maintenance of *Network Devices* or equipment from which the *Data Carrier* is not removable must only take place on the *Contractor's* site using procedures approved by *NOIS*. The procedures regarding maintenance must be included as an appendix in the *Security Plan*. | • | | | |
| 4.12.8 | Maintenance of equipment must exclusively take place on the *Contractor's* site, using procedures approved by *NOIS*. The procedures regarding maintenance must be set out in an appendix to the *Security Plan*. | | • | • | • |
| **4.13** | **Monitoring and logging** | | | | |
| 4.13.1 | *System* and *User* activities must at least be logged in accordance with the *JSCU Logging Essentials* guidelines. Any additional *Logging* required must be determined on the basis of a *Risk Analysis*. These log files must be available for a minimum of six months. | • | | | |
| 4.13.2 | *System* and *User* activities must at least be logged in accordance with the *JSCU Logging Essentials* guidelines. Any additional *Logging* required must be determined on the basis of a *Risk Analysis*. These log files must be available for a minimum of 12 months. | | • | • | • |
| 4.13.3 | Activities of *Users* within *Systems* must be traceable to individuals. | • | • | • | • |
| 4.13.4 | Measures must be in place (such as *IDS*, Intrusion Prevention *System* (*IPS*) and Security Information & Event Management (SIEM)) to detect and investigate deviations from the baseline (anomalies) and unusual creations, presence and/or termination of processes for threats. | • | • | • | • |
| 4.13.5 | Automatic alerts must be triggered on the basis of defined threshold values or use cases for logged system activities. | • | • | • | • |
| 4.13.6 | The capacity and availability of a log server must be monitored, including automatic alerting whenever a threshold value is exceeded. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.13.7 | Log files must only be accessed by *Authorised Users*. Access must be limited to read-only access. | • | • | • | • |
| 4.13.8 | *System* and *User* activities must at least be logged in accordance with the *JSCU Logging Essentials* guidelines. Any additional *Logging* required must be determined on the basis of a *Risk Analysis*. These log files must be available for a minimum of six months. | • | • | • | • |
| 4.13.9 | Log data about a suspected or actual *Security Incident* must be retained for as long as necessary for investigating and handling the *Security Incident* and must be provided to *NOIS* upon request. | • | • | • | • |
| 4.13.10 | Log data from which *Special Information* or information about the *Interest to be Protected* can be derived must be secured at the same security level as the *Interest to be Protected* to which they relate. | • | • | • | • |
| **4.14** | **Business continuity and recovery** | | | | |
| 4.14.1 | Technical and procedural measures must be in place and must be included in the *Security Plan* to ensure the contractually agreed level of *Availability* (*RTO* and *RPO*). | • | • | • | • |
| 4.14.2 | Provisions must be in place to continuously monitor the *Availability* of the components involved in processing and storing *Special Information*. Based on predictive analytics of usage, timely measures must be taken to expand capacity if required. | • | • | • | • |
| 4.14.3 | Restrictions must be imposed on *Users* and *Systems* regarding the use of common *Means*, so that a single *User* (or *System*) cannot compromise the *Availability* of *Systems* for other *Users* (or *Systems*). | • | • | • | • |
| 4.14.4 | Procedures for backup of *Special Information* and for recovery of processing must be documented and tested at least every 6 months. These procedures must be based on the type of data (files, databases, etc.), the maximum permissible period over which data may be lost (*RPO*) and the maximum permissible recovery time (*RTO*). | • | • | • | • |
| 4.14.5 | The *Security Plan* must include and describe backup activities and the site of the *Data Carriers* on which the backups are stored. | • | • | • | • |
| 4.14.6 | Backups must be kept in a site selected so as to prevent a *Security Incident* at the original site from causing damage to the backup. | • | • | • | • |
| 4.14.7 | Backups must be retained for a minimum of 1 year and a maximum equalling the term of the *Special Contract*. Upon termination of the *Special Contract*, they must be destroyed using a procedure approved by *NOIS*. A confirmation of destruction must be prepared, shared with *NOIS* and archived, in accordance with the 'Confirmation of Destruction' form. | • | • | • | • |
| 4.14.8 | Backups must be handled according to the same security level as the *System* on which the original data resides. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **4.15** | **Development and acquisition** | | | | |
| 4.15.1 | Software development (or commissioning) must be done through a documented Secure Software Development Life Cycle (SSDLC) methodology, in which:<br>• a standardised process (such as a code repository) must be used that is based on best practices;<br>• developers must be familiar with relevant secure coding practices;<br>• secure development must be an explicit part of all steps in the methodology;<br>• software must be used as much as possible to identify errors and vulnerabilities early. | • | • | • | • |
| 4.15.2 | Development-, Test-, Acceptance- and Production environments must be logically separated. *Systems* and applications in these environments must not affect *Systems* and applications in other environments. | • | | | |
| 4.15.3 | Development-, Test- and Acceptance environments must be physically separate from Production environments. *Systems* and applications in these environments must not affect *Systems* and applications in other environments. | | • | • | • |
| 4.15.4 | Development-, Test-, Acceptance- and Production environments must be secured at the same *Classification Level* as the *Special Information*. | • | • | • | • |
| 4.15.5 | *Users* must have separate *User Accounts* for Development-, Test-, Acceptance- and Production *Systems* to reduce the risk of errors. It must be clearly visible in which *System Users* are working. | • | • | • | • |
| 4.15.6 | Digital experimental or laboratory environments must be physically separated from other environments. | • | • | • | • |
| 4.15.7 | Transfers between Development-, Test-, Acceptance- and Production environments must be made in compliance with an established procedure. This procedure must be approved by *NOIS*. | • | • | • | • |
| 4.15.8 | Software must not be installed on a Production environment until a formal testing and acceptance procedure has been completed. | • | • | • | • |
| 4.15.9 | A log must be kept of acceptance tests. | • | • | • | • |
| 4.15.10 | Software must not be installed on a Production environment until a rollback strategy has been formulated and tested. | • | • | • | • |
| 4.15.11 | Incoming software (both on physical media and downloaded) must be checked for unauthorised changes (integrity check) using a checksum, *Certificate* or *Software Bill of Materials (SBOM)* provided by the *Supplier* through a separate channel. | • | • | • | • |
| 4.15.12 | In the design phase of projects as part of the *Special Contract*, *Risk Analyses* must be performed and measures must be defined. In the event of changes to the project design, security implications must also be taken into account and documented. Each year and whenever changes are made, it must be checked whether the security risks are still current and the measures up to date. | • | • | • | • |

## Chapter 4: Cyber

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| 4.15.13 | At the very least data entry must be checked for threshold values, invalid characters, incompleteness, format and inconsistency. | ● | ● | ● | ● |
| 4.15.14 | The *System* must include functions that can be used to determine whether data has been processed correctly (accurately and completely). | ● | | | |
| 4.15.15 | The *System* must include an automated transactional and processing error check that determines whether data have been processed correctly and completely. | | ● | ● | ● |
| 4.15.16 | The output functions of programmes must make it possible to determine the completeness and correctness of data. | ● | ● | ● | ● |
| 4.15.17 | *Systems* security must be tested against predetermined acceptance criteria. | ● | ● | ● | ● |
| 4.15.18 | Test data and test accounts must be deleted before *Systems* and/or components are put into production. | ● | ● | ● | ● |
| 4.15.19 | Acceptance of *Systems* or software must take place after implementation of the *ABRO 2026* requirements has been established. | ● | ● | ● | ● |
| 4.15.20 | When using *External Code Libraries* as part of the *Special Contract*, the *Contractor* must independently verify the quality and integrity and must share the related report with the *Contracting Authority*. A *SBOM* must be provided to *NOIS* upon request. | ● | ● | ● | ● |
| 4.15.21 | Measures must be taken to protect the *Source Code* developed or used as part of the *Special Contract* from unintended changes. | ● | ● | ● | ● |
| 4.15.22 | When *Source Code* is developed or used specifically as part of a *Special Contract*, only *Authorised Employees* must have access to it. | ● | ● | ● | ● |
| 4.15.23 | *Source Code* developed for the purpose of the *Special Contract* must never be stored through a *Cloud Solution*. | ● | ● | ● | ● |

# 5. CLOUD

## Introduction

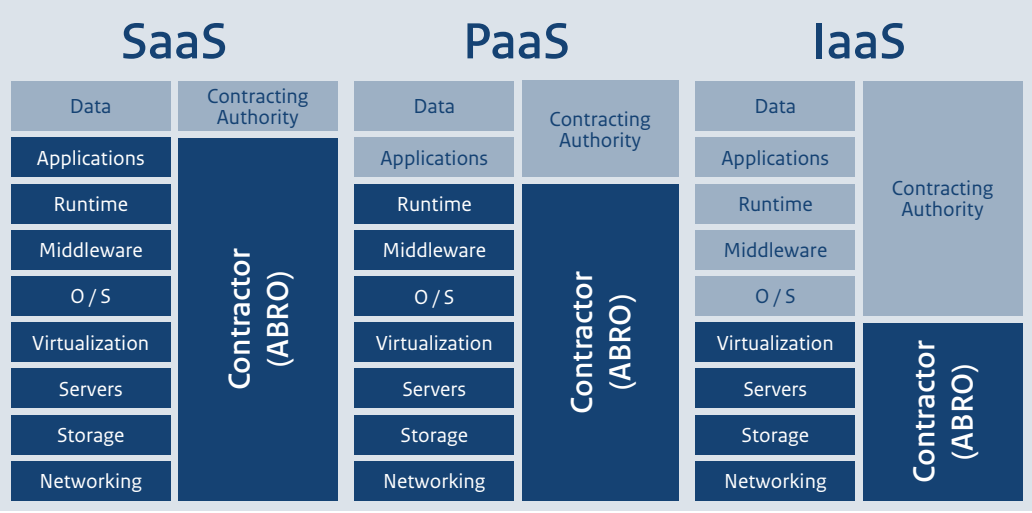
Specific security requirements have been set to facilitate the use of public *Cloud Solutions* as part of *Special Contracts*. *Cloud Solutions* must only be deployed for NLD RESTRICTED (ITBP 4). *Cloud Solutions* are not permitted to be used for information with a higher classification (NLD CONFIDENTIAL up to and including Stg. TOP SECRET).

*Private Cloud Solutions* do not fall within the scope of *Cloud Solutions* as referred to in this chapter. They are treated as regular IT solutions and thus assessed in accordance with Chapter 4, *Cyber*.

When *Cloud Solutions* are used, both the *Contracting Authority* and the *Cloud Service Provider (CSP)* must take security measures to adequately secure the *Special Information*.

## Type of Cloud Services and application of ABRO 2026

The specified requirements apply to both *SaaS*, *PaaS* and *IaaS* services. Depending on the type of services, *ABRO 2026* applies to different components of the *Cloud Solution*. When the *Contracting Authority* directly *Outsources* a service to a *CSP*, *ABRO 2026* applies to the components that fall under the responsibility of the *CSP*. For the components that fall under the responsibility of the *Contracting Authority*, the necessary measures must be implemented based on the prevailing policy. This situation is shown in the overview below. It requires clear responsibilities and close cooperation so that a comprehensive set of measures is created. When the *Contractor* uses a *CSP* for a *Special Contract*, *ABRO 2026* applies to both the *Contractor* and the *CSP*.



## Risk management

Prior to using a *Cloud Solution* as part of a *Special Contract*, the *Contracting Authority* must carry out a *Risk Analysis* to gain insight into the risks involved. Among other things, this *Risk Analysis* considers the *Confidentiality*, *Integrity* and *Availability* requirements, the assessed threats and the costs and benefits. The outcome of the *Risk Analysis* results in a contract-specific set of requirements based on *ABRO 2026*, which the *Contracting Authority* records in the agreement with the *Contractor*. In some cases this may result in an alternative interpretation of a security requirement than explicitly stipulated by *ABRO 2026*.

