**Handling Security Plan (HSP)**

**Rev. 1 (20190924)**

**Name of the company: Click here to type text**

**Identification/name of the HSP: Click here to type text**

**Version of the HSP: Click here to type text**

**Degree of confidentiality and protection of the HSP: Click here to type text**

**Approval date of the HSP by the FANC: Click here to type text**

**Application date of the HSP: Click here to type text**

**Expiry date of this version of the HSP: Click here to type text**

Table of Contents

[Preliminary remarks made by the FANC 5](#_Toc17118505)

[1. General 6](#_Toc17118506)

[1.1. Coordinates of the company 6](#_Toc17118507)

[1.1.1. ☐ ☐ Name of the natural or legal person 6](#_Toc17118508)

[1.1.2. Addresses of the company 6](#_Toc17118509)

[*1.1.2.1* ☐ ☐ *Head office* 6](#_Toc17118510)

[*1.1.2.2* ☐ ☐ *Operational headquarters* 6](#_Toc17118511)

[1.2. Short description of the company activities 6](#_Toc17118512)

[1.2.1. ☐ ☐ General 6](#_Toc17118513)

[1.2.2. ☐ ☐ The transports 6](#_Toc17118514)

[1.3. ☐ ☐ Typical steps of the handling 6](#_Toc17118515)

[1.4. ☐ ☐ Objectives of the security plan 7](#_Toc17118516)

[1.5. ☐ ☐ Name of the HSP and the version 7](#_Toc17118517)

[2. Responsibilities with regard to security 8](#_Toc17118518)

[2.1 Identification of the security coordinator 8](#_Toc17118519)

[2.1.1. ☐ ☐ Surname, Name 8](#_Toc17118520)

[2.1.2. ☐ ☐ Telephone numbers, fixed and mobile 8](#_Toc17118521)

[2.1.3. ☐ ☐ Email address 8](#_Toc17118522)

[2.1.4. ☐ ☐ Address 8](#_Toc17118523)

[2.1.5. ☐ ☐ Hierarchical position within the company (organigram) 8](#_Toc17118524)

[2.1.6. ☐ ☐ Qualifications 8](#_Toc17118525)

[2.2 Identification of the back-up 8](#_Toc17118526)

[2.2.1 ☐ ☐ Surname, Name 8](#_Toc17118527)

[2.2.2 ☐ ☐ Telephone numbers, fixed and mobile 8](#_Toc17118528)

[2.2.3 ☐ ☐ Email address 8](#_Toc17118529)

[2.2.4 ☐ ☐ Address 8](#_Toc17118530)

[2.2.5 ☐ ☐ Hierarchical position within the company (organigram) 9](#_Toc17118531)

[2.2.6 ☐ ☐ Qualifications 9](#_Toc17118532)

[3 Materials to be handled 10](#_Toc17118533)

[3.1 ☐ ☐ Description of the radionuclides 10](#_Toc17118534)

[4 Evaluation of the usual operations during the handling and the corresponding risks 11](#_Toc17118535)

[4.1 Evaluation of the risks 11](#_Toc17118536)

[4.1.1 ☐ ☐ Short description of the evaluation method used 11](#_Toc17118537)

[4.1.2 ☐ ☐ Risk analysis for each type of handling and situation 11](#_Toc17118538)

[5 Measures 12](#_Toc17118539)

[5.1 ☐ ☐ Management system 12](#_Toc17118540)

[5.2 Personnel 12](#_Toc17118541)

[5.2.1 ☐ ☐ Training 12](#_Toc17118542)

[5.2.2 ☐ ☐ Trustworthiness and access rights of persons 12](#_Toc17118543)

[5.3 Access management (information, vehicles, zones, material) 12](#_Toc17118544)

[5.3.1 ☐ ☐ Access control 12](#_Toc17118545)

[5.3.2 ☐ ☐ Access rights 12](#_Toc17118546)

