**Handling Security Plan (HSP)**

**Rev. 1 (20190924)**

**Naam van de onderneming/organisatie: Klik hier om tekst te typen**

**Identificatie/benaming van het HSP: Klik hier om tekst te typen**

**De versie van het HSP: Klik hier om tekst te typen**

**Graad van vertrouwelijkheid en bescherming van het HSP: Klik hier om tekst te typen**

**Datum van goedkeuring van het HSP door het FANC: Klik hier om tekst te typen**

**Datum vanaf wanneer het HSP van toepassing is: Klik hier om tekst te typen**

**Datum vanaf wanneer deze versie van het HSP niet meer gebruikt kan worden: Klik hier om tekst te typen**



Inhoud

[Voorafgaande opmerkingen door het FANC 5](#_Toc16497980)

[1. Algemeen 6](#_Toc16497981)

[1.1. Coördinaten van de onderneming 6](#_Toc16497982)

[1.1.1. ☐ ☐ Naam van de natuurlijke of rechtspersoon 6](#_Toc16497983)

[1.1.2. Adres van de onderneming 6](#_Toc16497984)

[*1.1.2.1* ☐ ☐ *Hoofdzetel* 6](#_Toc16497985)

[*1.1.2.2* ☐ ☐ *Exploitatiezetel* 6](#_Toc16497986)

[1.2. Korte beschrijving van de bedrijfsactiviteiten 6](#_Toc16497987)

[1.2.1. ☐ ☐ Algemeen 6](#_Toc16497988)

[1.2.2. ☐ ☐ De transporten 6](#_Toc16497989)

[1.3. ☐ ☐ Typische stappen tijdens de handling 6](#_Toc16497990)

[1.4. ☐ ☐ Objectieven/doelstellingen van het beveiligingsplan 7](#_Toc16497991)

[1.5. ☐ ☐ Benaming van het HSP en de versie 7](#_Toc16497992)

[2. Verantwoordelijkheden binnen de beveiliging 8](#_Toc16497993)

[2.1 Identificatie van de coördinator voor de beveiliging 8](#_Toc16497994)

[2.1.1. ☐ ☐ Naam, Voornaam 8](#_Toc16497995)

[2.1.2. ☐ ☐ Telefoon, vast en mobiel 8](#_Toc16497996)

[2.1.3. ☐ ☐ E-mail 8](#_Toc16497997)

[2.1.4. ☐ ☐ Adres 8](#_Toc16497998)

[2.1.5. ☐ ☐ Hiërarchische positie binnen de onderneming (organigram) 8](#_Toc16497999)

[2.1.6. ☐ ☐ Kwalificaties 8](#_Toc16498000)

[2.2 Identificatie van de plaatsvervanger 8](#_Toc16498001)

[2.2.1 ☐ ☐ Naam, Voornaam 8](#_Toc16498002)

[2.2.2 ☐ ☐ Telefoon, vast en mobiel 8](#_Toc16498003)

[2.2.3 ☐ ☐ E-mail 8](#_Toc16498004)

[2.2.4 ☐ ☐ Adres 8](#_Toc16498005)

[2.2.5 ☐ ☐ Hiërarchische positie binnen de onderneming (organigram) 8](#_Toc16498006)

[2.2.6 ☐ ☐ Kwalificaties 9](#_Toc16498007)

[3 Goederen die afgehandeld worden 10](#_Toc16498008)

[3.1 ☐ ☐ Beschrijving van de radionucliden 10](#_Toc16498009)

[4 Evaluatie van de gebruikelijke acties tijdens de handling en de bijhorende risico’s 11](#_Toc16498010)

[4.1 Evaluatie van de risico’s 11](#_Toc16498011)

[4.1.1 ☐ ☐ Een korte omschrijving van de gebruikte evaluatiemethode 11](#_Toc16498012)

[4.1.2 ☐ ☐ Risicoanalyse voor elk type van handling en situatie 11](#_Toc16498013)

[5 Maatregelen 12](#_Toc16498014)

[5.1 ☐ ☐ Beheersysteem 12](#_Toc16498015)

[5.2 Personeel 12](#_Toc16498016)

