PNRA-RG-926.01 February, 2021

FORMAT AND CONTENT OF PHYSICAL PROTECTION PLAN FOR RADIATION FACILITIES HAVING RADIOACTIVE SOURCES

REGULATORY GUIDE

PAKISTAN NUCLEAR REGULATORY AUTHORITY

For Further Details

Directorate of Policies and Procedures
PAKISTAN NUCLEAR REGULATORY AUTHORITY
P.O. Box 1912, Islamabad
www.pnra.org

TABLE OF CONTENTS

1. INTRODUCTION

The radioactive sources are widely used for beneficial purposes in industry, medicine, agriculture, research and education. Such diverse applications of radioactive sources demand an effective regulatory oversight to avoid loss, theft or sabotage of radioactive sources in order to reduce the risk of undue exposure to the radiation workers, general public and the environment.

Pakistan Nuclear Regulatory Authority (PNRA) has developed an effective regulatory framework for the safe and secure use of radioactive sources throughout their lifetime. Under the regulatory framework, the prime responsibility for safety and security of radioactive sources lies with the licensee.

PNRA is ensuring physical protection of radioactive sources through physical protection plan and regulatory oversight. "Regulations on Licensing of Radiation Facility(ies) other than Nuclear Installation(s) - (PAK/908) (Rev.1)" require submission of physical protection plan from applicant for issuance of license of radiation facilities having radioactive sources. Furthermore, Regulations 15(5), 19(1) and 20(1) of "Regulations on Security of Radioactive Sources - (PAK/926)" require the licensee to submit physical protection plan in accordance with the format and content as specified by the Authority for approval.

The physical protection plan is an important submission that describes the licensee's compliance to applicable regulatory requirements for the security of radioactive sources. This Regulatory Guide (RG) describes the standard format and content for the preparation of physical protection plan for radiation facilities having radioactive sources.

2. OBJECTIVE

This RG provides guidance to the applicant or licensee to prepare physical protection plan in accordance with the prescribed format and content.

3. SCOPE

This RG is applicable to radiation facilities and associated activities, having Category 1, 2 and 3 radioactive sources in manufacture, use, storage and transport, for development of physical protection plan.

Although, physical protection plan for Category 4 and 5 radioactive sources is not required by the Authority, however, licensee may develop physical protection plan for these sources as a good practice by using relevant sections of this RG.

4. GENERAL INSTRUCTIONS

Following are the general instructions, to be followed by the applicant or

licensee while formatting a physical protection plan:

i. The physical protection plan should be part of facility's overall management system;
ii. The physical protection plan should be prepared by authorized person in consultation with concerned security elements;
iii. It should provide clear, concise and up to date information;
iv. It should include a table of contents;
v. Definitions and abbreviations (if necessary) should be consistent throughout the document;
vi. Duplication of information should be avoided. In case where necessary, reference of relevant section should be made;
vii. Legible drawings, diagrams, maps, annexes and tables should be added wherever necessary with proper reference;
viii. The physical protection plan should be signed by authorized person and each page of the physical protection plan should contain a page number, a revision number (if applicable) and date; and
ix. The physical protection plan and related records should be protected against unauthorized disclosure.

5. FORMAT AND CONTENT OF PHYSICAL PROTECTION PLAN

The following sections and subsections describe the content and level of detail that should be included within the physical protection plan:

5.1 Introduction

The applicant or licensee should describe purpose of the facility, operations and nature of activities that involve radioactive sources. The applicant or licensee should also describe scope and objectives of its physical protection plan.

5.2 Facility Description

The applicant or licensee should address facility description that should include but not limited to the following:

i. Location (address);
ii. Relevant departments where the radioactive sources are either manufactured, used or stored including their details;
iii. Facility working hours; and
iv. Number of personnel visiting the facility (employees, general public, etc.).

5.3 Radioactive Source Description, Categorization and their Corresponding Security Levels

The applicant or licensee should provide details of radioactive sources such as radionuclide's reference activity (mentioned on source certificate), identification number of source, physical form, quantity, reference numbers of relevant No Objection Certificates (NOCs), etc., their location, application, corresponding category and applicable security levels based on criteria given at Annex I, in compliance with Schedule-I of "Regulations on Security of Radioactive Sources - (PAK/926)".

5.4 Map of the Secured Area

The applicant or licensee should provide map or layout of the secured area, locations of radioactive sources and associated entry & exit control points. The map or layout should show security measures, as appropriate, (e.g. fences, cages, locks, CCTV system, lights, intrusion detection and alarm system, tamper indicating devices, access control system), being taken by the facility for security of its radioactive sources. The details of security measures should be included separately as described below in section 5.8.

5.5 Organizational Structure and Responsibilities

The applicant or licensee should provide information about security department and its relationship with overall organizational structure of the facility. Security related responsibilities and clear lines of authorities of management, operating personnel and security personnel at the facility or during transport, as the case may be, should also be described as part of overall management system of the facility.

In case of transportation of radioactive sources, the licensee should provide details of designated contact person travelling with the vehicle and describe responsibilities of all the individuals involved in the transportation including transfer of responsibilities when a radioactive source is moved from origin to destination.

