# Radiation Protection Authority

# Zambia

# SAFETY GUIDE

## RPA SG 8

## Physical Protection of Radioactive Materials

2023

## NOTICE OF APPROVAL

Under the terms of Part II of the Ionising Radiation Protection Act No. 16 of 2005 and Part V of the Statutory Instrument No.98 of 2011, the Radiation Protection Authority (RPA) is authorized to establish or adopt standards of safety for protection of health and minimization of risk to life and the environment, and to provide for the application of these standards.

The Radiation Protection Authority Board (RPAB), has on the 19th December 2023 approved the safety guide on the safety and security of radioactive sources in medical exposure. This guide is approved for the purposes of providing practical guidance with respect to the Ionizing Radiation Protection General Regulations No. 98 of 2011.

This guide comes into effect on 19th December 2023

Brid. Gen. Dr. Major. Adrian Maleya

.....

CHAIRPERSON

Radiation Protection Authority Board

Dr. Boster Dearson Siwila PhD

.....

EXECUTIVE DIRECTOR

Radiation Protection Authority

## FOREWORD

Radiation Protection Authority (RPA) was established by the Ionising Radiation Protection Act No. 16 of 2005. It is a national regulatory body which implements the policies of the Zambian government relating to the protection of the public, workers and the environment from harmful effects of ionising radiation.

The risk of theft of radioactive materials and other associated activities has been demonstrated by the number of cases recorded in the incident and trafficking database (ITDB). Zambia has not been an exception to this risk as has been observed from the recorded cases of theft of radioactive materials. This safety guide was developed to assist licensees to follow systematic procedures, which will facilitate an effective implementation of the provisions of the radiation protection regulations. It also establishes minimum physical protection requirements for the protection of radioactive materials during storage, use and transport from theft and other unauthorized acts.

Preparation of this guide was carried out using guidance provided in the International Atomic Energy Agency Nuclear Security Series No. 11 "Security of Radioactive Materials" and International Atomic Energy Agency Nuclear Security Series No. 09 "Security of Radioactive Material in Transport."

## PREFACE

Radiation Protection Authority (RPA) was established by the Ionising Radiation Protection Act No. 16 of 2005. The structure of the implementation of the protection and safety was established to be compatible with the International Basic Safety Standards.

The structure was commensurate with the number and density and complexity of application and anticipated introduction of practices and sources within practices.

The essential element of the structured approach consisted of the following hierarchy:

- **Legislation** which established the Radiation Protection Authority and its powers and functions;
- **Radiation Safety Regulations** which prescribed the standards for radiation safety, waste safety and transport safety.
- **Radiation Protection and Safety Guides** which provides guidance for regulators, registrant and licensees and all stake holders to comply with the regulation as required by statutory instrument No. 98 of 2011(The ionising radiation (general) regulations, 2011).

The present radiation protection and safety guide seeks consistency with the IAEA International Atomic Energy Agency Nuclear Security Series No. 11 "Security of Radioactive Materials" and International Atomic Energy Agency Nuclear Security Series No. 09 "Security of Radioactive Material in Transport.".

**LIST OF ACRONYMS.**

| | |
|---|---|
| **RPAB** | Radiation Protection Authority Board |
| **PPS** | Physical Protection System |
| **TCC** | Transport Control Center |
| **IAEA** | International Atomic Energy Agency |
| **RPA** | Radiation Protection Authority |
| **ITDB** | Incident and Trafficking Database |

**Table of Contents**

## 1.0: INTRODUCTION

### 1.1 Background

(1) The threat of nuclear terrorism has been recognized as a matter of grave concern worldwide. States also recognize that nuclear security in one State might depend on the effectiveness of the *nuclear security regimes* in other States.

(2) A physical protection System which is defined as an integrated set of *physical protection measures* intended to prevent the completion of a *malicious act* is required to protect radioactive materials from falling in the wrong hands.

(3) A security system shall be designed by the facility`s security professionals to deter adversaries from committing a malicious act or to minimize through detection, delay and response the likelihood of an adversary succeeding in completing such a malicious act.

(4) Such an act would consist of a sequence of actions by one or more adversaries (threat) to obtain access to a source (target) either in order to commit an act of sabotage or another malicious act, or in order to remove the source without authorization.

### 1.2 Purpose

The purpose of the safety guide is giving the minimum physical protection requirements for radioactive materials in use, storage and in transit.

### 1.3 Scope

The document is divided in three main Parts. The first Section gives the general concepts in physical protection management. The second Section then covers physical protection requirements for radioactive materials classified under storage and during use. It sets out the requirements for radioactive materials under

category A, B and C. The third Section finally gives the physical protection requirements for radioactive materials during transportation.

## 2.0 SECURITY MANAGEMENT

### 2.1 Responsibility of the Licensee

The facility should

2.1.1 Develop, implement, test, periodically review and revise as necessary its security plan and comply with its provisions;

2.1.2 Cooperate and coordinate with the regulatory body and all other competent authorities having nuclear security responsibilities.