## Principles underlying the Cloud requirements

Essentially, industry standards and *Assurance Reports* are used to determine whether a *CSP* has implemented the appropriate internal controls and security measures. On top of this, additional requirements have been set to cover specific risks and enable the use of *Cloud Solutions* in the context of national security.

## Examples of application of ABRO 2026 to Cloud Solution

Several potential scenarios exist in which a *Cloud Solution*, and thus a *CSP*, plays a role in a *Special Contract*. A *CSP* can be the 'primary' *Contractor* and thus have a direct contractual relationship with the *Contracting Authority*. Another situation that occurs regularly is that of a *Contractor* providing a service that (partly) uses a *Cloud Solution* provided by the CSP in the capacity of *Subcontractor*. Each situation will need to be assessed to see which measures apply and where the responsibility for taking the measures lies. Two examples are explained below and summarised in Table 1.

## 1. The Contractor is a CSP

If the service provided by a *Contractor* is a *Cloud Solution* and the *Contractor* is thus considered a *CSP*, the *Cloud*-specific security requirements are leading, which means they largely replace the requirements set out in Chapters 3 and 4. In this situation, the *Contractor* must meet the requirements set out in Chapters 1, 2, and 5, as well as a limited number of requirements stipulated in Chapters 3 and 4. The requirements stipulated in Chapters 3 and 4 that also apply to *Cloud Solutions* are included in appendix 11.

## 2. The Subcontractor is a CSP

When a *Contractor* partly relies on a *Cloud Solution* for the provision of services and to this end uses a *CSP* in the capacity of *Subcontractor*, the *Cloud*-specific security requirements apply to that part of the service and the regular security requirements apply to the *Contractor*. In this situation, Chapters 1-4 apply to the *Contractor* and Chapters 1, 2, 5 and a limited number of requirements stipulated in Chapters 3 and 4 apply to the *CSP* in the capacity of *Subcontractor*. The requirements stipulated in Chapters 3 and 4 that also apply to *Cloud Solutions* are included in appendix 11.

Tabel 1 - Application of ABRO 2026 chapters relating to Cloud Solutions

| | **The Contractor is a CSP** and primarily provides a **Cloud Solution** | **The Contractor is not a CSP**, but uses a CSP in the capacity of Subcontractor | **The Subcontractor is a CSP**; the following chapters apply to the **Subcontractor** |
|---|---|---|---|
| CHPT1 - Management and Organisation | √ | √ | √ |
| CHPT2 - Personnel | √ | √ | √ |
| CHPT3 - Physical | * | √ | * |
| CHPT4 - Cyber (excluding Cloud) | * | √ | * |
| CHPT5 - Cloud | √ | - | √ |

* A limited number of requirements from Chapters 3 and 4 apply

If, either in the capacity of a *Contractor* or in the capacity of a *Subcontractor*, a *CSP* is unable to meet the *Cloud*-specific security requirements, then it must be determined in coordination with the *Contracting Authority* and *NOIS* how the required security level can be achieved, based on the requirements stipulated in Chapters 3 and 4.

# Chapter 5: Cloud

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **5.1** | **General** | | | | |
| 5.1.1 | The use of a *Public Cloud Service* (computing, storage, transport) is not permitted. | | • | • | • |
| 5.1.2 | The use of a *Public Cloud Service* (computing, storage, transport) for *Special Information* from *NATO*, *EU* or *ESA* is not permitted without prior approval from *NOIS*. | • | • | • | • |
| 5.1.3 | The *CSP* must neither be affiliated with, nor based in, nor carry out management activities in any country with an *Offensive Cyber Programme* against Dutch interests. | • | | | |
| 5.1.4 | The *Contracting Authority*'s data (including *Metadata* and telemetry) must remain at-rest, in-transit and in use within the Netherlands or, if approved by the *Contracting Authority*, the territory of the *European Economic Area (EEA)*. | • | | | |
| 5.1.5 | Management and maintenance of the *Cloud Service* and infrastructure as part of the *Special Contract* must take place within the territory of the *EEA*. | • | | | |
| 5.1.6 | The *Contractor* must meet the requirements relevant to *Cloud Services* as stipulated in *ABRO* 2026 Chapters 3 and 4, as referred to in appendix 11. | • | | | |
| **5.2** | **Governance** | | | | |
| 5.2.1 | The *Contractor* must carry out a *Risk Analysis* relating to the use of the *Cloud Service* based on the results of the *Risk Analysis* carried out by the *Contracting Authority* and based on relevant threats, including state actors. This *Risk Analysis* must be approved by the *Contracting Authority* in coordination with *NOIS* and included in the *Security Plan*. | • | | | |
| 5.2.2 | Throughout the contract period, the *CSP* must have a SOC2 type 2 report based on all trusted services criteria, or an *Assurance Report* that *NOIS* assesses to be equivalent, for the full scope of activities. This statement must be provided to *NOIS*. | • | | | |
| 5.2.3 | Based on the latest *CSA Cloud Control Matrix (CCM)*, the *CSP* must implement measures and must be able to demonstrate their design, existence and operational effectiveness, or must substantiate why one or more controls do not apply, based on a *Risk Analysis* approved by the *Contracting Authority*. This is included in the *Security Plan*. Any related changes must be reported to *NOIS* immediately. | • | | | |
| 5.2.4 | Prior to their implementation, changes to an *Assurance Report* relevant to the *Special Contract* or changes to measures affecting *CSA CCM* controls must be submitted to *NOIS* for approval. | • | | | |
| 5.2.5 | The *CSP* must include a *Contract*-specific *Cloud* security chapter in the *Security Plan*, which sets out::<br>• how the CSA *CCM* controls have been implemented and where they deviate from the controls;<br>• which additional measures apply based on the *Risk Analysis*.<br><br>Additional measures must be determined in coordination with *NOIS* and approved by the *Contracting Authority*. | • | | | |

## Chapter 5: Cloud

| ABRO req. no. | ABRO requirement | ITBP 4 / NLD RES | ITBP 3 / NLD C | ITBP 2 / NLD S | ITBP 1 / NLD TS |
|---|---|---|---|---|---|
| **5.3** | **Setting up security measures** | | | | |
| 5.3.1 | The *CSP* must provide *NOIS* with a *Contract*-specific architecture that specifies at least:<br>• which IT services, functionality and business processes apply;<br>• at which sites (support) operations, computing, storage and transport take place;<br>• which infrastructure, network and system components are used for the development and operation of the *Cloud Service(s)*;<br>• whether, and if so which, IT functions are assigned or outsourced to *Suppliers* by the *CSP*. | • | | | |
| 5.3.2 | The division of roles and responsibilities between the *CSP* and the *Contracting Authority* for the implementation and execution of the security measures applicable to the Cloud Service must be set out in an *SLA* and a *DAP*. A copy of each must be included in the *Security Plan*. | • | | | |
| 5.3.3 | Based on the *Risk Analysis*, the *CSP* must set up additional *Monitoring* and *Logging*, where applicable, in coordination with *NOIS*, aimed at detecting state actors. | • | | | |
| 5.3.4 | The *CSP* must set up the *Cloud Service* and infrastructure according to the *Secure by default* concept. | • | | | |
| **5.4** | **Cryptography and key management** | | | | |
| 5.4.1 | The *CSP* must support key management that is performed entirely by the *Contracting Authority*, or must support that the *Contracting Authority* may engage a third party with an *ABRO Declaration*, other than the *CSP*, based on a *Risk Analysis* coordinated with *NOIS*. | • | | | |
| 5.4.2 | The *Contracting Authority*'s data at-rest and in-transit must be encrypted in accordance with the latest industry standards. | • | | | |
| **5.5** | **Compliance** | | | | |
| 5.5.1 | The *CSP* must fully cooperate with compliance reviews and investigations by the *Contracting Authority* or *NOIS* related to the *Special Contract*, whether or not carried out by a certified third party. | • | | | |
| 5.5.2 | The CSP must have and provide procedures for handling questions from government agencies relating to investigations that require access to *Tenants* or the *Contracting Authority*'s data. At the very least the procedures must include:<br>• checking the legal basis for the questions relating to investigations;<br>• informing the *Contracting Authority* and *NOIS* to the best of their ability of the questions relating to investigations and involving them in handling these questions;<br>• possibilities for the *Contracting Authority* to appeal against the questions relating to investigations. | • | | | |
| 5.5.3 | The *CSP* must have measures in place and must set up processes to allow for execution of the *Contracting Authority*'s exit strategy and subsequent provisions, as included in the *Contract* with the *Contracting Authority*. | • | | | |

# 6. ABBREVIATIONS AND TERMS

| | |
|---|---|
| **ABDO** | General Security Requirements for Defence Contracts. Regulations for the adequate security of *Interests to be Protected* (including *Special Information*) that are or will be entrusted to a *Supplier* outside the Ministry of Defence. Within the framework of national security, *ABDO* sets requirements for the *Confidentiality, Integrity and Availability (CIA)* of *Contractors* in terms of people, processes, *Resources* and organisation to safeguard the *CIA* of *Interests to be Protected*. |
| **ABRO** | General Security Requirements for *Central Government* Contracts. Regulations for the adequate security of *Interests to be Protected* (including *Special Information*) that are or will be entrusted to a *Supplier* outside the *Central Government*. Within the framework of national security, *ABRO* 2026 sets requirements for the *Reliability* of *Contractors* in terms of people, processes, *Resources* and organisation to safeguard the *CIA* of *Interests to be Protected*. This is the product of continued development of the General Security Requirements for Defence Contracts *(ABDO)*. |
| **ABRO Declaration** | The formal statement that, based on the judgment of the *Netherlands Office for Industrial Security (NOIS)* (Nationaal Bureau Industrieveiligheid, NBIV), the *Contractor* meets the security requirements contained in *ABRO* 2026 for the *Special Contract* referred to. An *ABRO Declaration* only applies to the *Special Contract* for which it was issued. In the event that a request originates from a foreign *Contracting Authority* or is directed at a foreign *Contractor*, it is referred to as *Facility Security Clearance (FSC)* instead of an *ABRO Declaration*. |
| **Access-to-site** | A type of *ABRO Declaration* under which frequent access is to be granted to *Contractor's* employees to a site, *Compartment* or *System* of the *Contracting Authority*, where an *Interest to be Protected* may or may not be present. |
| **Administrator** | A *User* who is responsible for configuring, managing and maintaining *Systems*, applications or *Network* components. An *Administrator* typically has elevated *Rights* and privileges to modify settings, manage *User* and *System Accounts*, assign access *Rights* and implement security measures. |
| **Administrator Account** | A *User Account* with elevated or full access *Rights* to *Systems*, applications or *Networks*. This account is used by *Administrators* to perform management and configuration tasks, such as creating and deleting *User Accounts*, modifying *Rights*, and configuring security setting. |
| **AI Systems** | Artificial Intelligence *Systems*. *Systems* with the ability to achieve a complex goal through flexible adaptation to the environment. This includes Large Language Models and Machine Learning. Such a *System* is able to automatically learn and improve based on experience or data without being explicitly programmed to do so. |
| **Approved Means** | Software and hardware that has been found suitable for use for the intended functionality within the framework of a *Special Contract*. Approval is given by different authorities, depending on the intended use and the *Contracting Authority*. See also appendix 9. The application for and issuance of the approval is done through *NOIS*. |
| **Assurance Report(s)** | A formal statement issued by an independent auditor or accountant, which confirms that certain information is reliable. |
| **Authentication** | The process by which the identity of a *User*, *System* or entity is verified. |
| **Authentication Data** | Information used to *Authenticate* a *User*, *System* or entity and to grant access to secure *Systems* or data. |
| **Authorised Employee** | Employees of the *Contractor*, or hired externally by the *Contractor*, who have permission from the *Contractor* to take cognisance of or have access to an *Interest to be Protected*. |