[5.2.1 ☐ ☐ Opleidingen 12](#_Toc16498017)

[5.2.2 ☐ ☐ Trustworthiness (betrouwbaarheid) en toegangsrechten van personen 12](#_Toc16498018)

[5.3 Toegangsbeheer (informatie, voertuigen, zones, materialen) 12](#_Toc16498019)

[5.3.1 ☐ ☐ Toegangscontrole 12](#_Toc16498020)

[5.3.2 ☐ ☐ Toegangsrechten 12](#_Toc16498021)

[5.3.3 ☐ ☐ Beheer van toegangsmiddelen (sleutels, badges, codes, …) 12](#_Toc16498022)

[5.4 Beheer van de uitrustingen 12](#_Toc16498023)

[5.4.1 ☐ ☐ Onderhoud van veiligheidsuitrustingen 12](#_Toc16498024)

[5.4.2 ☐ ☐ Testen 13](#_Toc16498025)

[5.4.3 ☐ ☐ Compenserende maatregelen 13](#_Toc16498026)

[5.5 ☐ ☐ Samenwerking met de overheidsdiensten (Politie, …) 13](#_Toc16498027)

[5.6 Punctuele dreiging 13](#_Toc16498028)

[5.6.1 ☐ ☐ Informatiekanalen 13](#_Toc16498029)

[5.6.2 ☐ ☐ Punctuele dreiging 13](#_Toc16498030)

[5.7 Het beheer van gebruikelijke handelingen en situaties (cf. sectie 4) 13](#_Toc16498031)

[5.7.1 ☐ ☐ De leiding en toezicht 13](#_Toc16498032)

[5.7.2 ☐ ☐ Tracking 13](#_Toc16498033)

[5.7.3 ☐ ☐ Interfaces met de betrokken partijen 13](#_Toc16498034)

[5.7.4 ☐ ☐ Detectie 14](#_Toc16498035)

[5.7.5 ☐ ☐ Vertraging 14](#_Toc16498036)

[5.7.6 ☐ ☐ Respons 14](#_Toc16498037)

[6 Kennisgeving van beveiligingsincidenten en mogelijke interventies. 15](#_Toc16498038)

[6.1 ☐ ☐ Kennisgeving van bedreigingen, inbreuken op de beveiliging of hieraan verbonden incidenten 15](#_Toc16498039)

[6.2 ☐ ☐ Acties ondernomen bij handelingen met kwaadwillig opzet 15](#_Toc16498040)

[7 Beveiligingsplannen 16](#_Toc16498041)

[7.1 Evaluatie 16](#_Toc16498042)

[7.1.1 ☐ ☐ Oefeningen 16](#_Toc16498043)

[7.1.2 ☐ ☐ Algemene evaluatie 16](#_Toc16498044)

[7.2 ☐ ☐ Revisie en actualisering 16](#_Toc16498045)

[8 Informatie 17](#_Toc16498046)

[8.1 ☐ ☐ Fysieke beveiliging 17](#_Toc16498047)

[8.2 ☐ ☐ Verspreiding 17](#_Toc16498048)

[9 ☐ ☐ Bijkomende informatie die door de handler werd aangeleverd 18](#_Toc16498049)

[10 ☐ ☐ Bijlagen 19](#_Toc16498050)

[11 ☐ ☐ Handtekeningen 20](#_Toc16498051)