### 2.2 Security Plan

The facility should;

2.2.1 Prepare a security plan as part of its application to obtain authorisation for the material in use, storage or transportation, or of a facility;

2.2.2 Ensure that there is an approved security plan in place at all times for the use, storage and transport of the material, and for the facilities;

2.2.3 ensure that the security plan meets the nuclear security requirements;

2.2.4 The security plan should include, at a minimum, the topics included in Annex 1.

2.2.5 Implement the security plan upon approval and authorization by the Authority as part of the authorization conditions;

2.2.6 Review the security plan regularly to ensure it remains up to date with the current operating conditions and the nuclear security system;

2.2.7 Review the security plan every two years and submit it for prior approval to the Authority before making any modifications to the nuclear security system which should be reflected in the security plan.

## 2.3 Contingency Plan

As a part of its security plan, the facility should prepare a contingency plan to counter malicious acts effectively and to provide for appropriate response.

## 2.4 Integrated Management System

The facility should establish an integrated management system, including a quality assurance programme, which ensures that:

2.4.1 Nuclear security is given a high priority;

2.4.2 a threat assessment is conducted;

2.4.3 The nuclear security system is designed, implemented, operated and maintained in a condition capable of effectively protecting against the threats identified;

2.4.4 Assurance is given that the components of the nuclear security system are of high quality for their intended use;

2.4.5 Quality control mechanisms and procedures are established for reviewing and assessing the overall effectiveness of the nuclear security system;

2.4.6 Due priority is given to development and maintenance of a nuclear security culture

2.4.7 Clear lines of authority for decisions on nuclear security are defined;

2.4.8 Organizational arrangements and lines of communication are established that result in an appropriate flow of information on security at and between the various levels in the entire organization of the facility;

2.4.9 A manager having appropriate seniority, independent of facility operations, is designated as having overall responsibility for administering the nuclear security system;

2.4.10 Responsibilities for each individual with a nuclear security role are clearly identified and each individual is appropriately trained, qualified and adequately equipped;

2.4.11 There is adequate financial and human resource capacity to operate and maintain the nuclear security system; and

2.4.12 The nuclear security interface with safety, nuclear material accounting and control, radioactive material inventory control activities is managed in a manner such that these functions are mutually supportive and do not adversely affect each other.

## 2.5 Accounting and inventory

The Facility should:

2.5.1 maintain a record indicating the results of each periodic check required, including the date and time when the check was performed, the individual who performed the check, and the means used to verify the presence of radioactive material.

2.5.2 Report to the Authority and should assist as requested in efforts to locate and recover the radioactive material If the facility cannot verify the presence of radioactive material

2.5.3 Perform an annual inventory of radioactive material as of January and provide the results in writing to Authority.

2.5.4 Adjust the inventory upon transfer or receipt of radioactive material and provide the adjusted inventory to the Authority within 30 days of the transfer or receipt.

Individual radioactive material records should include the:

(a) location of the material;

(b) radionuclide;

(c) radioactivity on a specified date;

(d) serial number or unique identifier of the device in which the radioactive material is contained, if applicable;

(e) chemical and physical form;

(f) material use history, including recording all movements into and out of the licensee associated facility;

(g) receipt, transfer or disposal of the radioactive material;

(h) other information, as appropriate, to enable the radioactive material to be identifiable and traceable.

## 2.6 Training and Qualification

2.6.1 In order to ensure an effective operation of the nuclear security system the facility should provide initial training and refresher training annually in the area of nuclear security for the personnel.

2.6.2 The nuclear security training program should cover the following topics:

2.6.2.1 Objective of nuclear security;

2.6.2.2 Roles and responsibilities of the persons holding permanent access authorization to the site;

2.6.2.3 Security culture; and

2.6.2.4 Duties of the general staff in the case of a security event.

2.6.7 The facility should ensure that the personnel with responsibility for the nuclear security of material, facility or activity:

2.6.7.1 Are instructed in the security plan, including the contingency plan, as well as implementing procedures, their responsibilities, and the appropriate response to nuclear security events;

2.6.7.2 Receive training on security awareness that addresses the nature of security related threats.

2.6.8 The facility should routinely evaluate and as necessary update training programmes.

## 2.7 Protection of Information

2.7.1 The facility should

2.7.1.1 Identify sensitive information, the disclosure of which could compromise nuclear security;

2.7.1.2 Protect the sensitive information, in accordance with the provisions of State Security Act and the Zambia Information and Telecommunications Act, Cyber Security, Cyber Security and Cyber Crimes Act, 2021, Data Protection Act, 2021

2.7.2 Specific documents on radioactive sources should be controlled and distributed only to individuals authorised to know (need-to-know-basis).