| | |
|---|---|
| **Authorisation(s)** | The authority of a *User*, account, *System* or software process to access a digital or physical *Resource*, site, information, data or *System* and to perform specific actions. In the physical domain, this concerns a person's access to a *Compartment*. In the digital domain, this can involve *Authorisations* linked to an account for a natural person, but also, for example, a software process in which the *Authorisations* are linked to a *Service Account*. |
| **Availability** | The assurance that authorised *Users* or *Systems* have timely access to information and related *Company Resources* at the right times. |
| **Background Investigation (BI and BI+)** | An investigation by the police pursuant to Article 49q of the Netherlands Police Act and the Decree on screening of police officers and external law enforcement support in which the background, *Integrity* and suitability of current and future police officers are investigated to ensure that they meet the ethical and professional standards required for the performance of their duties. This investigation may consist of background checks, security checks and interviews, among other things. There are two types of investigation: the *Background Investigation* (BI) and the *Background and Environment Investigation* (BI+). |
| **Biometrics** | Method to *Authenticate* a *User* based on biological measurements or physical characteristics, such as a fingerprint or iris scan. |
| **BMS** | Building Management *System*. An integrated *System* that centralises and automates the management and control of technical installations and services in a building. |
| **CCM** | Cloud Control Matrix. A framework of security controls designed to ensure fundamental security principles in *Cloud Solutions*. |
| **Central Government** | The *Central Government* consists of all ministries, implementing organisations and inspectorates that fall under the responsibility of a minister and the High Councils of State. |
| **Certificate** | A statement issued by an independent body that a product, process or person complies with the requirements in the *Certificate*. In a digital context, it is a digital document that proves the identity of a *User*, *System* or entity. This can be used, for example, to establish a secure connection. The document is issued by a trusted third-party organisation (Certificate Authority). |
| **Certificate of Conduct** | A certificate from the Justis Department (Judicial agency for Testing, Integrity and Screening) of the Ministry of Justice and Security, showing a person's past behaviour does not constitute an objection to performing a specific task or position. This may also include an international equivalent, provided it is based on international agreements for the mutual recognition of such certificates. As a minimum, a *Certificate of Conduct* is required when an employee has access to and may have knowledge of a Level 4 *Interest to be Protected* or Departmental *Confidential Information*. |
| **Certificate of No Objection** | A statement that, from a national security perspective, there is no objection to a particular person fulfilling a particular . This may also include an international equivalent, provided it is based on international agreements for the mutual recognition of such decisions. |
| **Chemically Anchored** | A fixing technique in which chemical mortar is used to firmly anchor *Security Resources* in materials such as concrete or brickwork. |
| **Classification** | The *Classification Domain* and *Level* established for the relevant *Special Information* by the owner of the information, such as NLD RESTRICTED, NLD SECRET or *NATO* SECRET. |
| **Classification Level** | Indication of the expected adverse consequences for the interests of the State, its allies or one or more ministries if (part of) the information becomes known to unauthorised persons. Within a *Classification Level*, a distinction can be made between different *Markings*, which are treated as the respective *Classification Level*. |
| **Classification Domain** | Designation of a defined environment with an owner, such as *NATO*, NLD, UK, *EU or ESA*, for which the *Special Information* is intended. |

| | |
|---|---|
| **Clear Desk** | The principle that no sensitive information is left at a workplace. |
| **Clear Screen** | The principle that a *User* locks their workstation when leaving it. |
| **Cloud (Solution)** | A model for enabling on-demand *Network* access to a shared pool of configurable computer resources (e.g. *Networks*, servers, storage, applications and services) that can be rapidly provisioned and released. A distinction is made between *SaaS*, *PaaS* and *IaaS*. |
| **Compact Interest to be Protected** | *Interest to be Protected* that can reasonably be physically stored in a lockable *Storage Unit*, such as a laptop. |
| **Company Resource** | All *Resources* on which or through which company information can be stored and/or processed and with which access to buildings, work areas and ICT *Resources* can be gained: a device, an *ICT Resource* or a defined data set. |
| **Compartment** | A designated, secure, separate, lockable physical space where an *Interest to be Protected* is processed or stored. This can be a space of various dimensions, such as a room, floor, building, shipping container, factory hall or site. |
| **Compromise** | Cognisance of or access to an *Interest to be Protected* by unauthorised persons, or the loss of an *Interest to be Protected*, where it has been established or can reasonably be assumed that the *Confidentiality, Integrity or Availability* of an *Interest to be Protected* has been compromised. |
| **Confidentiality** | Ensuring that information can only be accessed by those authorised to do so. |
| **Contracting Authority** | The ministry, agency or police that hires the *Contractor* to carry out a *Special Contract*. This may also be a foreign government organisation or international organisation based on an international treaty. When applying *ABRO 2026* to a *Subcontractor* while the intended security objective of a requirement relates to the cooperation between the *Contractor* and that *Subcontractor* within the framework of the *Special Contract*, the term *Contractor* is assumed to refer to the *Contracting Authority*. |
| **Contractor** | The company or organisation selected as the *Supplier* to provide a requested service or goods within the framework of a *Special Contract*. When applying *ABRO 2026* to a *Subcontractor* while the intended security objective of a requirement relates to the cooperation between the *Contractor* and that *Subcontractor* within the framework of a *Special Contract*, the term *Subcontractor* is assumed to refer to the *Contractor*. |
| **Control** | The capacity to influence a company's policy based on factual or legal circumstances. Having relevant influence on the policy of a company can be the result of financial, organisational and formal links (appointment rights, voting rights on shares), direct or indirect links (subsidiaries and sister companies), collaboration in a group, or informal partnerships. |
| **Crypto Administrator** | A *Position of Confidentiality* in which the employee in question is responsible for processing, administering and managing *Cryptographic Security Solutions*. |
| **Cryptographic Security Solutions** | Hardware or software (including physical and digital keys) that uses encryption to guarantee the *Confidentiality* and *Integrity* of information, both in-rest and in-transit. |
| **CSA** | Cloud Security Alliance. An organisation that focuses on developing and promoting best practices for security in *Cloud* computing and providing educational resources for organisations. |
| **CSC** | Cloud Service Consumer. A customer or *User* of *Cloud* services provided by a *Cloud Service Provider*. |
| **CSP** | Cloud Service Provider. A company that provides *Cloud*-based platforms, infrastructure, applications or storage services to other organisations or individuals via a *Network* connection. |
| **CVSS** | Common Vulnerability Scoring System |

| | |
|---|---|
| **Cyber** | A prefix used to indicate matters relating to computers, *Networks* and the digital world (such as: cybercrime, cybersecurity, cyberthreat). |
| **Cyber Security Officer** | A specific *Security Officer* with responsibilities related to and expertise in the field of cybersecurity and information security, who can support a *Security Officer* with specific *Cyber*-related issues. |
| **DAP** | Document Agreements and Procedures. A type of agreement that establishes the mutually agreed cooperation between a customer and a supplier regarding a purchased service or product. A *DAP* can be an agreement between both internal (customer) and external (supplier) parties within an organisation. A *DAP* is hierarchically subordinate to a Service Level Agreement *(SLA)* and, in addition to other service documentation, is an appendix to the general main agreement. |
| **Data Carriers** | Physical *Resources*, such as hard drives, on which digital data can be stored. |
| **Delay Time** | The cumulative delaying effect of organisational, physical and/or electronic security measures on an intruder. For the purpose of determining the *Security Effectiveness*, this represents the time between the detection/verification of an intrusion and the *Compromise* of an ITBP. Measures that have a delaying effect on an intruder prior to detection/verification do not contribute to the *Security Effectiveness*. |
| **DISS** | Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). |
| **DMZ** | Demilitarised Zone. A physical or logical part of a *Network* that contains the services of an organisation that can be accessed externally (from another untrusted *Network* or the internet), so that internal services and workstations cannot be accessed directly (e.g. mail and web servers). |
| **DNS** | Domain Name System. A *System* that links internet domain names to *IP Addresses* and vice versa. |
| **DoS/DDoS** | (Distributed) Denial of Service. Making a computer, computer *Network* or service unusable by overloading the bandwidth, memory or processing capacity. In a *DDoS attack*, the attack is carried out by a collection of computers or other devices that simultaneously try to disable a computer (*Network*) or service, with this attack being coordinated centrally, often via a botnet. |
| **DSA** | Designated Security Authority |
| **EAMS** | Electronic Access Management System |
| **EEA** | European Economic Area. The territory consisting of the *EU* Member States and Norway, Liechtenstein and Iceland - or the territory of the United Kingdom or Switzerland. |
| **Electronic Security Screening** | Investigation into the potential presence of undesirable equipment in a *Compartment*. |
| **Emergency Destruction Plan** | Part of the *Security Plan* that describes clear procedures and instructions for the emergency destruction of an *Interest to be Protected*. Emergency destruction only takes place in exceptional circumstances where national security is at risk. In such cases, the prescribed destruction procedures are deviated from. |
| **Employee holding a Position of Confidentiality** | A person assigned to a *Position of Confidentiality*. |
| **Employee(s) Involved** | Employees of the *Contractor* or hired externally by the *Contractor* who perform work under a *Special Contract*. |
| **ESA** | European Space Agency |

| | |
|---|---|
| **Escrow Agent** | A third party where digital keys are or *Source Code* is stored. |
| **EU** | European Union |
| **External ARC** | External Alarm Receiving Centre. An alarm receiving centre operated by a third party where signals are received from the *IDAS* and other detection systems when an alarm is triggered, and from which alarm response is organised and coordinated. |
| **External (Network) Connection** | An *External Connection* is a connection or interface between a *Trusted System* or *Network* and an untrusted *System* or *Network*. |
| **External Code Libraries** | Collections of reusable code, developed by third parties outside of in-house development teams, that can be imported and used within a software project to implement certain functions and capabilities. |
| **Elevated Privileges or access Rights** | Special *Rights* or privileges (both physical and logical) that are granted to certain employees or *Systems*, allowing them to perform actions that are outside the normal authorisation limits. These authorisations are often necessary for *System* management, maintenance or for specific roles within an organisation. Abuse of *Elevated Privileges* or access *Rights* often increases the risk of a *Compromise* and therefore requires additional or specific measures. |
| **Foreign Partner** | A foreign equivalent of *NOIS* that supervises industrial security in the country in question on behalf of that country. |
| **FSC** | Facility Security Clearance. The statement from *NOIS* to an applicant (usually a foreign applicant) that a company is capable of carrying out a *Special Contract* from a security perspective. |
| **GISS** | General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) |
| **Hardening** | The process of disabling or removing unused functions in hardware and software and limiting the *Rights* of other functions, where possible with the aim of reducing the attack surface and therefore the risk of attacks. |
| **Hardware Token** | A physical *Resource* that often has a cryptographic module to establish the authenticity of a *User*. For example, for *Multi Factor Authentication*. |
| **Highest Executive Authority** | The highest body within an organisation, institution or government entity that is responsible for making strategic decisions and setting general policy. This body has the ultimate say in the direction and management of the organisation and is often charged with supervision, approval of budgets, compliance with legal requirements, and safeguarding the interests of stakeholders. |
| **High-Risk Country** | A country that, through its intentions, policies or actions, poses a (potential) threat to the interests of the State, its allies or one or more ministries. For guidance, one can also look at the countries named in the Staatscourant and in the recent annual reports of *GISS* and *DISS*. |
| **HSM** | Hardware Security Module. A physical device for managing and generating digital keys and performing cryptographic processing with measures to prevent (undetected) physical and non-physical manipulation. |
| **IaaS** | Infrastructure as a Service. The capability provided to the consumer is to provision processing, storage, *Networks*, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). |