# Voorafgaande opmerkingen door het FANC

1. Dit formulier is van toepassing op alle handlers die in het kader van de modale reglementen (bv. het ADR, cf. paragraaf 1.10.3.2.) een HSP moeten ontwikkelen.
2. Alle velden die voorzien zijn, moeten door de handler worden ingevuld.
   1. Indien de handler van mening is dat een bepaalde vraag niet op hen van toepassing is, kan hij/zij dit verantwoorden in het bijhorende tekstveld.
   2. Indien de handler van mening is dat de gevraagde informatie beter in een bijlage kan aangeleverd worden, kan hij/zij verwijzen naar deze bijlage. Indien nodig, gelieve specifiek te verwijzen naar waar deze informatie in de bijlage staat.
   3. Indien het FANC reeds beschikt over de gevraagde informatie, gelieve dan aan te geven waar we deze informatie kunnen terugvinden.
3. Opgepast met de informatie in het beveiligingsplan: neem de nodige maatregelen om de vertrouwelijkheid ervan te waarborgen.
4. De twee vakjes die voor elke titel staan, zijn bestemd voor de evaluatie van het HSP door het FANC.
5. De informatie in het HSP moet gericht zijn op beveiliging (security), m.a.w. de preventie van handelingen met kwaadwillig opzet. Maatregelen in het kader van management, stralingsbescherming of veiligheid (safety) mogen uiteraard vermeld worden, indien zij bijdragen – zelfs indirect – tot de beveiligingsdoelstellingen.
6. Indien de handler een beveiligingsplan heeft opgesteld volgens een andere reglementering, kan hij/zij dit vermelden onder sectie ‘9. Bijkomende informatie die door de vervoerder werd aangeleverd’. Indien de vervoerder wil verwijzen naar dat beveiligingsplan om bepaalde secties van het HSP in te vullen, moet hij dat doen zoals beschreven onder punt 2) hierboven en het beveiligingsplan in bijlage toevoegen (cf. Sectie ’10. Bijlagen’).

# Algemeen

## Coördinaten van de onderneming

## Naam van de natuurlijke of rechtspersoon

*Vermeld eveneens, naargelang het geval, het nummer van de Kruispuntbank van Ondernemingen (KBO) of het Rijksregisternummer (RRN).*

**Klik hier om tekst te typen.**

## Adres van de onderneming

## Hoofdzetel

**Klik hier om tekst te typen.**

## Exploitatiezetel

**Klik hier om tekst te typen.**

## Korte beschrijving van de bedrijfsactiviteiten

*Korte beschrijving van de bedrijfsactiviteiten om het kader waarin het HSP werd opgesteld, te kunnen duiden.*

### Algemeen

**Klik hier om tekst te typen.**

### De transporten

**Klik hier om tekst te typen.**

## Typische stappen tijdens de handling

*Beschrijf de verschillende stappen van een typische handling. Vb.:*

* *Lossen aankomend voertuig*
  + *Waar gebeurt dit? Om welk type voertuigen gaat het?*
* *Tijdelijke opslag buiten beveiligde locatie*
  + *Wat zijn de plaatsen waar de radioactieve bronnen worden neergezet voor deze naar een beveiligde locatie gaan? Hoe lang duurt dit doorgaans? Hoe worden de bronnen verplaatst?*
* *Tijdelijke opslag binnen beveiligde locatie*
  + *Waar worden de bronnen opgeslagen? Hoe lang duurt dit doorgaans?*
* *Tijdelijke opslag buiten beveiligde locatie (klaarzetten voor vertrek)*
  + *Waar gebeurt dit? Hoe lang?*
* *Laden vertrekkend voertuig*
  + *Waar gebeurt dit? Om welk type voertuigen gaat het?*

**Klik hier om tekst te typen.**

## Objectieven/doelstellingen van het beveiligingsplan *Lijst de verschillende kwaadwillige handelingen op die men in het beveiligingsplan wil voorkomen (diefstal van radioactieve materialen, opzettelijk radiologische gevolgen willen veroorzaken, …) .*

**Klik hier om tekst te typen.**

## Benaming van het HSP en de versie

*Geef een naam aan het HSP (Vb. ‘HSP A’) en geef aan over welke versie het gaat (Vb. ‘Rev. 0’). Herneem deze informatie als voetnoot.*

**Klik hier om tekst te typen.**

# Verantwoordelijkheden binnen de beveiliging

## Identificatie van de coördinator voor de beveiliging

### Naam, Voornaam

**Klik hier om tekst te typen.**

### Telefoon, vast en mobiel

**Klik hier om tekst te typen.**

### E-mail

**Klik hier om tekst te typen.**

### Adres

**Klik hier om tekst te typen.**

### Hiërarchische positie binnen de onderneming (organigram)

*Deze informatie moet toelaten de hiërarchische positie van deze persoon binnen de organisatie te bepalen.*