2.7.3 This information should include:

2.7.3.1 Specific locations of the radioactive sources;

2.7.3.2 The facility security plan and contingency plans;

2.7.3.3 Vulnerabilities of the facility;

2.7.3.4 Radioactive source utilization log;

2.7.3.5 Transport security plan;

2.7.3.6 Proposed dates and times of shipment of radioactive sources.

## 2.8 Trustworthiness Verification

2.8.1 The facility should establish and implement a programme which will:

2.8.1.1 Implement measures to determine and periodically review the trustworthiness of authorized individuals with access to sensitive information and unescorted access to nuclear or other radioactive material; and

2.8.1.2 Follow a graded approach when implementing measures to determine and review trustworthiness.

2.8.2 The facility should ensure that persons whose trustworthiness has not been determined, such as temporary repair, service or construction workers for a limited period and visitors, should be escorted by persons with authorized unescorted access.

## 2.9 Nuclear Security Culture

2.9.1 The facility should develop appropriate management structures, allocate sufficient resources and put in place appropriate management systems ensuring personnel adopt a strict and prudent approach to, and to seek continuous improvement in, nuclear security;

2.9.2 The facility should provide

2.9.2.1 A commitment to quality of performance in all nuclear security activities;

2.9.2.2 A high priority to nuclear security, even overriding operational demands;

2.9.2.3 A clear process to resolve any conflict regarding the relative priorities of safety, security and operations;

2.9.3 The facility should communicate and make understood to everyone affected to give due priority to nuclear security culture

2.9.4 The facility should develop a self-assessment programme to assess the nuclear security culture in its organization as a basis for identifying ways to strengthen that culture.

## 2.10 Testing and Maintenance of Security Systems

2.10.1 The facility should establish a sustainability programme, develop and implement means and procedures for evaluations, including testing, and maintenance of the nuclear security system.

## 2.11 Reporting and Investigation of Nuclear Security Events

2.11.1 The facility should immediately inform the Authority in Annex 2 as provided in the regulations and law enforcement agencies in the case of the following nuclear security events:

2.11.1.1 Detection of an unauthorised removal or sabotage, or its attempt, within twenty-four hours;

2.11.1.2 Confirmed absence or accounting discrepancy in the amount of nuclear material and radioactive sources in use, storage or transport, promptly;

2.11.1.3. If storage containers or packages of nuclear material and radioactive sources have been tampered with, within twenty-four hours

2.11.1.4. Any malfunctioning of the nuclear security system, within 24 hours;

2.11.1.5 Any breach of the security of sensitive information, within 24 hours.

2.11.2 The facility should investigate the nuclear security event and its causes, circumstances and consequences, take appropriate action to remedy the circumstances and to prevent a recurrence of similar situations.

2.11.3 The facility should submit a report to the Authority about the results of the examination and the corrective actions.

## 2.12 Corrective Actions and Compensatory Measures

2.12.1 When the Authority (or the authorized person) determines that the nuclear security systems does not provide the required level of protection, Whenever the nuclear security system is determined to be incapable of providing the required level of protection, the licensee should immediately implement corrective actions and/or compensatory measures to provide adequate protection.

## 3.0 PHYSICAL PROTECTION MEASURES FOR MATERIALS IN USE AND STORAGE

### 3.1 Security System Design

3.1.1 The facility should design the nuclear security system to perform

3.1.1.1 Deterrence,

3.1.1.2 Detection,

3.1.1.3 Delay, and

3.1.1.4 Response

3.1.2 Nuclear security functions in an effective combination, in order to achieve the following requirements:

3.1.2.1 Ensure control of, and be able to account for all nuclear and other radioactive material used and stored under its authorisation;

3.1.2.2. Ensure that the nuclear security system provides adequate delay after the detection of a potentially malicious or otherwise unauthorized act and alerting the response forces to allow the response forces to interrupt malicious acts before the adversary successfully completes such an act or timely pursuit following unauthorised removal;

3.1.2.3 Ensure that the nuclear security system minimizes the chance of sabotage committed by an insider and to prevent unauthorized removal of material by an insider;

3.1.2.4. Ensure that nuclear security measures are integrated and effective against unauthorized removal and sabotage, and designed based on the more stringent applicable requirements

3.1.2.5. Ensure that the nuclear security system preserves its effectiveness under every weather condition, in every part of the day and in every phase of use, processing, storage;

3.1.2.6 Ensure that the detection and response function of the nuclear security system complies with the single failure criterion.

## 3.2 Interface with Safety

3.2.1 The facility should ensure that nuclear security interface with nuclear safety, radiation protection and nuclear material accountancy and control, and radioactive material inventory control activities is managed in a manner such that these functions are mutually supportive and do not adversely affect each other.