| | |
|---|---|
| **ICT Resource(s)** | A (physical or logical) technical *Resource* (such as hardware, software, application or facility) with which an IT service is realised or used, in whole or in part and directly or indirectly. |
| **IDAS** | Intrusion Detection and Alerting System. A *System* that is used to signal and alert unauthorised physical access to a room. |
| **IDS** | Intrusion Detection System. A *System* that analyses *Network* and system activities with the aim of detecting any attempts to gain unauthorised access to digital *Systems* or information and sending out subsequent alerts. |
| **Incident Response Procedure** | A procedure that includes the steps that must be taken in the investigation and handling of a detected *Security Incident*. |
| **Integrity** | Ensuring the accuracy, completeness and timeliness of information and its processing. |
| **Interest to be Protected** | Persons, information, *Systems*, materiel, goods, images and objects, which in the event of *Compromise*, or the possibility of *Compromise*, may trigger adverse consequences, or a risk thereof, for the *Confidentiality*, *Availability* and *Integrity* of the primary processes of the *Central Government*, parts of said processes or for other interests of the State, its allies or one or more ministries.<br><br>*Interests to be Protected* are divided into four categories (ITBP 1, ITBP 2, ITBP 3 and ITBP 4, with ITBP 1 requiring the strongest security level). |
| **Interface** | A connection between two or more *Networks* or *Systems* through which information, whether or not of a different *Classification Level*, can be exchanged. |
| **Internal ARC** | Internal Alarm Receiving Centre. An alarm receiving centre managed by the *Contractor* where signals are received from the *IDAS* and other detection systems when an alarm is triggered, and from which an alarm response is organised and coordinated. |
| **International Network Connection** | Links to *Networks* of, for example, foreign governments, *NATO*, *EU* or *ESA* that are set up to exchange international *Special Information*. |
| **Intervention** | The response to an alarm (suspected attempt to *Compromise* an *Interest to be Protected*) with the aim of verifying the alarm and, if necessary, stopping the *Compromise* of the *Interest to be Protected* or safeguarding it. It therefore concerns the entirety of measures and/or activities with the aim of preventing *Compromise* of an *Interest to be Protected* and restoring the security level. Intervention should take place by trained and *Authorised Persons*, maintaining the *Need-to-Know* and *Need-to-Be* principles. |
| **Intervention Time** | The time between detection/verification of an attempted *Compromise* and on-site intervention by employees, *Security Personnel* or the police. |
| **IP Address** | Internet Protocol Address. An *IP Address* is a unique identification number on a *Network* assigned to each device on that *Network* that uses the Internet Protocol to communicate. |
| **JSCU Logging Essentials** | Guidelines from the Joint Sigint Cyber Unit (JSCU) of *GISS* and *DISS* for setting up *Logging*, as published on the GitHub of the Joint Sigint Cyber Unit. |
| **KVM Switch** | A device that allows *Users* to manage and operate multiple *Systems* with a single keyboard, monitor and mouse. |
| **Logging** | The recording of data relating to (attempts at) access to or activities that affect an *Interest to be Protected*, both physically and digitally. |
| **Malware** | Software with unwanted/malicious functionality, such as viruses and trojans. |

| | |
|---|---|
| **Marking** | Designation on information that implies a certain method of handling and restriction of distribution. If determined by the *Contracting Authority*, a *Marking* is handled in accordance with the established ITBP category. |
| **Means of Transport** | Physical means used for moving (*Sending/Transporting*) an *Interest to be Protected*. The *Means of Transport* must comply with set security standards and protocols to ensure the *Confidentiality, Integrity and Availability (CIA)* of the *Interest to be Protected*. |
| **Metadata** | Data that describes the properties of other data. For example, who the data belongs to, who sent it, or when it was last modified. |
| **Mitigate** | Minimising the risk of a (digital) *Compromise* by means of security measures or minimising the effect of a (digital) *Compromise* by means of *Intervention(s)*. |
| **Mobile Equipment** | Portable electronic devices such as smartphones, tablets and laptops that provide access to *Special Information* or generate, process or store it. |
| **Monitoring** | The continuous monitoring of (physical) environments, *Networks* and *Systems* to detect anomalous activities and (potential) attempts to *Compromise*. |
| **MoU** | Memorandum of Understanding. A bilateral treaty in which security agreements are made. For example, about the mutual recognition of a *Certificate of No Objection* and the equivalent of the other country concerned. |
| **Multi Factor Authentication** | A security measure that requires multiple factors to establish a *User's* identity before access can be granted to a *System* or *Compartment*. |
| **NATO** | North Atlantic Treaty Organisation |
| **Need-to-Be** | The principle that a person only has physical or digital access to an environment when this is necessary for the performance of their work. |
| **Need-to-Know** | The principle that a person only has knowledge of or access to certain information when this is necessary for the performance of their work. |
| **Need-to-Use** | The principle that a person may only make physical or digital use of *Resources* or information when this is necessary for the performance of their work. |
| **Network** | A composition of interconnected *Systems*, devices, and other components that communicate and exchange data. |
| **Network Devices** | *Electronic Equipment* that establishes a *Network* using wired or wireless connections, such as a switch or a firewall. |
| **NOIS** | National Industrial Security Office (Nationaal Bureau Industrieveiligheid, NBIV). The organisation charged with promoting measures regarding the security of data and material affecting national security. In this context, *NOIS* offers support to the *Contracting Authority* in monitoring compliance with *ABRO 2026* regarding *Special Contracts* initiated by the *Contracting Authority* or *Contracting Authorities*. |
| **Non-Disclosure Agreement** | A legally binding statement that certain information will not be disclosed to unauthorised persons. |
| **Offensive Cyber Programme** | The use of cyber-attacks, organised or encouraged by a government, to serve its own interests. This concerns, among others, countries that have been named as such in the most recent annual reports of *DISS* and *GISS*. |

| | |
|---|---|
| **OSI Model Layers** | The OSI model (Open Systems Interconnection) is an ISO standardised reference model for categorising communication between *Systems*. Layers 2, 3 and 4 refer to the *Data Link*, *Network* and *Transport* layers respectively. |
| **Outsourcing** | All forms of business activities that contribute directly to the service to be provided, for which third-party services are used in full or in part. This includes the provision of components when *Compromise* of components poses a security risk to the *Interest to be Protected*. |
| **PaaS** | Platform as a Service. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including *Network*, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |
| **PAM** | Privileged Access Management. A security method and technology aimed at managing and controlling access to *Systems* and to sensitive information by *Users* with privileged (elevated) *Rights* within an organisation. |
| **Patch(ing)** | The process of applying a specific update to software or *Systems* in which new or modified software code (a patch) is added to resolve security issues, fix bugs or improve functionality. |
| **Penetration Test(s)** | A test for physical and digital vulnerabilities of a *System* or application with the aim of resolving or mitigating the vulnerabilities found. |
| **Physical Access Authentication Resources** | All forms of (spare) keys, passes, electronic keys or other physical objects that can be used to gain access to a *Compartment* or *Storage Unit*. |
| **Position of Confidentiality** | A position in which national security could be harmed. |
| **Private Cloud** | A *Cloud* infrastructure that is made available for the exclusive use of a single organisation with multiple *Users* (e.g. departments). It can be owned, managed or operated by that same organisation, a third party or a combination of both. |
| **Prohibited Area** | Large concentrations of *State Secrets* at a single site may be grounds for that site to be designated a *Prohibited Area* by Royal Decree. A *Prohibited Area* is secured in accordance with ITBP category 1. Personnel requiring access ('*Need-to-Be*') must have a security clearance level corresponding to the highest available *Classification*. |
| **Proxy** | A computer system or application that functions as an intermediary between requests from workstations and resources from servers. |
| **PSC(C)** | Personnel Security Clearance (Certificate). The certificate declaring that a person is authorised to access or take cognisance of an *Interest to be Protected* (including *Special Information*) in an international context. |
| **PSI** | Project Security Instruction. A document in which further security requirements are recorded, usually in the context of a foreign contract. |
| **Public Cloud** | A *Cloud* infrastructure that is made available to a large audience or multiple organisations. All related hardware, software and supporting infrastructure are the property of the *Supplier*. |
| **RASCI** | Responsible, Accountable, Support, Consulted and Informed. This is a table that records which functions fulfil which role for each activity within a process. |
| **Recordings** | A representation of a situation or object recorded on a medium based on acoustic, visual or other types of signals. |

| | |
|---|---|
| **Remote Access** | The access to *Systems*, *Networks* and data from a workstation or *Mobile Device* that makes a connection to the local IT infrastructure through an external *Network*. |
| **Remote Administration** | Performing administration activities from a workstation or *Mobile Device* that uses an external *Network* to connect to the local IT infrastructure set up for the purpose of a *Special Contract*. |
| **Remote Maintenance** | Carrying out maintenance work from a workstation or *Mobile Device* that connects to the local IT infrastructure set up for a *Special Contract* through an external *Network* connection. |
| **Removable Data Carrier** | Storage devices that can be removed and taken along. Such as CDROMs, USB sticks, removable disks or tapes. |
| **Report** | The official reporting or notification of an event, situation or finding to an authorised person or body. This can relate to a variety of matters such as *Security Incidents*, complaints, problems or other relevant information that requires action or attention. The purpose of a *Report* is to inform the responsible party so that they can take appropriate measures. |
| **Resource(s)** | Equipment, software, hardware, *Network* cabling and other technology that processes or communicates information. |
| **RfV** | Request for Visit. The request to the relevant security authorities for permission to visit a government organisation or a company abroad. |
| **Rights** | (Access) *Rights* and permissions assigned to a *User* or *Administrator Account* to enable specific capabilities within a *System* or access to information, such as managing *User* or *System* configurations or modifying information elements. |
| **Risk Analysis** | The process of systematically determining the likelihood and consequences of events affecting the interests of an organisation. This process consists of at least identifying (what can happen), assessing (how likely it is and what the consequences are) and evaluating risks. |
| **RPO** | Recovery Point Objective. The maximum acceptable amount of data loss that an organisation can tolerate after an outage, breach or disruptive event. |
| **RTO** | Recovery Time Objective. The maximum duration of outage of a *System* or *Network* that an organisation can tolerate. |
| **SaaS** | Software as a Service. The capability provided to the consumer is to use the provider's applications running on a *Cloud* infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying *Cloud* infrastructure including *Network*, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited *User*-specific application configuration settings. |
| **SAL** | Security Aspect Letter. A document setting out more detailed security requirements, usually as part of smaller projects abroad. |
| **SBOM** | Software Bill of Materials. An inventory of all software components, libraries and modules used in the development of a software application. It provides an overview of the origin, versions and licensing information of these components, as well as their interdependencies. |
| **Scrubber** | A standalone *System* that checks *Removable Data Carriers* for the presence of *Malware* and quarantines them if necessary. |
| **Secure by default** | A security principle in which a *System*, product, or service is designed and configured to provide the best possible security by default, without requiring *Users* to make additional adjustments. Hence, all security settings and measures are activated by default, minimising the risk of security breaches due to unnoticed or unconfigured settings. |