[5.3.3 ☐ ☐ Management of the access tools (keys, badges, codes, …) 12](#_Toc17118547)

[5.4 Equipment management 12](#_Toc17118548)

[5.4.1 ☐ ☐ Maintenance of the security equipment 12](#_Toc17118549)

[5.4.2 ☐ ☐ Tests 13](#_Toc17118550)

[5.4.3 ☐ ☐ Compensatory measures 13](#_Toc17118551)

[5.5 ☐ ☐ Cooperation with the authorities (Police, …) 13](#_Toc17118552)

[5.6 Punctual threat 13](#_Toc17118553)

[5.6.1 ☐ ☐ Information channels 13](#_Toc17118554)

[5.6.2 ☐ ☐ Punctual threat 13](#_Toc17118555)

[5.7 Management of the usual operations and situations (cf. section 4) 13](#_Toc17118556)

[5.7.1 ☐ ☐ Management and supervision 13](#_Toc17118557)

[5.7.2 ☐ ☐ Tracking 13](#_Toc17118558)

[5.7.3 ☐ ☐ Interfaces with the parties involved 13](#_Toc17118559)

[5.7.4 ☐ ☐ Detection 14](#_Toc17118560)

[5.7.5 ☐ ☐ Delay 14](#_Toc17118561)

[5.7.6 ☐ ☐ Response 14](#_Toc17118562)

[6 Notification of security incidents and possible interventions. 15](#_Toc17118563)

[6.1 ☐ ☐ Notification of threat, security breaches or related incidents 15](#_Toc17118564)

[6.2 ☐ ☐ Actions taken in case of malicious acts 15](#_Toc17118565)

[7 Security plans 16](#_Toc17118566)

[7.1 Evaluation 16](#_Toc17118567)

[7.1.1 ☐ ☐ Exercises 16](#_Toc17118568)

[7.1.2 ☐ ☐ General evaluation 16](#_Toc17118569)

[7.2 ☐ ☐ Revision and updating 16](#_Toc17118570)

[8 Information 17](#_Toc17118571)

[8.1 ☐ ☐ Physical protection 17](#_Toc17118572)

[8.2 ☐ ☐ Dissemination of information 17](#_Toc17118573)

[9 ☐ ☐ Additional information provided by the carrier 18](#_Toc17118574)

[10 ☐ ☐ Attachments 19](#_Toc17118575)

[11 ☐ ☐ Signatures 20](#_Toc17118576)

# Preliminary remarks made by the FANC

1. This form applies to all handlers having the obligation to draw up a HSP within the framework of the modal regulations (e.g. the ADR, see paragraph 1.10.3.2.).
2. All fields on the form must be completed by the handler.
	1. If the handler considers a question not applicable, he/she can justify this in the corresponding text field.
	2. If the handler thinks it would be easier to provide the requested information in an attachment, he/she can refer to this attachment. If necessary, please specifically refer to the exact location of the information within the attached document.
	3. If the FANC is already in possession of the requested information, please indicate where the information can be found.
3. Please beware when providing information in the security plan: take all necessary measures to guarantee its confidentiality.
4. The two checkboxes before each title are meant for the evaluation of the HSP by the FANC.
5. The information in the HSP must focus on security, in other words the prevention of acts of malevolence. Measures within the framework of management, radiation protection or safety can also be mentioned, as far as they contribute – be it indirectly – to the security objectives.
6. If the handler established a security plan based on a different regulation, he/she can mention this in section ‘9. Additional information provided by the handler’. If the handler wants to refer to that security plan to complete certain sections of the HSP, he should proceed as described in point 2) above and attach the security plan (see Section ’10. Attachments’).