3.2.2 The facility should

3.2.2.1 Assess and address the safety and security interfaces in the design of its nuclear security system;

3.2.2.2 Ensure that consultation and coordination are established and maintained between those responsible for nuclear safety, nuclear material accountancy and control, radioactive material inventory control, radiation protection, management of crisis situations and working and operational conditions, in order to ensure that regulatory requirements are met in a mutually supporting way;

3.2.2.3 Ensure that the nuclear security system is operated effectively in cooperation with, and mutual support to the requirements for nuclear safety, nuclear material accountancy and control, radioactive material inventory control, radiation protection, management of crisis situations and nuclear and conventional emergency management;

3.2.3 The authorized person should ensure that the nuclear security system and its components are independent of the systems, structures and components

important to nuclear safety and radiation protection, in order to ensure that the safety critical systems, structures and components remain fully functional during the operation or failure of the nuclear security system;

3.2.4 The authorized person should ensure the safe operation during the modification of the nuclear security system in a way that

3.2.4.1 The systems, structures and components important to nuclear safety or radiation protection remain fully applicable to fulfil their functions during the implementation of the modification works; and

3.2.4.2 The persons working in nuclear safety or radiation protection related duties can perform their activity without being impeded;

3.2.5 The authorized person should ensure that the nuclear security system is assisted by nuclear material accountancy and control, and inventory control measures to deter and detect the unauthorised removal of material.

## 3.3 Requirements for Security Level A

3.3.1 Security goal

The facility should establish and implement a security system which should provide a high level of protection of radioactive material against unauthorized removal.

3.3.2. Detection

The facility should:

3.3.2.1 Provide immediate detection of unauthorized access to locations in which radioactive material is present and immediate detection of attempted unauthorized removal of

radioactive material, including by an insider, through the use of an electronic intrusion detection system and/or continuous surveillance by operator personnel.

3.3.2.2 Provide immediate assessment of detection through the use of remote video monitoring or direct observation by operator or response personnel.

3.3.2.3 Provide a means to detect loss through verification by daily checking through physical checks, video monitoring, and tamper indicating devices.

3.3.3. Delay

The Facility should furnish delay sufficient to provide a high level of protection against unauthorized removal of radioactive material through a system of at least two layers of barriers

3.3.4. Response

The facility should

3.3.4.1 Provide immediate communication to response personnel through rapid, dependable, diverse means of communication, such as phones, cell phones, radios; and

3.3.4.2 Provide for immediate response with sufficient resources to interrupt and defeat the adversary through arrangements with a designated response force including provision for sufficient personnel, equipment, and training, documented in a response plan.

## 3.4 Requirements for Security Level B

3.4.1. Security goal

The Facility should establish and implement a security system which should provide an intermediate level of protection of radioactive material against unauthorized removal.

3.4.2. Detection

The facility should:

3.4.2.1 Provide immediate detection of any unauthorized access to locations where radioactive material is present through the use of electronic intrusion detection systems and/or continuous surveillance by operator personnel.

3.4.2.2 Provide detection of attempted unauthorized removal of radioactive material through the use of tamper detection equipment and periodic checks by operator personnel.

3.4.2.3 Provide immediate assessment of detection through remote video monitoring and/or direct observation by operator or response personnel.

3.4.2.4 Provide a means to detect loss through verification and weekly checking through physical checks, tamper detection equipment.

3.4.3. Delay

The facility should furnish delay measures sufficient to provide an intermediate level of protection against unauthorized removal through a system of two layers of barriers

3.4.4. Response

The Facility should:

3.4.4.1 Provide immediate communication to response personnel through rapid, dependable means of communication, such as phones, cell phones, radios.

3.4.4.2 Provide immediate initiation of response to interrupt unauthorized removal through the use of equipment and procedures to immediately initiate response.

## 3.5 Requirements for Security Level B Portable Devices

3.5.1. Detection

The facility should:

3.5.1.1 Provide immediate detection of unauthorized access to locations where radioactive material is and detection of attempted unauthorized removal of radioactive material through visual or electronic observation by at least two operator personnel.

3.5.1.2 Provide immediate assessment of detection through observation by operator personnel.

3.5.1.3 Provide a means to detect loss through verification through daily checks after field use.

3.5.2. Delay

The facility should furnish delay measures to provide an intermediate level of protection against unauthorized removal by affixing the device to a stationary object if possible.

3.5.3. Response

The facility should:

3.5.3.1 Provide immediate communication to response personnel through at least two persons, each equipped with an independent mobile communication device.

3.5.3.2 Provide immediate initiation of response to interrupt unauthorized removal through advance notification to local response force, and communication after detection.

## 3.6 Requirements for Security Level C

3.6.1. Security goals

The Facility should establish and implement a security system which should provide a baseline level (Prudent Management Practice) of protection of radioactive material against unauthorized removal.

3.6.2. Detection

The facility should:

3.6.2.1 Provide detection of unauthorized removal of radioactive material through observation by operator personnel.

3.6.2.2 Provide a means to detect loss through verification through monthly checking by physical checks, tamper indicating equipment.