| | |
|---|---|
| **Security Agreement** | A multi- or bilateral covenant that facilitates the exchange and mutual protection of *Special Information* between two or more countries, also referred to as a *General Security Agreement (GSA)*. |
| **Security Effectiveness** | In the context of physical security, this concerns the period of time during which an unauthorised person can gain knowledge of, or access to, an *Interest to be Protected*. The *Security Effectiveness* depends on the delaying effect of the security measures taken in the physical domain (*Delay Time*) in relation to the *Intervention Time*. The *Security Effectiveness* is positive when the *Delay Time* is longer than the *Intervention Time*. In this case, *Intervention* will prevent a *Compromise*. A negative *Security Effectiveness* exists when the *Delay Time* is shorter than the *Intervention Time*. In this case, *Intervention* can only take place after a *Compromise* has taken place and *Intervention* ensures that the period in which the *Compromise* occurs is as short as possible. |
| **Security Incident** | An event that can lead or has led to a disruption of the normal course of events regarding the integral security of an *Interest to be Protected*, as a result of which the interests of the State, its allies or one or more ministries have been or could be jeopardised. |
| **Security Lighting** | A form of (outdoor) lighting designed to improve safety and deter crime. The aim is to keep areas well-lit at night so that potential threats or intruders can be more easily spotted. |
| **Security Officer** | An employee of the *Contractor* who has been nominated by the *Contractor* to *NOIS* as *Security Officer*. Following approval, the *Security Officer* shall be appointed by *NOIS*. A *Security Officer*, or their replacement, is responsible for the implementation, execution and supervision of compliance with the prescribed security measures. The *Security Officer* is the contact person for *NOIS*. |
| **Security Personnel** | Persons responsible for maintaining security at the *Contractor's* premises. This may involve both internal staff and external *Security Personnel*. |
| **Security Plan** | Description of how the security of a *Special Contract* and an *Interest to be Protected* is implemented based on the guidelines for drawing up a *Security Plan* set out in ABRO 2026. |
| **Security Screening** | The process based on the Security Investigations Act that leads to the issuance, refusal or revocation of a *Certificate of No Objection*. |
| **Security Systems** | *Systems* primarily designed to detect or control access to a *Compartment* or an *Interest to be Protected*. |
| **Segment** | A part of a larger *Network* that is logically or physically separated from other parts of *Network* components. In the case of physical separation, each *Segment* must use separate *Network* components such as switches, routers, cabling and firewalls, so that no physical infrastructure is shared. |
| **Self-Inspection** | Critical evaluation of design, existence and operational effectiveness of security measures by the *Contractor*. |
| **Sending** | The physical presentation of an *Interest to be Protected*, particularly *Special Information*, to a postal company that arranges for *Transport* to its final destination. Such *Transport* is generally not monitored |
| **Service Account** | A type of account created for running specific applications or services. These accounts are designed to perform automated tasks without human intervention, such as running a database service. In principle, a *Service Account* only has the *Rights* required to perform the assigned tasks. |
| **Signatures** | Characteristics of *Malware* based on which identification is possible. |
| **Significant Influence** | A formal or informal interest in an organisation through which changes in business operations, strategy or capabilities can be initiated and/or implemented by or on behalf of the stakeholder. |

| | |
|---|---|
| **SLA** | Service Level Agreement. Formal agreement between a service provider and a client, specifying the expected service quality and performance. It contains measurable criteria to assess the services provided. |
| **Sound Reduction Measurement** | A check to determine whether the sound is sufficiently muted for the relevant security level. This is part of an *Electronic Security Inspection*. |
| **Source Code** | The readable text that a programmer has written in a programming language. There are various programming languages, such as C, C++ and Pascal. The *Source Code* is converted by a compiler into a machine code that a computer can execute. |
| **Special Contract** | A government contract that affects national security, awarded by a public organisation as the *Contracting Authority* to a civilian party as the *Contractor* and involving an *Interest to be Protected*. |
| **Special Information** | Information that can have adverse consequences for the interests of the State, its allies or one or more ministries if non-authorised persons were to take cognisance of such information. *Special Information* is information that has been given a classification and must be secured accordingly. *Special Information* falls into an ITBP category, depending on the *Classification Level*. *Special Information* is always an *Interest to be Protected*, but an *Interest to be Protected* is not always classified. |
| **State Secret** | *Special Information* whose secrecy is required in the interest of the State or its allies. |
| **Storage Unit** | An object designed for the safe and organised storage of materials or documents with appropriate security measures in accordance with relevant NEN standards, such as a safe. |
| **Subcontractor** | A *Supplier* to which the *Contractor* has outsourced certain activities within the framework of the *Special Contract*, which provides the *Supplier* in question with access to or cognisance of an *Interest to be Protected*. Even if a *Supplier* does not have direct access to or cognisance of an *Interest to be Protected*, but does fulfil a crucial role in the context of a *Special Contract*, it can be designated as a *Subcontractor* based on a *Risk Analysis* in consultation with the *Contracting Authority*. |
| **Supplier** | An individual or organisation that supplies goods, materials or services to another entity. |
| **System** | An assembly of hardware, software, *Network* components, IT infrastructure and processes that work together to perform specific tasks or functions. |
| **System Account** | A type of account used by the operating system itself to run *System* processes and services (default account). These accounts are essential to the functioning of a *System* and are often created by a *System* during the installation of the operating system. *System Accounts* usually have extensive *Rights* within a *System* to ensure that they can perform all necessary tasks required for the management and operation of the operating system. |
| **System Documentation** | A document or set of documents that describe the implementation of a *System* to enable management to be carried out. |
| **Technical Infrastructure** | All *ICT Resources* for generic use, such as servers, firewalls, *Network* devices, operating systems for *Networks* and servers, database management systems, and management and security tools, including associated system files. |
| **TEMPEST** | The countering of potentially compromising emissions from electronic systems that could lead to the unauthorised capture, processing and reproduction of data. |
| **Tenant** | A separate and isolated instance within a shared *Cloud* environment. |
| **Transport** | Physical and monitored transportation of an *Interest to be Protected* or *Special Information*, while safeguarding *Confidentiality, Integrity and Availability (CIA)*. |

| | |
|---|---|
| **Trusted** | In accordance with a security level set by a competent authority, e.g. *Trusted* Zones or *Trusted Networks*. |
| **User** | An *Authorised Employee* who has access to information systems to perform their duties. *Users* are granted limited access *Rights* that provide only the access necessary to fulfil their role, in accordance with the principle of 'least privilege'. |
| **User Account** | An individual login account assigned to a specific individual to access *Systems*, applications or information resources to carry out their work. *User Accounts* are granted limited access *Rights*, tailored to the assigned tasks of the specific *User* and configured in accordance with the principle of 'least privilege'. |
| **Virtualisation** | A technology that allows one or more physical computer *Systems* (the host) to be split into multiple virtual machines (VMs) or containers, which can run independently of each other. A virtual machine has its own operating system and applications, and functions as if it were a separate physical computer. A container has a collection of software needed to run an application. |
| **Visitor** | An unauthorised person who, on the basis of *Need-to-Know* and *Need-to-Be*, has access to a *Compartment* under the supervision of an *Authorised Employee*. |
| **WAN** | Wide Area Network. A type of *Network* that covers a large geographical area, often on a national or even international scale. *WANs* connect multiple smaller *Networks*, such as LANs (Local Area *Networks*) or MANs (Metropolitan Area *Networks*), allowing devices and *Users* at different sites to communicate with each other. |
| **Wireless Communication** | A method for *Sending* information between two or more points by means of electromagnetic waves. Examples include Bluetooth, WiFi and 5G. |
| **Zero Footprint** | Using mechanisms to prevent sensitive information from being stored locally or from otherwise being retrievable during or after the use of a device. |
| **Zoning Measurement** | The measurement performed to determine which *TEMPEST* measures are required. |

# APPENDIX OVERVIEW

1. Setting up the security organisation
2. Security Officer
3. Crypto Custodian
4. List of Interests to be Protected
5. Physical security
6. Constructional measures
7. Transport and Sending
8. Labelling and destruction of Data Carriers
9. Approved Means
10. Scrubber
11. Cloud

# **APPENDIX 1:** SETTING UP THE SECURITY ORGANISATION

Each *Contractor* must have an integral security policy, or a security policy specifically prepared for the *Special Contract*. What's more, the *Contractor* must introduce a *Security Officer* to *NOIS* (see Appendix 2). In line with the security policy, the *Security Plan* is prepared by the *Security Officer*. Developing the *Security Plan* starts with a *Risk Analysis*, which details the risks that the *Contractor* will need to consider when executing the *Special Contract*.

It also describes which security measures have been realised and which still need to be realised. The *Self Inspection List* can be used for this purpose.

If a company executes multiple *Special Contracts*, it may be an option to prepare an integral *Security Plan* and secondary *Security Plans* for each *Special Contract* or site. In the case of an international contract, a *Project Security Instruction (PSI)* must be prepared stipulating the security requirements.

At the very least, the *Security Plan* addresses the following points:

- A description of the current *Special Contract(s)* including a clear description of the *Interest(s) to be Protected* on the company site and the *Classification Domain* and *Level* of *Special Information* on the company site;
- The roles and responsibilities relating to the *Special Contract(s)*, including the contact details of the *Security Officer* and, if applicable, of the *Deputy Security Officer, (Deputy) Cyber Security Officer* and *Crypto Custodian*;
- A *Risk Analysis* relating to the *Special Contract(s)*;
- A detailed *Incident Response Procedure*;
- Each component of the *Security Plan* must include a reference to the *ABRO* requirements complied with;
- An overview of and explanation to *ABRO* requirements for which no security measures have been implemented or which are yet to be realised;
- An updated *Self Inspection List* including an overview of the required security measure adjustments and the *Security Plan*;
- The procedure(s) for issuing, renewing and revoking digital *Certificates*.

Approval by *NOIS* is required for several aspects and procedures. Such approval may be obtained by recording said aspects and procedures in the *Security Plan* and receiving approval of the plan from *NOIS*:

| Section | Requirements |
|---|---|
| 4.1 Management of ICT Resources | 4.1.9 en 4.1.10 |
| 4.3 Identification and Authentication | 4.3.18 en 4.3.41 |
| 4.4 Configuration management | 4.4.3 |
| 4.5 Network security | 4.5.11, 4.5.13, 4.5.23, 4.5.24, 4.5.25, 4.5.34 en 4.5.35 |
| 4.6 Endpoint security | 4.6.12 |
| 4.7 Management of Mobile Equipment | 4.7.3 en 4.7.4 |
| 4.12 Maintenance | 4.12.7 en 4.12.8 |
| 4.14 Business continuity and recovery | 4.14.7 |
| 4.15 Development and acquisition | 4.15.7 |

At least once a year, the *Contractor* evaluates the *Security Plan*, using the *Self Inspection List* and a renewed *Risk Analysis*, to determine whether the *Security Plan* is still satisfactory or needs to be adjusted. In addition to the annual evaluation, a *Security Incident* or changing threat landscape may be another reason to revise the *Security Plan*. The *Security Plan* and any immediate or later changes are submitted to *NOIS* for approval. The *Contractor* is responsible for keeping track of the versions and changes in the *Security Plan's*.

# APPENDIX 2: SECURITY OFFICER

## Security Officer

On behalf of their employer, the *Security Officer* is responsible for the *Special Contract*'s security and serves as the primary contact for *NOIS*. One *Security Officer* is appointed. It is also possible to designate one or more *Deputy Security Officers*, for example to replace the *Security Officer* in their absence. A *Cyber Security Officer* may likewise be appointed, who can support the *Security Officer* in cybersecurity matters.

## Appointing and removing a Security Officer

The *Highest Executive Authority* of the *Contractor* nominates a candidate *(Deputy) (Cyber) Security Officer* to *NOIS*, using the appropriate '*Appointment* of *Security Officer*' form. After *NOIS*'s approval, a *(Deputy) (Cyber) Security Officer* is appointed.

There may be reasons why a *(Deputy) (Cyber) Security Officer* is or must be removed from their position. One of those reasons may be a change of position or role within the organisation. The *Contractor* must submit a request for removal using the '*Security Officer Removal*' form.

## Duties and responsibilities

The *Security Officer* may delegate duties, such as issuing authorisations for access to a *Compartment*, or have, e.g., a *Secondary Security Officer* support them. However, the *Security Officer* continues to be accountable.

The *Security Officer*'s responsibilities include:

- Preparing and updating the *Security Plan* at least once a year, or doing so if any changes occur;
- Coordinating and supervising the security relating to the *Special Contract*;
- Executing and updating a *Risk Analysis* for the *Special Contract*, at least once a year;
- Executing and repeating a *Self Inspection* using the *Self Inspection List*, at least once a year;
- Directly, independently and factually informing and advising the *Highest Executive Authority* of the *Contractor* on security matters relating to the *Special Contract*;
- Maintaining up-to-date records of *Interests to be Protected* (including copies);
- Capturing data on access to and insights into an *Interest to be Protected* and retaining this data to enable subsequent investigations into *Security Incidents*;
- Monitoring to see whether the registration of *Special Contract(s)* and *Employee(s) Involved* is up to date;
- Collaborating in compliance checks and investigations by or in coordination with *NOIS* that relate to a *Special Contract*;
- Reporting and investigating *Security Incidents* in coordination with *NOIS* and taking any additional security measures;
- Monitoring compliance with established regulations for the *Transport* and *Sending* of an *Interest to be Protected*;
- Providing information, training and guidance on security awareness;
- Coordinating international visits with *NOIS* related to the *Special Contract*;

- Maintaining an up-to-date overview of the entire chain of *Suppliers* and *Subcontractors* involved in the *Special Contract*;
- Regularly informing any *Deputy Security Officer* or *Cyber Security Officer* of procedures and *Security Incidents*, so they can execute the duties in the *Security Officer's* absence.