# General

## Coordinates of the company

## [ ]  [ ]  Name of the natural or legal person

*Also mention, depending on the case, the number of the Crossroads Bank for Enterprises (CBE) or the National Register Number (NRN).*

**Click here to type text.**

## Addresses of the company

## [ ]  [ ]  Head office

**Click here to type text.**

## [ ]  [ ]  Operational headquarters

**Click here to type text.**

## Short description of the company activities

*Short description of the company activities allowing us to define the context this HSP has been established in.*

### [ ]  [ ]  General

**Click here to type text.**

### [ ]  [ ]  The transports

**Click here to type text.**

## [ ]  [ ]  Typical steps of the handling

*Describe the different steps of a typical handling. E.g.:*

* *Unloading inbound vehicle*
	+ *Where does this happen? What type of vehicles are involved?*
* *Temporary storage outside secured location*
	+ *What are the locations where the radioactive sources are placed before they go to a secured location? For how long are they usually stored there ? How are the sources moved?*
* *Temporary storage within a secured location*
	+ *Where are the sources stored? For how long are they usually stored there ?*
* *Temporary storage outside secured location (preparation for departure)*
	+ *Where does this happen? For how long?*
* *Loading outbound vehicle*
	+ *Where does this happen? What type of vehicles are involved?*

**Click here to type text.**

## [ ]  [ ]  Objectives of the security plan

*Provide a list of the different malicious acts that you want to prevent with this security plan (theft of radioactive material, intentionally causing radiological consequences, …) .* **Click here to type text.**

## [ ]  [ ]  Name of the HSP and the version

*Give the HSP a name (e.g. ‘HSP A’) and specify the version (e.g. ‘Rev. 0’). Also mention this information in the footer.*
**Click here to type text.**

# Responsibilities with regard to security

## Identification of the security coordinator

### [ ]  [ ]  Surname, Name

 **Click here to type text.**

### [ ]  [ ]  Telephone numbers, fixed and mobile

**Click here to type text.**

### [ ]  [ ]  Email address

 **Click here to type text.**

### [ ]  [ ]  Address

**Click here to type text.**

### [ ]  [ ]  Hierarchical position within the company (organigram)

*This information should allow to determine the hierarchical position of this person within the organisation.* **Click here to type text.**

### [ ]  [ ]  Qualifications

*This information should allow to evaluate the expertise and the training of the person involved.* **Click here to type text.**

## Identification of the back-up

## ☐ ☐ Surname, Name

**Click here to type text.**

## ☐ ☐ Telephone numbers, fixed and mobile

**Click here to type text.**

## [ ]  [ ]  Email address

**Click here to type text.**

### [ ]  [ ]  Address

**Click here to type text.**

### [ ]  [ ]  Hierarchical position within the company (organigram)

*This information should allow to determine the hierarchical position of this person within the organisation.***Click here to type text.**

### [ ]  [ ]  Qualifications

*This information should allow to evaluate the expertise and the training of the person involved.*
**Click here to type text.**

# Materials to be handled

##  [ ]  [ ]  Description of the radionuclides

*Specify for frequently handled transports what radioactive materials are involved and give as many details as possible about the radionuclides, the activity, the packaging, etc…***Click here to type text.**

# Evaluation of the usual operations during the handling and the corresponding risks

## Evaluation of the risks

### [ ]  [ ]  Short description of the evaluation method used

*Describe briefly how the risks have been evaluated. If a specific method has been used, please specify.*
**Click here to type text.**

### [ ]  [ ]  Risk analysis for each type of handling and situation

*Here it is sufficient to mention the risk analysis results of the situations that were retained under section 1.3.*
**Click here to type text.**

# Measures

## [ ]  [ ]  Management system

*The implementation of this HSP must be incorporated in a management system.*

*If this is the case, please mention it. Please also mention if the management system was submitted to the FANC (Import and Transport Service), and on which date.*

*If the management system has not been submitted to the FANC (Import and Transport Service), please briefly describe it.*

*If the implementation of this HSP is not incorporated in a management system, please also mention this.*

## Personnel

## 5.2.1 [ ]  [ ]  Training

*Describe how the training courses relating to security are organised.*
**Click here to type text.**