**Klik hier om tekst te typen.**

### Kwalificaties

*Deze informatie moet het mogelijk maken de ervaring en gevolgde opleiding(en) van de betrokken persoon te evalueren.*

**Klik hier om tekst te typen.**

## Identificatie van de plaatsvervanger

## ☐ ☐ Naam, Voornaam

**Klik hier om tekst te typen.**

## ☐ ☐ Telefoon, vast en mobiel

**Klik hier om tekst te typen.**

## E-mail

**Klik hier om tekst te typen.**

### Adres

**Klik hier om tekst te typen.**

### Hiërarchische positie binnen de onderneming (organigram)

*Deze informatie moet toelaten de hiërarchische positie van deze persoon binnen de organisatie te bepalen.***Klik hier om tekst te typen.**

### Kwalificaties

*Deze informatie moet het mogelijk maken de ervaring en gevolgde opleiding(en) van de betrokken persoon te evalueren.*   
**Klik hier om tekst te typen.**

# Goederen die afgehandeld worden

## Beschrijving van de radionucliden

*Voor frequent afgehandelde transporten, beschrijf om welke radioactieve materialen het gaat en geef zo veel mogelijk details over radionuclide, activiteit, verpakking enz.*

**Klik hier om tekst te typen.**

# Evaluatie van de gebruikelijke acties tijdens de handling en de bijhorende risico’s

* 1. **Evaluatie van de risico’s**

* + 1. Een korte omschrijving van de gebruikte evaluatiemethode

*Beschrijf bondig op welke wijze de risico’s werden geëvalueerd. Indien er gebruik werd gemaakt van een specifieke methode, gelieve deze te vermelden.*   
**Klik hier om tekst te typen.**

* + 1. Risicoanalyse voor elk type van handling en situatie

*Het volstaat hier om enkel de resultaten van de risicoanalyse weer te geven van de situaties die weerhouden werden onder sectie 1.3*.  
**Klik hier om tekst te typen.**

# Maatregelen

## Beheersysteem

*De implementatie van dit HSP moet opgenomen zijn in een beheersysteem.*

*Indien dit het geval is, gelieve dit te vermelden. Gelieve eveneens te vermelden of dit beheersysteem aan het FANC (Dienst Invoer en Transport) werd voorgelegd, en op welke datum.*

*Indien dit systeem niet aan het FANC (Dienst Invoer en Transport) werd voorgelegd, gelieve het bondig te beschrijven.*

*Indien de implementatie van dit HSP niet werd opgenomen in een beheerssysteem, gelieve dit te vermelden.*

## Personeel

## 5.2.1 Opleidingen

*Beschrijf hoe de opleidingen met betrekking tot de beveiliging worden georganiseerd.*   
**Klik hier om tekst te typen.**

## 5.2.2 Trustworthiness (betrouwbaarheid) en toegangsrechten van personen

*Beschrijf hoe de trustworthiness van de personen wordt gegarandeerd en wat de relatie is met hun toegangsrechten.***Klik hier om tekst te typen.**

## Toegangsbeheer (informatie, voertuigen, zones, materialen)

### Toegangscontrole

*Beschrijf de middelen die geïnstalleerd werden om mogelijke doelwitten te beschermen tegen manipulatie met kwaadwillig opzet.*   
**Klik hier om tekst te typen.**

### Toegangsrechten

*Beschrijf op welke wijze toegangsrechten worden toegekend, toegepast en ingetrokken.*  
**Klik hier om tekst te typen.**

### Beheer van toegangsmiddelen (sleutels, badges, codes, …)

*Beschrijf hoe het beheer en de bescherming van deze toegangsmiddelen gebeurt.***Klik hier om tekst te typen.**

## Beheer van de uitrustingen

### Onderhoud van veiligheidsuitrustingen

*Beschrijf hoe het onderhoud van beveiligingssystemen gebeurt.*  
**Klik hier om tekst te typen.**

### Testen

*Beschrijf hoe de testen van de veiligheidssystemen worden georganiseerd.***Klik hier om tekst te typen.**

### Compenserende maatregelen

*Beschrijf de compenserende maatregelen die voorzien zijn indien veiligheidssystemen niet meer naar behoren werken.***Klik hier om tekst te typen.**