The *Cyber Security Officer* supports the *Security Officer* on *Cyber*-related security issues.
Examples include:

- Maintaining an up-to-date record of digital *Special Information*;
- Monitoring the implementation of essential *Cyber* security measures to ensure the *Confidentiality, Integrity and Availability* of an *Interest to be Protected*;
- Monitoring the *Confidentiality, Integrity and Availability* of the *Contractor*'s digital infrastructure;
- Coordinating the registration and handling of *Cyber*-related *Security Incidents*;
- Monitoring orderly and traceable procedures in case of changes to *Cyber* Security measures or the *Contractor's* digital infrastructure;
- Regularly informing the *Security Officer* about pending matters, such as the handling of *Cyber Security Incidents*.

# APPENDIX 3: CRYPTO CUSTODIAN

## Crypto Custodian

A *Crypto Custodian* is in charge of taking care of *Cryptographic Security Solutions*. A *Crypto Custodian* must have certified knowledge of cryptography. The *Highest Executive Authority* of the *Contractor* nominates a candidate *Crypto Custodian* to *NOIS* using the appropriate 'Appointment of *Crypto Custodian*' form. The *Security Officer* may also fulfil the role of *Crypto Custodian*. In that case, both the ' Appointment of Security Officer' form and the 'Appointment of Crypto Custodian' form must be submitted.

When the National Distribution Authority or the *Contracting Authority* provides the *Contractor* with cryptographic keys as part of a *Special Contract*, at least two *Crypto Custodians* are appointed, unless otherwise agreed with *NOIS*.

If, as part of an international contract, nationality requirements are set by the *Contracting Authority*, they must be complied with by the *Contractor*. This may also apply to a *Crypto Custodian* and is indicated by the *Contracting Authority*.

## Duties and responsibilities

In respect of *Cryptographic Security Solutions* as part of a *Special Contract*, the *Crypto Custodian* is responsible for:

- Complying with the *Contracting Authority*'s connection conditions, advice on deployment and manufacturer's advice and documenting the compliance in the *Security Plan*;
- Providing instructions for *Administrators* and training *Administrators*;
- Providing *User* instructions and training *Users*;
- *Authorising Users* and *Administrators* of *Cryptographic Security Solutions*;
- Documenting agreements, laws and regulations in the *Security Plan* that *Cryptographic Security Solutions* must comply with and implementing them in cryptographic techniques;
- Recording the process, actors and their responsibilities (in accordance with *RASCI*) relating to the management of *Cryptographic Security Solutions* in the cryptography policy as part of the *Security Plan*;
- Monitoring the validity of cryptographic keys in accordance with the cryptography policy as part of the *Security Plan*;
- Reporting and complying with the procedure for (potentially) compromised *Cryptographic Security Solutions* in consultation with *NOIS* and the owner of the cryptographic key(s);
- Acting as the primary contact for the owner of the cryptographic key(s);
- Registering the *Cryptographic Security Solutions* being used;
- Managing, issuing, loading and periodically counting keys, as well as listing *Cryptographic Security Solutions*;
- Storing, packaging and *Transporting Cryptographic Security Solutions*;
- Disposing and destroying *Cryptographic Security Solutions*.

# APPENDIX 4: LIST OF INTERESTS TO BE PROTECTED

The *List of Interests to be Protected* is prepared by the *Contracting Authority* prior to the *Special Contract* and then handed over to the *Contractor*. In respect of information, information systems, materiel, goods and objects relating to the *Special Contract*, the *List of Interests to be Protected* shows which ITBP category or *Classification Level* applies. In addition, the importance of the *Confidentiality, Integrity and Availability* of the information, information systems, materiel, goods and objects is set out clearly. A *Classification Designation List* is a way to map out the *Interests to be Protected* and the related ITBP categories or *Classification Level*s.

The *List of Interests to be Protected* thus provides insight into the applicable level(s) of the *Interest(s) to be Protected* under the *Special Contract*. In addition, the *Contractor* provides insight into the sub-areas, and thus the *ABRO* 2026 chapters, applicable for the *Special Contract*. Based on this *List of Interests to be Protected*, the *Contractor* coordinates with *NOIS* to apply the essential security measures in line with the requirements stipulated in *ABRO* 2026.

## List of Interests to be Protected in the event of Outsourcing

Where a *Contractor Outsources* work for the *Special Contract* to one or more *Subcontractor(s)*, the *Contractor* must prepare a *List of Interests to be Protected* for the work executed by the *Subcontractor(s)* involved. The *List of Interests to be Protected* is prepared in coordination with the *Contracting Authority* and *NOIS*, providing the *Contracting Authority* and *NOIS* with permanent insight into the *Subcontractor(s)* with access to an *Interest to be Protected*.

## Foreign equivalent

Companies may also qualify for a *Special Contract* from *NATO*, *EU* or a foreign government organisation. Hence, apart from national *Interests to be Protected*, *NATO*, *EU* or foreign *Interests to be Protected* may be involved. For the company involved *NOIS* acts as the Designated Security Authority (DSA) on behalf of those organisations and countries. It is often a condition that agreements regarding this are documented in a *Security Treaty* or a so-called *Memorandum of Understanding (MoU)*.

*NATO* and *EU* regulations, and often international treaties, too, require the inclusion of a specific *'Project Security Instruction' (PSI)* in contracts with *NATO*, *EU* and foreign governmental organisations where it involves security requirements of large projects. In this respect a *'Security Aspect Letter' (SAL)* is often used for smaller projects. The contents of a *PSI* and *SAL* share many similarities with *ABRO* 2026. For instance, the PSI and *SAL* have a *'Security Classification Guide'* and a *'Security Classification Checklist'*, the equivalent of the *List of Interests to be Protected* included in *ABRO* 2026. *ABRO* 2026 is used to inspect companies working on such *Special Contracts*.

# APPENDIX 5: PHYSICAL SECURITY

Physical security measures are implemented to prevent an unauthorised person from gaining physical access to an *Interest to be Protected*. The *Interest to be Protected* must be secured such that *Compromise* is prevented as well as detected and/or identified. A combination of Organisational, Constructional, Electronic and Reactive measures is implemented to achieve this.

- Organisational measures:
  Organisational measures may include access control and the process of identification, *Authentication* and *Authorisation* of persons. In this respect the '*Need-to-Know*' and '*Need-to-Be*' principles are taken into account at all times.
- Constructional measures:
  Constructional measures form the backbone of physical security measures. Examples include intruder-resistant walls, intruder-resistant glass and reinforced fittings on doors and windows (also see Appendix 6).
- Electronic measures:
  Electronic measures include all material electronic, electrical or optical devices that have an observing, directing, signalling or alarming position. Examples include camera systems (CCTV), access management systems (such as *EAMS*) and various types of detectors (such as *IDSS*).
- Reactive measures:
  The reaction to perceived or actual *Security Incidents* is essential for an *Interest to be Protected*. Examples of reactive measures are procedures for alarm follow-up, alarm verification and *Intervention*.

Determination of the required measures is based on inside-out reasoning, with the *Interest to be Protected* as a starting point. An *Interest to be Protected* must be placed in a *Compartment*. In addition, a *Compact Interest to be Protected* - such as a laptop, but also larger objects that can reasonably be physically stored - must be placed in an appropriate *Storage Unit*. Appropriate Organisational, Constructional, Electronic or Reactive security measures must then be taken to counteract *Compromise* of the *Interest to be Protected*, detect this and to have *Intervention* take place in a timely manner.

Physical security measures are always organised according to a layered structure, such as by placing an *Interest to be Protected* in a *Storage Unit* and placing this *Storage Unit* in a locked room or, for example, a *Compartment*. The layered structure of physical security measures ensures that *Delay Time* is realised. What's more, it prevents the breach of a single security measure from immediately leading to *Compromise* of the *Interest to be Protected*.

## Security Effectiveness

The *Security Effectiveness* forms the basis for determining the physical security measures required. The *Security Effectiveness* derives from the *Delay Time* and the *Intervention Time*. In determining the required *Delay Time* insight needs to be gained into the physical threats and risks relating to the *Special Contract* and the *Interest to be Protected*. To this end, a *Risk Analysis* needs to be performed. In addition, it is important to gain insight into the means available to a potential offender, for which the offender profile can be used. Upon request, *NOIS* can provide such a profile.

*ABRO* 2026 defines the required *Security Effectiveness* for the various ITBP categories, also see the following table.

| ITBP category | Security Effectiveness |
|---|---|
| ITBP 1 and ITBP 2 | *Interests to be Protected* in this category require a positive *Security Effectiveness*. Hence, *Intervention* must always take place before *Compromise* has occurred (*Intervention Time* < *Delay Time*). |
| ITBP 3 | *Interests to be Protected* in this category require a *Security Effectiveness* of 120 minutes at the most. Hence, *Intervention* must always take place within 120 minutes of *Compromise* (*Intervention Time* - *Delay Time* < 120 minutes). |
| ITBP 4 | *Interests to be Protected* in this category require no *Security Effectiveness*. *Compromise* or attempts to do so must be detected, but no time has been set for this. After detection of *Compromise*, *NOIS* will be notified within 48 hours. |

## Example for ITBP 1 and 2

In realising positive *Security Effectiveness*, it must thus be determined what measures are needed to slow down an offender to such an extent following an alert that *Intervention* always takes place before *Compromise*. This depends on the *Intervention Time*. When the *Intervention Time* is 15 minutes, less or less strict measures are needed to delay an offender than when the *Intervention Time* is 30 minutes.

The *Intervention Time* in the following example is 30 minutes, so the joint physical security measures must have a *Delay Time* of at least 30 minutes to realise a positive *Security Effectiveness*. One of the ways to do so can be by installing vibration sensors on the *Storage Unit* and by using a *Storage Unit* that provides sufficient *Delay Time* in accordance with the NEN standards described in Appendix 6.

The *Delay Time* depends on the means that an offender may reasonably have available. The NEN standards and the offender's means available can be used to determine the *Delay Time* of a physical security measure. Another option is to install detection equipment outside the *Compartment*. So after having been detected, an offender would first have to break through the constructional protection of the *Compartment*, after which they would also need to force their way into the *Storage Unit*. Suppose the *Compartment* ensures a 10-minute Delay Time. A 20-minute *Delay Time* for the *Storage Unit* would then be enough, as this would result in an aggregate 30-minute *Delay Time*.

In both options, it would still take an offender 30 minutes after detection to gain actual access to the *Interest to be Protected*. Since *Intervention* takes place within 30 minutes in this example, the offender will be blocked before the *Interest to be Protected* is compromised.

The *Contractor* consults with *NOIS* about the physical security measures to be taken. Figure 1 shows a schematic representation of a calculation example.