## 5.2.2 [ ]  [ ]  Trustworthiness and access rights of persons

*Describe how the trustworthiness of persons is guaranteed and what the relation is to their access rights.* **Click here to type text.**

## Access management (information, vehicles, zones, material)

### [ ]  [ ]  Access control

*Describe the means that have been installed to protect potential targets against maliciously intended manipulation.*
**Click here to type text.**

### [ ]  [ ]  Access rights

*Describe how access rights are granted, applied and withdrawn.*
**Click here to type text.**

### [ ]  [ ]  Management of the access tools (keys, badges, codes, …)

*Describe the management and the protection of these access tools.***Click here to type text.**

## Equipment management

### [ ]  [ ]  Maintenance of the security equipment

*Describe how the maintenance of the security systems is organised.*
**Click here to type text.**

### [ ]  [ ]  Tests

*Describe how the security systems tests are organised.***Click here to type text.**

### [ ]  [ ]  Compensatory measures

*Describe the compensatory measures that are foreseen in case the security systems are no longer working properly.***Click here to type text.**

## [ ]  [ ]  Cooperation with the authorities (Police, …)

*Describe what is foreseen with regard to the cooperation with the authorities if incidents with malicious intent should occur.*
**Click here to type text.**

## Punctual threat

### [ ]  [ ]  Information channels

*Describe the information channels that enable the company to follow the evolution of the punctual threat****.*Click here to type text.**

### [ ]  [ ]  Punctual threat

*Describe the measures taken as a function of the threat level.*
**Click here to type text.**

## Management of the usual operations and situations (cf. section 4)

### [ ]  [ ]  Management and supervision

*Describe how and by whom the management and the supervision of the transports are ensured.*
**Click here to type text.**

### [ ]  [ ]  Tracking

*Describe the tracking system.*
 **Click here to type text.**

### [ ]  [ ]  Interfaces with the parties involved

*Describe how the continuity of the security remains guaranteed between the different parties (carriers, multimodal organisations, senders and recipients). The transfer of the security responsibility must be treated and documented.*
 **Click here to type text.**

### [ ]  [ ]  Detection

*Specify for each of the steps described under 1.3 how detection is guaranteed.*

**Click here to type text.**

### ☐ ☐ Delay

*Specify for each of the steps described under 1.3 how delay is maximised.*

 **Klik hier om tekst te typen.**

### ☐ ☐ Response

*Specify for each of the steps described under 1.3 how response is initiated.*

 **Klik hier om tekst te typen.**

# Notification of security incidents and possible interventions.

## [ ]  [ ]  Notification of threat, security breaches or related incidents

*Describe how the notification of this type of incidents is organised within the organisation and towards the relevant authorities.***Click here to type text.**

## [ ]  [ ]  Actions taken in case of malicious acts

*Describe what measures are taken on organisation level in order to respond to malicious acts without delay.***Click here to type text.**

# Security plans

## Evaluation

### [ ]  [ ]  Exercises

*Describe how the exercises related to the HSP are organised.*
**Click here to type text.**

### [ ]  [ ]  General evaluation

*Describe the general evaluation of the HSP.*
**Click here to type text.**

## [ ]  [ ]  Revision and updating

*Description of this process.*
**Click here to type text.**

# Information

## [ ]  [ ]  Physical protection

*Describe the physical protection measures that guarantee the protection of the sensible information (i.a. HSP).***Click here to type text.**

## [ ]  [ ]  Dissemination of information

*Describe the measures that guarantee that information is disseminated only to the persons authorised and in need of this information.***Click here to type text.**

# [ ]  [ ]  Additional information provided by the carrier

*In this section the carrier can provide, if necessary, additional information/comments that could not be mentioned in the other sections.*

**Click here to type text.**

# [ ]  [ ]  Attachments

*List of the attachments added to the HSP.*
**Click here to type text.**

# [ ]  [ ]  Signatures

*The HSP must be signed by the person mandated to represent the company, the security coordinator and his/her back-up.*
**Click here to type text.**

\*\*\*