3.6.3. Delay

The facility should furnish delay sufficient to provide a baseline level of protection unauthorized removal through the use of one barrier or through the presence of operator personnel.

3.6.4. Response

The facility should:

3.6.4.1 Provide prompt communication to response personnel through rapid, dependable means of communication, such as phones, cell phones, radios; and

3.6.4.2 Implement appropriate action in the event of unauthorized removal of a radioactive material through procedures for identifying necessary actions in accordance with a response plan.

## 4.0 SECURITY DURING TRANSPORT OF RADIOACTIVE MATERIALS

4.1 Prudent Management Practices

4.1.1 The *Licensee is* responsible for:

4.1.1.1 Ensuring all employees who are involved with the transport hold verifiable documentation, including;

4.1.1.2 manifest (packaging list) with a schedule and an inventory of the packages,

4.1.1.3 licenses, certificates and operating documents where applicable; and

4.1.1.4 any necessary work permits.

4.1.1.5 Maintaining records associated with the custody and movement of the material (*e.g., Tracking packages by count and unique tamper seal as provided by the Authority*).

4.1.1.6 Providing crewmembers with photographic identification cards and developing procedures to positively verify and document identification of individuals from other organizations (i.e., carriers).

4.1.1.7 Establishing the reliability of employees who are involved in the transport.

4.1.1.8 Employing key control practices for both the vehicle locks and the cargo compartment locks.

4.1.1.9 Restricting access to only those persons that have a need to access the material;

4.1.1.10 Securing and storing the package while in transport (e.g., in a locked conveyance or storage area);

4.1.1.11 Utilizing carriers with package tracking systems (e.g., bar code system to monitor the status of the shipment), as appropriate;

4.1.1.12 Not using public transport for the transport of nuclear material or *radioactive material*;

4.1.1.13 Not leaving packages or conveyances unattended.

4.1.1.14 The driver must keep the vehicle and the cargo area locked at all times to prevent unlawful removal.

4.1.1.15 Use a closed vehicle for the conveyance of the material or an open vehicle with a closed cargo area.

4.1.1.16 Providing drivers of road conveyances with effective communication capability.

## 4.2 Security Measures for the Basic Security Level

4.2.1 General Requirements

4.2.1.1 The authorized person should ensure that radioactive material is only transferred to authorized persons.

4.1.2.2 The authorized person should ensure that:

a) the conveyance should be secured by locking the vehicle and cargo compartment;

b) areas within temporary storage terminals, temporary storage sites, vehicle depots, berthing areas and marshoulding yards used for the temporary storage during carriage of radioactive material should be properly secured, well-lit and, where possible and appropriate, not accessible to the general public.

c) security measures should be applied to the radioactive material consistent with the measures applied during use and storage.

d) Each member engaged in the transport of radioactive material members should carry with them means of identification, which includes their photograph, during carriage of radioactive material.

4.2.1.2 Facility should ensure that:

a) all persons engaged in the transport of radioactive material receive training, including training in the elements of security awareness;

b) Security awareness training should address the nature of security risks, recognising security risks, methods to address and reduce such risks and actions to be taken in the event of a security breach;

c) The content of the training has to be approved by the Authority;

d) Such training should be provided or verified upon employment and periodically supplemented with refreshing training;

e) Records of all security training received should be kept by the employer and made available to the employee or competent authority, upon request; and

f) Records should be kept by the employer for 5 years.

4.2.1.4 Facility should provide appropriate crew members with details of emergency contacts.

4.2.1.5 The Facility should ensure that the Shippers, carriers, and receivers cooperate with each other and with the appropriate authorities to exchange relevant information on applying security measures and responding to security incidents.

4.2.1.6 A facility should protect sensitive information relating to transport operations, such as information on the schedule and route, including dissemination only to persons with a need to know.

4.2.1.7 A facility should predetermine the trustworthiness of individuals involved during transport of radioactive material.

4.2.1.8 The facility should ensure that the receiver has procedures in place to verify package contents, which should include notifying the authorized person, shipper and carrier if radioactive material is

discovered to be missing or when a package has not been delivered by the expected time.

4.2.1.9 The facility should ensure that the shipper and carrier have procedures in place to respond to notification from the receiver. Through the course of the inquiry, if it is determined that the package or its contents have been lost, stolen or diverted, the authorized person should act to locate and recover the package or its contents and notify Authority as soon as practical.

4.2.1.10 The facility should perform security verifications of conveyances when the license is issued to verify that security measures associated with the conveyance are effective. Procedures should be established to ensure the security of keys to conveyances and locks. The integrity of the locks and seals should be verified before dispatch, before leaving any stopping point on the route and on arrival by staff specifically and previously authorized to undertake this verification.

4.2.1.11 Provide individuals engaged in the transport of radioactive material members with appropriate written procedures on required security measures, which should include information addressing how to respond to a security incident during transport.