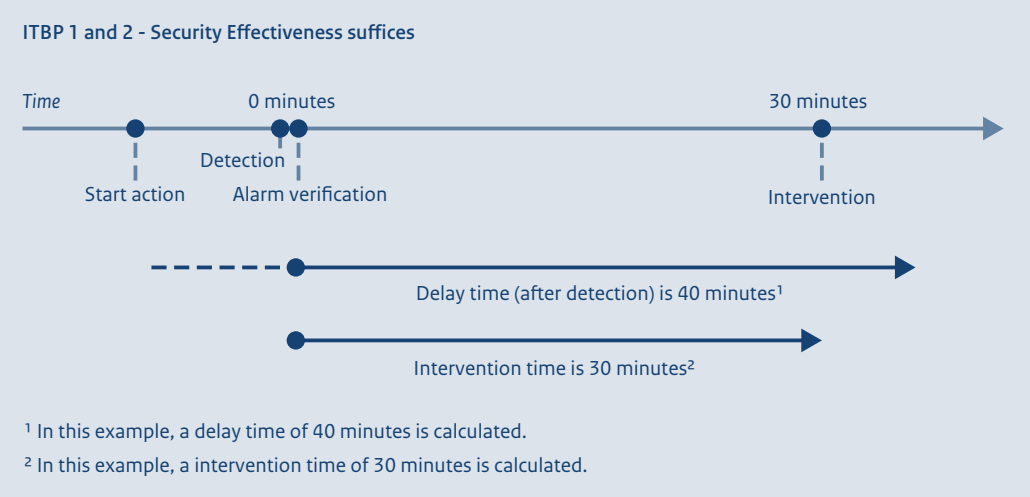



Figure 1: Calculation example ITBP 1 and 2

In the example in Figure 1, a 40-minute *Delay Time* is generated. The *Intervention Time* is 30 minutes after detection, thus realising the required positive *Security Effectiveness*. Hence, in this situation there is no *Compromise* of the *Interest to be Protected*.

The physical security measures must be designed such that a positive *Security Effectiveness* is realised. The following table shows another timeline, where this is not the case (figure 2). The *Intervention Time* in this example is 50 minutes after detection. The realised *Delay Time* is 30 minutes, allowing the offender 20 minutes of unauthorised access to the *Interest to be Protected*.

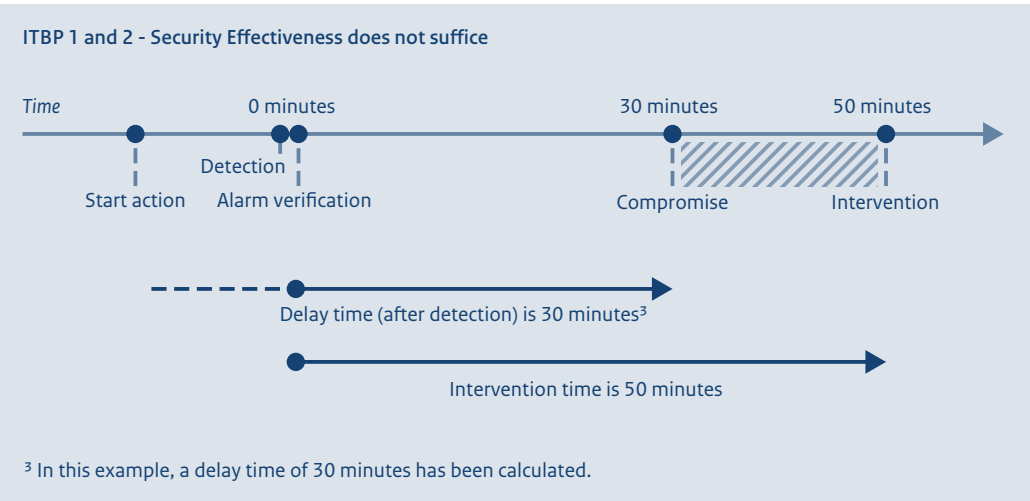



Figure 2: Calculation example where positive security returns were not realised

## Example for ITBP 3

The physical security measures in the following example realise a 30-minute *Delay Time* (Figure 3). This means that 30 minutes after detection, a non-authorised person has access to or can take cognisance of an *Interest to be Protected*. Examples of security measures to generate *Delay Time* include

placing an *Interest to be Protected* in a *Storage Unit*, such as a safe. ITBP 3 requires *Intervention* to take place no later than 120 minutes after *Compromise*. The safe in this example has a 30-minute *Delay Time*, so an offender would need 30 minutes to force the safe. Since it is equipped with vibration sensors, the safe triggers an alert and initiates *Intervention* as soon as the offender starts forcing the safe. The *Intervention Time* in this example is 140 minutes. So the *Security Officer* or the *Security Personnel* present are on site no later than 140 minutes after the *Alert*. Since it takes the offender 30 minutes to force the safe, the offender has access to the *Interest to be Protected* for a maximum of 110 minutes and thus *Compromise* occurs before *Intervention* takes place.

In the following example *Intervention* takes place within 110 minutes of *Compromise*. Hence, the *Security Effectiveness* is 110 minutes, which is within the required 120 minutes. In this case, too, the *Contractor* consults with *NOIS* about the physical security measures to be taken. The following figure shows a schematic representation of this example (Figure 3).

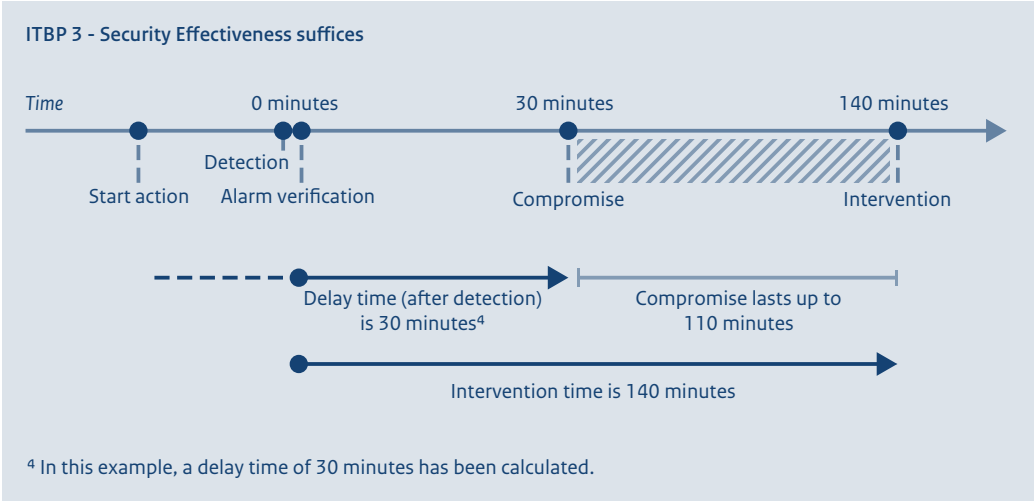



Figure 3: Calculation example ITBP 3

ITBP 3 requires realising a 120-minute *Security Effectiveness*. The following table shows another time-line, where this is not the case (Figure 4). The *Intervention Time* in this example is 150 minutes after detection. The *Delay Time* realised is 20 minutes, resulting in a 130-minute *Security Effectiveness*, which is more than the required 120 minutes.

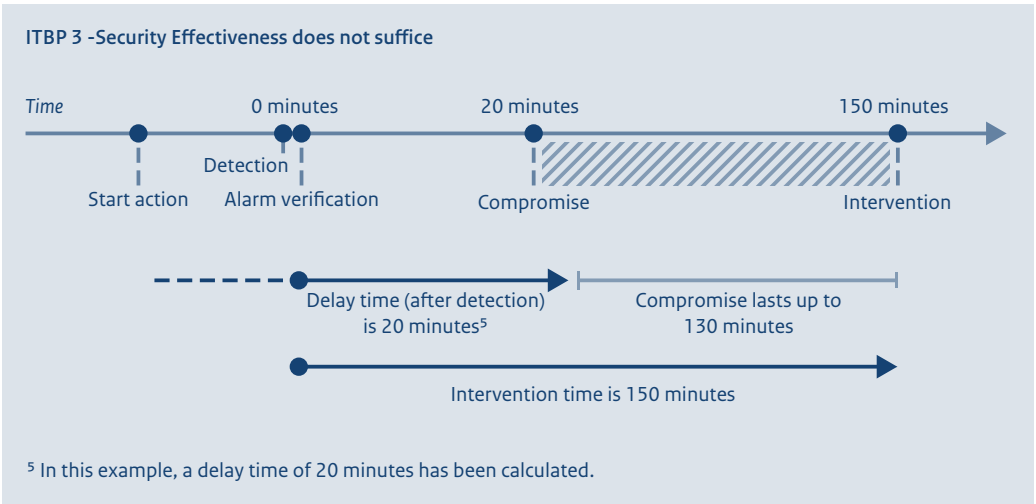



Figure 4: Calculation example where the required *Security Effectiveness* is not realised

# APPENDIX 6: CONSTRUCTIONAL MEASURES

Constructional security measures are an important part of the mix of Organisational, Contructional, Electronic and Reactive measures. So in the event of plans for new construction or constructional changes, it is important to address adequate constructional measures at the required security level in a timely manner. In the case of existing construction, the *Contractor* consults with *NOIS* about the physical security measures to be taken. Examples of constructional measures are:

- Burglar-resistant walls;
- Reinforced doors;
- Burglar-resistant glass;
- Reinforced fittings on doors and windows;
- Fencing and other site adjustments.

Constructional measures are an important barrier against non-authorised persons trying to gain physical access to an *Interest to be Protected*. Examples include break-ins, usually with the aim of theft, espionage or sabotage, but also erroneous access by non-authorised employees. The relevant NEN standards may be used to determine the required constructional measures. The table on the next page includes an overview.

An *Interest to be Protected* must be placed in a (constructional) *Compartment*. If it is a *Compact Interest to be Protected* (such as a laptop or *Special Information*), the *Compact Interest to be Protected* must be placed in a *Storage Unit*.

## Measures to restrict visibility and noise level

Visual security measures (restricting the visibility) and acoustic security measures (restricting the noise level) are necessary as well. These measures must prevent non-authorised persons on the outside of the *Compartment* from gaining knowledge, either with or without the use of means, of the *Interest to be Protected*.

Security measures to restrict visibility prevent non-authorised persons on the outside of the work-space from taking cognisance of an *Interest to be Protected*. These measures are necessary regardless of the *Classification* and/or *Marking*. Security measures to restrict the noise prevent non-authorised persons from gaining knowledge, either with or without the use of auditory means, of an *Interest to be Protected* by observation (eavesdropping) from the outside of the workspace. These measures are not necessary for ITBP 4.

Such security measures are implemented in meeting rooms, briefing rooms and work areas in which an *Interest to be Protected* is discussed or dealt with.

## Appendix 6.1: Overview of NEN standards

The following table shows an overview of relevant NEN standards on physical security.

| | |
|---|---|
| NEN-EN 5096 | Intruder resistance<br>• Facade elements with doors, windows, shutters and fixed infillings<br>• Requirements, classification and test methods |
| NEN-EN 1143 | Secure storage units<br>• Requirements, classification and methods of test for resistance to burglary |
| NEN-EN-1627 | Pedestrian doorsets, windows, curtain walling, grilles and shutters<br>• Burglar resistance<br>• Requirements and classification |
| NEN-EN 50131 | Alarm systems<br>• Intrusion and hold-up alarm systems |
| NEN-EN 50136 | Alarm systems, specifically alarm transmission systems and equipment |
| NEN-EN-IEC 62676 | Video surveillance systems for use in security applications |

# APPENDIX 7: TRANSPORT AND SENDING

An *Interest to be Protected* is more vulnerable during *Transport* or *Sending* than when it is located in a protected site. This is because it is not possible to fall back on the Organisational, Contructional, Electronic and Reactive measures protecting the *Interest to be Protected* in the normal situation within the *Compartment*. The increased vulnerability raises the possibility of *Compromise* of the *Interest to be Protected*. If international *Transport* and *Sending* is involved, this vulnerability increases even further.

An important principle underlying *Transport* or *Sending* of an *Interest to be Protected* is that it must be kept to a minimum. If the execution of the *Special Contract* requires an *Interest to be Protected* to be moved outside the *Compartment*, the *Security Officer* must approve this in advance. It is equally important to verify that the receiving party, such as a *Subcontractor*, has implemented appropriate security measures to ensure the required security level of the *Interest to be Protected*

In the *Security Plan* the *Security Officer* describes how to deal with *Transport* and *Sending* of an *Interest to be Protected*. This includes at least the following points:

- (Additional) relevant legislation and regulations;
- International agreements, as stipulated in a *PSI* or *SAL*;
- *Risk Analysis* relating to *Transport* and *Sending*, including associated threats;
- Role of the *Contracting Authority* in *Transport* and *Sending*;
- Dealing with practical issues, such as transfer, waiting times and overnight stays.