## Samenwerking met de overheidsdiensten (Politie, …)

*Beschrijf wat er voorzien is in de samenwerking met de overheidsdiensten indien er zich incidenten met kwaadwillig opzet voordoen.*   
**Klik hier om tekst te typen.**

## Punctuele dreiging

### Informatiekanalen

*Beschrijf de informatiekanalen die de onderneming in staat stellen om de evolutie in de punctuele dreiging te kunnen opvolgen****.*Klik hier om tekst te typen.**

### Punctuele dreiging

*Beschrijf de maatregelen die genomen worden in functie van het dreigingsniveau.*   
**Klik hier om tekst te typen.**

## Het beheer van gebruikelijke handelingen en situaties (cf. sectie 4)

### De leiding en toezicht

*Beschrijf hoe en door wie de leiding en het toezicht op de transporten worden verzekerd.*   
**Klik hier om tekst te typen.**

### Tracking

*Beschrijf hoe de tracking gebeurt.*  
 **Klik hier om tekst te typen.**

### Interfaces met de betrokken partijen

*Beschrijf hoe de continuïteit van de beveiliging gegarandeerd blijft tussen de verschillende partijen (vervoerders, multimodale organisaties, afzenders en bestemmelingen). De overdracht van de beveiligingsverantwoordelijkheid moet worden behandeld en gedocumenteerd.*   
 **Klik hier om tekst te typen.**

### Detectie

*Gelieve voor elk van de fases beschreven in 1.3 aan te geven hoe detectie wordt verzekerd.* **Klik hier om tekst te typen.**

### ☐ ☐ Vertraging

*Gelieve voor elk van de fases beschreven in 1.3 aan te geven hoe vertraging wordt gemaximaliseerd.*

**Klik hier om tekst te typen.**

### ☐ ☐ Respons

*Gelieve voor elk van de fases beschreven in 1.3 aan te geven hoe respons wordt geïnitieerd.*

**Klik hier om tekst te typen.**

# Kennisgeving van beveiligingsincidenten en mogelijke interventies.

## Kennisgeving van bedreigingen, inbreuken op de beveiliging of hieraan verbonden incidenten

*Beschrijf hoe de kennisgeving van dit type incidenten gebeurt binnen de organisatie en naar de betrokken autoriteiten.***Klik hier om tekst te typen.**

## Acties ondernomen bij handelingen met kwaadwillig opzet

*Beschrijf welke maatregelen op niveau van de organisatie genomen worden zodat handelingen met kwaadwillig opzet onverwijld beantwoord worden.***Klik hier om tekst te typen.**

# Beveiligingsplannen

## Evaluatie

### Oefeningen

*Beschrijf de organisatie van de oefeningen die betrekking hebben op het HSP.*   
**Klik hier om tekst te typen.**

### Algemene evaluatie

*Beschrijf hoe de algemene evaluatie van het HSP gebeurt.*   
**Klik hier om tekst te typen.**

## Revisie en actualisering

*Beschrijving van dit proces.*   
**Klik hier om tekst te typen.**

# Informatie

## Fysieke beveiliging

*Beschrijf de fysieke beveiligingsmaatregelen die de garantie geven de gevoelige informatie te beschermen (ia HSP).***Klik hier om tekst te typen.**

## Verspreiding

*Beschrijf de maatregelen die de verspreiding van informatie enkel toelaat aan de personen die gemachtigd zijn en nood hebben aan deze informatie.***Klik hier om tekst te typen.**

# Bijkomende informatie die door de handler werd aangeleverd

*Onder deze sectie kan de handler, indien nodig, bijkomende informatie/opmerkingen plaatsen die niet kon vermeld worden onder de andere hoofdstukken.*

**Klik hier om tekst te typen.**

# Bijlagen

*Lijst van de bijlagen die aan het HSP werden toegevoegd.*   
**Klik hier om tekst te typen.**

# Handtekeningen

*Het HSP moet ondertekend worden door de persoon die het mandaat heeft de onderneming te vertegenwoordigen, de coördinator voor de beveiliging en zijn plaatsvervanger .*   
**Klik hier om tekst te typen.**

\*\*\*