### 4.2.2. Equipment-related elements

4.2.2.1 A facility should ensure the application of devices, equipment or other arrangements to deter, detect, delay and respond to theft, sabotage or other malicious acts affecting the conveyance or its cargo and should ensure that these systems are operational and effective at all times

4.2.2.2 The package in 4.2.3 (1) above should incorporate security seal which, while intact, demonstrate that the package has not been opened.

4.2.2.3 A facility should ensure that;

a) The package be carried in secure and closed or sheeted conveyances, compartments or freight containers unless there are overriding safety or operational considerations.

b) The Package be attached by tie-downs and the cargo doors of the conveyance remain locked whenever the packages are loaded on the conveyance.

c) Carriage of packages weighing more than 2000 kg that are locked, and secured to the conveyance, is appropriate for transport on open vehicles. Whenever it is necessary to use open conveyances, the load should be covered or hidden from view unless precluded by safety requirements.

4.2.2.5 During transport, facility should provide continuous, reliable mobile communication for the driver.

## 4.3 Security Measures for The Enhanced Security Level

4.3.1. Security management: General requirements

4.3.1.1 In addition to the requirements for Prudent Management Practices and for basic security level the following requirements apply to enhanced security level.

a) take measures based on need to know to protect sensitive information relating to transport operations, detailed information on the schedule and route including electronic systems and computer systems.

b) Apply a two-person rule to manage keys for the locks of the package (if applicable, e.g. if it is a source container) and freight container.

*c)* Ensure a vehicle with radioactive materials is never left unattended

d) When a stop cannot be avoided, the vehicle must be parked in well-lit and secure areas which are continuously under surveillance by *security guards.*

e) Provide the driver and other personnel with physical protection responsibilities for a particular shipment with written instructions including, location of authorized stops, operation of alarm systems and actions to be taken in case of theft of the vehicle.

f) Ensure that the consignee checks the integrity of the packages and locks and seals to verify that the security of the consignment has not been compromised and accepts the shipment and notifies the consignee immediately upon arrival.

g) Ensure that the receiver notifies the shipper of non-arrival within 30minutes after the estimated time of arrival at the destination.

h) Transport radioactive materials in such transport vehicle which exclusively transports the given material.

**4.3.2. Transport Security Plan**

4.3.2.1 Prior to commencing shipment or a series of similar shipments of radioactive material a licensee and other participants engaged in the carriage of radioactive material should adopt, implement and comply with a security plan.

4.3.2.2 The facility should submit a transport security plan for approval by Authority.

4.3.2.3 The transport security plan referred above should include at least the following elements:

a) Specific allocation of security responsibilities of organizations and persons engaged in the transport of radioactive material, with provision of appropriate authority to carry out their responsibilities;

b) Provisions for keeping records of radioactive material packages or types of radioactive material transported;

c) Provisions for review of current operations and vulnerability assessment, including intermodal transfer, in-transit storage, handling and distribution as appropriate;

d) Clear statements of security measures, including: training, policies including response to conditions of a higher-level threat, verification of new employees and employment, operating practices (e.g., choice and use of routes where known, use of guards, access to radioactive material packages requiring the enhanced transport security level in temporary storage, proximity to vulnerable infrastructure), equipment and resources that are to be used to reduce security related risks;

e) Effective procedures and equipment for timely reporting and dealing with security related threats, breaches of security or security related incidents (e.g., contingency plans);

f) Procedures for evaluating and testing security plans and procedures for periodic review and update of the plans;

g) Measures to protect sensitive information;

h) Measures to ensure that the distribution of sensitive transport information is limited, to maintain security of the information. Such measures should not preclude the provision of transport documents and shipper's declaration as required by the applicable dangerous goods regulations;

i) Measures to monitor the location of the shipment; and

j) Where appropriate, a facility should provide details concerning agreements on the point of transfer of responsibility for security.

4.3.2.5 A Facility should develop and implement a contingency plan which should be incorporated into the transport security plan to ensure adequate response to malicious acts.

4.3.2.6 A facility should conduct exercises to assess and validate the transport security plan and to train the participants on how to respond to nuclear security events.

4.3.2.7 A facility should periodically review as necessary and comply with the provisions of a transport security plan.

4.3.2.8 The facility should modify the transport security plan as needed to reflect changes in the threat level.

4.3.2.9 In the event that any aspect of the transport is subcontracted, the facility should ensure that the subcontractor complies with the transport security plan or has other equivalent security measures in place.

### 4.3.2 Arrangements prior to shipment

4.3.3.1 Authorized person should ensure that the shipper/carrier gives the receiver, the authority and other relevant authorities advance notification of the planned shipment.

4.3.3.2 This notification should specify the mode of transport (road/rail/water/air), the estimated time of arrival of the shipment and the exact point of handover if this is to be done at some intermediate point before the ultimate destination.

4.3.3.3 This advance notification should be supplied in 48hrs sufficient time to enable the receiver to make adequate security arrangements.