If a *Security Incident* occurs unexpectedly during *Transport* or *Sending*, the *Incident Response Procedure* must be initiated immediately.

## Sending

*Sending* is defined as the physical presentation of an *Interest to be Protected*, in particular *Special Information*, to a postal company that arranges for usually uncontrolled transport to its final destination. It is only permitted to send ITBP 4/NLD RESTRICTED.

Prior to *Sending*, the *Interest to be Protected* involved must be packaged such that the contents are not visible and not identifiable, and that any breach can be detected. An immediate acknowledgement of receipt is also required. *Sending* outside the Netherlands is done by registered mail, with a track and trace number.

In addition, when *Sending* an *Interest to be Protected*, an acknowledgement of receipt is required. In such situations, an acknowledgement of receipt is enclosed with the packaging of the *Interest to be Protected*. The recipient must return the signed acknowledgement of receipt, bearing at least a signature and date, to the sender. The sender must ensure that the acknowledgement of receipt is received within a reasonable time. A reasonable time is defined as:

- Within the Netherlands: 2 weeks;
- Within Europe: 3 weeks;
- Outside Europe: 1 month.

If the acknowledgement of receipt is not returned within the above deadline, the sender must make enquiries with the recipient. If this is unsuccessful, the sender must notify the *Security Officer*. If the *Transport* has not arrived, this must be treated as a *Security Incident*.

## Transport

*Transport* is defined as the physical and controlled transportation of an *Interest to be Protected* or *Special Information* while safeguarding the *Confidentiality, Integrity and Availability*. The *Transport* of an *Interest to be Protected* is usually bespoke and the *Contracting Authority* stipulates security measures for such *Transport*.

Prior to a *Transport* of *Special Information* of ITBP 3, ITBP 2 and ITBP 1, a transport plan must be prepared in accordance with the 'Transport Plan' form and submitted to the *Contracting Authority* for approval in coordination with *NOIS*. The transport plan describes the actual set-up of the *Transport* in line with the guidelines in the *Security Plan*. *Transport* of an ITBP 1 only takes place after prior approval of the *Contracting Authority*.

The *Contractor* has a number of options for the *Transport* of *Special Information* of ITBP 2, 3 and 4 within the Netherlands:

- *Transport/courier company* with *ABRO Declaration*;
- *Transport* by *Authorised Employees*.

Prior to *Transport* and *Sending*, the *Special Information* must be carefully packaged. The transport plan describes how the *Special Information* is to be packaged.

## International Transport

For international *Transport*, the transport plan must be agreed with *NOIS* and submitted to the *Contracting Authority* for approval at least 10 working days prior to *Transport*. In addition to the requirements and measures for securing *Transport* listed in *ABRO* 2026, specific bilateral or multilateral agreements may have been made for international *Transport* of a domestic or foreign *Interest to be Protected*. This is usually stipulated in a *PSI* or *SAL*.

# APPENDIX 8: LABELLING AND DESTRUCTION OF DATA CARRIERS

It is important for *Data Carriers* to be labelled with the *Classification* and/or *Marking* that indicates how *Data Carriers* must be handled and stored. When the *Special Contract* has been terminated or *Data Carriers* are no longer required for the *Special Contract*, the *Data Carriers* must be destroyed.

## Labelling of Data Carriers

| | Application | Classification text | Method of application | Location of classification/ marking |
|---|---|---|---|---|
| **Document** | Entire document is classified and/ or marked | *Classification* and/or *Marking* in capital letters (only on first page or in colophon: listing the person determining the *Classification*, date when this has been determined, and period of validity). | • Handwritten<br>• Printed<br>• Stamped | • Top and bottom of each page<br>• On cover<br>• On appendix<br><br>(Adding copy and page numbering) |
| **Document** | Appendix has a higher classification and/or marking than main document | Highest *Classification* and/ or *Marking* in capital letters.<br><br>(In colophon: listing the person determining the *Classification*, date when this has been determined, and period of validity) | • Handwritten<br>• Printed<br>• Stamped | On cover of main document: <highest *Classification/Marking*> with addition, without appendix (x) <*Classification/ Marking*> or <unclassified/ unmarked>.<br><br>On the appendix (or appendices) at the top and bottom of each page.<br><br>(Adding copy and page numbering). |
| **Document** | Various *Classifications* in a single document. | (NLD TS): section with information classified as NLD TOP SECRET<br><br>(NLD S): section with information classified as NLD SECRET<br><br>(NLD C): section with information classified as NLD CONFIDENTIAL<br><br>(NR) section with information classified as NLD RESTRICTED | • Handwritten<br>• Printed<br>• Stamped | Highest *Classification* at top and bottom of each page. Add abbreviation of *Classification* at the beginning of each section. (Adding copy and page numbering). |

| | Application | Classification text | Method of application | Location of classification/ marking |
|---|---|---|---|---|
| **Removable Data Carriers** | All *Classifications* and/or *Markings*. | Highest level of *Classification* and/or *Marking* in capitals. | Engrave, brand or inscribe *Data Carriers* with waterproof marker, or apply a sticker with *Classification / Marking*, colour or ribbon/label. | Place stickers or (engraved) text visibly. If possible, place a sticker or (engraved) text on both sides. |
| **Workstations** | All *Classifications* and/or *Markings*. | Highest level of *Classification* and/or *Marking* in capitals. | Sticker with *Classification / Marking*. | Place stickers visibly on system case and top screen. |
| **Laptops** | All *Classifications* and/or *Markings*. | Highest level of *Classification* and/or *Marking* in capitals. | Sticker with *Classification / Marking*. | Place stickers visibly on outside screen/flap. |

Labelling *Data Carriers* in the above manner may attract unwanted attention. If so, the colour system below may be used. If this is done, the table of user instructions must be described in the *Security Plan*.

## Labelling of Data Carriers using colour system

| | | | |
|---|---|---|---|
| | **Red** | ITBP 1 | NLD TOP SECRET |
| | **Blue** | ITBP 2 | NLD SECRET |
| | **Green** | ITBP 3 | NLD CONFIDENTIAL |
| | **Yellow** | ITBP 4 | NLD RESTRICTED |
| | **White** | | Unclassified |

## Destruction of Data Carriers

| | ITBP 4<br>NR | ITBP 3<br>C | ITBP 2<br>S | ITBP 1<br>TS |
|---|---|---|---|---|
| Paper | Shred L < 30mm | Shred L < 25mm<br>B < 3mm | Shred L < 25 mm<br>B < 3 mm | Shred L < 25 mm<br>B < 3 mm and burn |
| Paper as part of international contract | B < 5mm | Shred max. 25mm2 | Shred max. 25mm2 | Shred max. 25mm2 |
| Film | Shred max. | Shred (destruction grade P4*, max 160mm2) | Shred (destruction grade P5*, max. 30mm2) | Shred (destruction grade P5*, max. 30mm2) and burn |
| Optical Data Carriers (CD/NRD) | 25mm(2 | Shred (destruction grade O4*, max. 30mm2) | Shred (destruction grade O5*, max | Shred (destruction grade O5*, max. 10mm2) and burn |
| Tapes | Shred | Shred (destruction grade T4*, max. 160mm2) | Shred (destruction grade T5*, max. 30mm2) | Shred (destruction grade T5*, max. 30mm2) and burn |
| Hard drive | Break | Shred (destruction grade H4*, max 2000mm2) | Shred (destruction grade H5*, max 320mm2) | Shred (destruction grade H5*, max. 320mm2) and burn |
| USB flash drive | Drill | Shred (destruction grade E4*, max. 30mm2 | Shred (destruction grade E5*, max. 10mm2) | Shred (destruction grade E5*, max. 10mm2) and burn |
| Other | Break | Shred | Shred | Shred and burn |

*In accordance with DIN 66399

# APPENDIX 9: APPROVED MEANS

Several requirements refer to the use of *Approved Means*. In many cases, this involves *Cryptographic Security Solutions* or specific software for securing connections. A limitative selection of evaluated products is used for both Dutch and international *Special Contracts*. Using these *Means* is only permitted when the evaluated version is used and the advice on deployment are fully complied with. These advice on deployment can be requested through *NOIS*.

## International

Evaluated products, such as from *NATO* or *EU* or based on international treaties (*MoU*, GSA), are used for international *Special Contracts*. Use of these *Means* is always coordinated with *NOIS*.

## National

The list of the *GISS* Resilience Unit ('AIVD Unit Weerbaarheid') of evaluated products is leading for all *Classification Levels*. The Resilience Unit's list is available on the *GISS* website.

In certain situations, the selection of evaluated products may be insufficient. In exceptional cases, an application can be submitted through *NOIS* to obtain approval for the use of a non-evaluated product, subject to strict conditions. In addition, the applicable *ABRO* requirements must be met, one of which is that the products neither originate from nor depend on countries with a known *Offensive Cyber Programme* against the Dutch State.

# APPENDIX 10: SCRUBBER

## Purpose of a Scrubber

Before they are used, *Removable Data Carriers* are checked with a purpose-built *Scrubber*. A *Scrubber* is a stand-alone *System* that checks *Removable Data Carriers* for the presence of *Malware* and quarantines them if necessary.

A *Scrubber* at least complies with the following characteristics:

- It is a completely isolated system, without any connection to other *Networks*, and with all wireless connections being disabled;
- It is secured at the highest *Classification Level* of the data;
- No data is left on a *Scrubber*, which means data is completely removed after processing;
- At least two different types of *anti-Malware* software are used and they are different from *anti Malware* software applied in the *Network* on which the *Removable Data Carrier* will ultimately be used;
- The indicators used, such as virus definitions and *Signatures*, are no more than seven days old and a process is described to renew these indicators in a timely manner.

If this renewal is not performed, then the *Scrubber* is disabled and its use is made impossible until the moment when the virus definitions and *Signatures* have been renewed. Upon detection of *Malware*, the *(Cyber) Security Officer* is notified.

## Practical examples of operation

The following describes a few example situations in which a *Scrubber* is used:

1. When an approved USB stick arrives, it is first decrypted and scanned by the *Scrubber* before being placed in a *Network* with *Interests to be Protected*. Next, the USB stick is transferred to the *Trusted Network*.

2. When an encrypted file arrives through an untrusted *Network*, it is first decrypted and scanned on the *Scrubber*. Next, the file is moved to a *Trusted Network* on an approved USB stick.

3. When data is sent, it is recommended to first have it scanned by the *Scrubber* before placing it on an approved USB stick.

# APPENDIX 11: CLOUD

Chapter 5 describes the requirements that apply specifically to *Cloud solutions*. In addition, some specific requirements from Chapter 3 and Chapter 4 likewise apply to *Cloud solutions*. These are listed in the following table.

## Relevant requirements for Cloud solutions from Chapter 3 and Chapter 4

| | Hoofdstuk 3 - Fysiek | Hoofdstuk 4 - Cyber |
|---|---|---|
| Specific requirements | 3.1.10<br>3.1.11<br>3.1.12<br>3.1.13 | 4.5.20<br>4.13.8<br>4.13.9<br>4.15.20 |
| Section* | | 4.6 Endpoint Security<br>4.7 Management of *Mobile Equipment*<br>4.8 Cryptography |

* Cryptography, Endpoint Security and management of *Mobile Equipment*

Depending on the exact design of the *Cloud service* to be provided, the stipulated requirements in the sections 'Cryptography', 'Endpoint Security' and 'Management of *Mobile Equipment*' of Chapter 4 also apply.

- The requirements stipulated in the section 'Cryptography' apply to a *Cloud solution* when *CSP* is responsible for key management.
- The requirements stipulated in the sections 'Endpoint Security' and 'Management of *Mobile Equipment*' apply to a *Cloud Solution* when the workstations or *Mobile Equipment* used by the *Contracting Authority* to use the *Cloud Solution* are not managed by the *Contracting Authority*.

**This document is a publication of:**
Government of the Netherlands

January 2026