4.3.3.4 The authorized person should ensure that prior agreements among shipper, receiver, and carrier specify the time, place and procedures for transferring security responsibilities.

4.3.3.5 Prior to the commencement of each shipment, the authorized person should ensure that the receiver has confirmed readiness to accept delivery (and handover, if applicable) at the expected time.

4.3.3.6 The authorized person should ensure that a pre-shipment security verification of the conveyance and security systems is conducted prior to commencing transport in order to ensure that the security measures are implemented as described in the transport security plan and are functioning normally.

4.3.3.7 Immediately prior to loading and shipment, and after any intermodal transfer, the authorized person should ensure that a search of the conveyance is conducted to verify that the security of the consignment has not been compromised.

4.3.3.8 Immediately following completion of the search, the conveyance should be placed in a secure area or kept under guard surveillance pending its loading and shipment for transport and unloading.

4.3.3.9 Prior to commencement of transport, the authorized person should receive confirmation of the receiver of the ability and readiness to accept delivery at the expected time.

4.3.4. Route selection

A facility should

4.3.4.1 plan in advance an alternative route in addition to the primary routes which all should be identified in the transport security plan.

4.3.4.2 provide the exact description of the movements within the city together with how the transport should avoid peak traffic hours and avoid densely populated areas.

4.3.4.3 Pay special attention to each evident source of danger, like civil demonstrations and natural sources of dangers (i.e., flood, fire, stone fall) when selecting the transport route.

4.3.4.4 Verify prior to the transport the availability and security related characteristics of the selected route.

4.3.5 Transport schedule

4.3.5.1 The transport time, namely the duration spent by the vehicle on the road and the mode of transport should be determined as follows:

4.3.5.2 the number of vehicles and re-loading should be minimized, the regularity should be avoided in scheduling of vehicles;

4.3.5.3 If the transport takes more than one day, then

4.3.5.4 The transport should be arranged without stops by more drivers to be changed; and

4.3.5.5 a guarded and monitored night-time stop meeting the security requirements should be arranged in advance,

4.3.5.6 No stop should take more than 24 hours.

4.3.5.7 Arrangements should be made with the police service or other authorized persons along the route to ensure a secure area is available for temporary/emergency storage.

4.3.6 Authorisation of Shipment

4.3.6.1 The facility should obtain a transit license in line with section 21 of the Ionising Radiation Protections Act No. 16 of 2005.

4.3.6.2 The facility should obtain a further authorisation of each shipment 2 days prior to commencing transport and should be conditional on a current threat assessment and intelligence information.

4.3.6.3 When directed by the Authority based on the threat assessment or intelligence information, a facility should conduct a detailed route surveillance to observe the current environment.

4.3.6.4 The Facility should comply with all specific limitations and conditions related to the circumstances particular to the given shipment as specified by Authority.

4.3.7. Equipment-related elements

A facility should ensure that:

4.3.7.1 Appropriate security seals are used inside and outside the vehicle or container.

4.3.7.2 All openings to the vehicle should be installed with sensors capable of sending a signal to the driver and contact points specified in the transport security plan when an attempt of intrusion into the vehicle is detected.

4.3.7.3 The vehicle is fitted with a video surveillance system capable to monitor from the transport control center the load or the loading area at least when the loading area of the vehicle is opened and/or is in open position.

4.3.7.1 Load compartment should be fitted with cameras with a monitor in the driver's cabin.

4.3.7.1 The package is secured in the vehicle with quality locking mechanisms. These should include door locks, cargo area locks and locks securing the equipment to the vehicle, depending upon configuration.

4.3.7.2 The package is tied down to the vehicle bed using strong chains, nuts, bolts, ratcheting and related devices.

*4.3.7.3* The transport vehicle is fitted with an immobilisation system to control the vehicle in an attempt of forced vehicle theft which *should be self-arming and do not rely on the driver remembering to set it.*

4.3.7.4 Load compartment is isolated from the driver/passenger area.

4.3.7.5 Vehicles are fitted with radios or some other means of two-way communications between the driver and contact points specified in the transport security plan. Such systems should be redundant, diverse and secure.

4.3.7.6 During the transport, the security escort should establish regular communication with the driver of the vehicle, the shipper, the consignee, the local authorities and response forces concerned by the route of the transport until the consignment is received by the consignee.

4.3.7.7 A *Mobile or fixed* in cab duress alarms is provided for use by the driver in transit.

4.3.7.8 A comprehensive security information package is provided and use *tracking methods or devices* to monitor the movement of packages or conveyances containing *category 1* radioactive material.

4.3.7.9 All packages are tracked during transport to ensure that the status of the package can be determined at any time.

4.3.7.10 Guards accompany each shipment, including before and during loading and unloading operations. Guards should be appropriately equipped and trained.

4.3.7.11 Each transport vehicle is accompanied by two (2) escort vehicles, each carrying armed or unarmed guard force personnel.

4.3.7.12 Guards conduct surveillance of the route and to initiate an appropriate response. Continuous surveillance of the packages or locked cargo hold, or compartment holding the packages, should be maintained by the guards at all times, especially when the conveyance is not in motion.

A facility should provide Additional security measures for Industrial and well logging devices which will include:

4.3.7.13 Provision of tie down arrangements and installation of a high security locks to the radiography source transport container.

4.3.7.14 Separate transport container with facility to tie down the container to the vehicle and locking the container with a high security lock with shielded shackle to prevent cutting and removing the lock.

4.3.8 Transport Control Center (TCC)

The Facility, shipper and/or carrier should utilize a Transport Control Center (TCC) for the monitoring of transport of nuclear or other radioactive material.

(1) The Licensee, shipper and/or carrier should use a TCC for the purpose of

keeping track of the current location and security status of the shipment, alerting TCC in case of an attack and maintaining continuous secure two-way voice communication with the shipment and the TCC.

(2) The TCC should be protected in a manner approved by the Authority. While the shipment is in progress, TCC should be staffed by qualified personnel whose trustworthiness has been predetermined.

(3) The Licensee, shipper and/or carrier should ensure that the conveyance crew are instructed to report to the TCC every 15 minutes, at each overnight stopping place, at the place(s) of handover of the shipment, and upon arrival at the final destination.

4.3.9 Response Forces

The Licensee should decide to provide response forces commensurate with the threat to deal with nuclear security events by arriving in time to prevent unauthorized removal.

## 4.4 ADDITIONAL SECURITY MEASURES

4.4.1 A facility may be required by the Authority to provide additional security measures in addition to those in Part II and III in view of the threat or the nature of the material being transported.

4.4.2 If the current or potential threat warrants additional physical protection measures to protect against sabotage, the facility should identify and implement such measures, which can and may include:

4.4.2.1 Postponing the shipment,

4.4.2.2 rerouting the shipment to avoid high threat areas,

4.4.2.3 enhancing the robustness of the package or the conveyance, detailed route surveillance to observe the current environment, and/or

4.4.2.4 the provision of additional guards.

## 4.5 MODE SPECIFIC PROVISIONS

4.5.1 Provisions for road transport

4.5.1.1 The facility should maintain a continuous attendance of the road conveyance during transport where possible.

4.5.1.2 If a road movement cannot be completed without overnight or extended stops, then a facility should protect the radioactive material during such stops in a manner that duly protects the material against malicious acts, according to the comparable level of security for use and storage.

4.5.1.3 A facility should take security requirements for radioactive materials within a facility as a basis for defining security requirements during in-transit storage.

4.5.1.4 A facility should ensure that a transport vehicle driver is accompanied by one or two additional appropriately qualified and equipped personnel.

4.5.1.4 A facility should ensure Road vehicles transporting Category 1 quantities of radioactive material should be equipped with automatic and real time tracking capability that is monitored remotely or other tracking arrangements approved by Authority

**Annex 1: Security plan for Radioactive Materials in Use and Storage**

## 1. ADMINSTRATIVE INFORMATION

1.1. Introduction and schedule for implementation

1.2. Facility description

1.2.1. General facility description, mission and operations

1.2.2. Facility layout

1.3. Security policy

1.3.1. Management policy

1.3.2. Nuclear security culture

1.3.3. Quality assurance

1.3.4. Trustworthiness policy

1.3.5. Sustainability programme

1.4. Security organization

1.4.1. Security organization structure

1.4.2. Security management and allocation of responsibilities

1.4.3. Qualification requirements for security personnel

1.4.4. Security personnel training

1.4.5. Guards/response force armament and equipment

1.5. Information management

1.5.1. Computer security management

## 2. DEFINING PHYSICAL PROTECTION SYSTEM

2.1. Objectives and requirements of the PPS

2.2. Target identification

2.3. Threat definition

2.4. Law enforcement liaison

## 3. PHYSICAL PROTECTION SYSTEM

3.1. Facility protection strategies

3.2. Description of the PPS

3.2.1. Insider threat mitigation programme

3.3. Transport of Radioactive material

3.4. Physical Protection System testing, evaluation and maintenance

3.4.1. Types of testing and evaluation

3.4.2. Frequency of testing and evaluation

3.4.3. Maintenance

3.4.4. Expansion and upgrade

3.5. Compensatory measures

## 4. RESPONSE PLANNING

4.1. Organization and responsibilities

4.2. Security forces

4.2.1. Guards

4.2.2. On-site response force

4.2.3. Off-site response force

4.2.4. Central Alarm Station staffing

4.3. Contingency plans

4.4. Incident communications, command and control

4.5. Response to higher threat conditions

## 5. POLICIES AND OPERATIONAL PROCEDURES

5.1. Required elements of the security plan

5.2. Review, evaluation, audit and update of the security plan

## 5.3. Reporting of threats or incidents