5.6 Trustworthiness of Personnel

The applicant or licensee should describe the ways to confirm the trustworthiness and reliability through background checks of all its personnel authorized for unescorted access to secured area and sensitive information. On the basis of background checks, the licensee should furnish character certificates that such personnel are deemed trustworthy and reliable. Licensee may attach such character certificates with its physical protection plan.

The licensee is responsible for assessing past and current character and reputation of operating and security personnel in order to provide reasonable assurance before allowing unescorted access to those personnel to radioactive source or any related

sensitive information. The licensee should perform trustworthiness and reliability verification during hiring process and update periodically for every three (3) years for personnel associated with radioactive sources. The scope of background checks should encompass at least three (3) years preceding the date of the trustworthiness verification.

The licensee should consider the following indicators in determining the integrity, character and reliability (through background checks) of its personnel having role in security of radioactive sources:

i. **Confirmation of Identity:** Confirm the true identity of personnel from original documentation (e.g. CNIC or passport);

ii. **Financial Record:** Confirm the financial record of personnel from reliable sources such as bank statement;

iii. **Criminal Record:** Confirm the criminal record of the personnel from the local police station;

iv. **Moral Conduct:** Confirm the moral conduct including illegal drug use, hostility towards fellow workers, etc. (e.g. medical records);

v. **Motivation:** Confirm the motivation of personnel from job performance including indication of deceitful or illegal behavior;

vi. **Verification of References:** Determine the character and reputation of personnel by obtaining independent information through individuals who know or previously knew the person; and

vii. **Employment History:** The personnel employment history for most recent three (3) years including records from each employer in which the person has worked for one or more years.

5.7 Protection of Sensitive Information and Computer System

The applicant or licensee should identify and classify sensitive information (both in hard and soft forms) and should describe the measures for its protection.

The applicant or licensee should also describe cyber security measures for computer systems important to safety and security.

Cyber security enables licensees to consider strategies to protect computer based systems, including communication systems and instrumentation and control systems that process, handle, store and transmit information that is directly or indirectly important to safety or security of radioactive sources. The licensee should consider cyber security for the following categories:

i. Digital devices that support the security of radioactive sources;

ii. Equipment (important to safety or security) with software-based control, operation, and automation features;

iii. Computers used to maintain source inventories, audit data, and records necessary for compliance with security requirements; and

iv. Digital technology used to support incident response communications and coordination.

For effective cyber security of computer and computer-based system, the licensee should ensure at least the following measures:

i. Restrict the number of personnel granted administrative rights or accounts on each computer;

ii. Beyond physical controls for protecting digital assets, take other types of controls, which may be technical (e.g. firewalls, account passwords, antivirus software) or administrative (e.g. policies, procedures, guidelines, trainings);

iii. Keep computers isolated from one another (no communications connectivity, or creation of an "isolated" Local Area Network (LAN));

iv. Disable wireless interfaces when they are not needed;

v. Disable all open and unused network ports;

vi. Develop password policy that defines how complex passwords need to be generated and how often or under what condition they need to be changed; and

vii. Use storage devices that are password protected or encrypted, and are only accessible to authorized users.

5.8 Security Measures

The applicant or licensee should include the description of security system designed (detection, delay and access control), installed and implemented in order to protect radioactive sources in accordance with regulatory requirements mentioned in "Regulations on Security of Radioactive Sources - (PAK/926)". The details should be described as per following subsections:

5.8.1 Detection

The applicant or licensee should describe detection measures taken as per following details:

i. The measures used to detect unauthorized access to secured area either by electronic intrusion detection system or operating personnel, as applicable;

ii. The measures used to detect unauthorized removal of radioactive sources either by electronic tamper detection device or operating

personnel, as applicable;

iii. The measures used for assessment of detection either through CCTV camera or operating or security personnel, as applicable;

iv. The measures for communication to response personnel such as telephone, cell phone, walkie-talkie, etc.;

v. The measures for physical verification of radioactive sources on periodic basis (such as fortnightly basis for Category 1 and 2 and monthly basis for Category 3) to ensure their presence. The measures for physical verification may include physical checks, remote video monitoring, verification of seals or other tamper indicating devices and radiation measurements at designated measurement points; and

vi. For mobile radioactive sources in use, continuous visual surveillance by operating personnel as a detection measure.

It may be noted that electronic intrusion detection system (e.g. passive infrared sensor, dual technology sensors, balanced magnetic switch, or any other motion detection sensors), electronic tamper detection device and CCTV system are mandatory for Category 1 radioactive sources as per "Regulations on Security of Radioactive Sources - (PAK/926)".

5.8.2 Delay

The applicant or licensee should describe delay measures such as walls, cages, robust doors, locks, etc. at secured area to increase adversary task time relative to facility response time.

It may be noted that at least two layers of delay barriers are mandatory for Category 1 and 2 radioactive sources.

5.8.3 Access Control

The applicant or licensee should describe access control measures for controlling access to secured area and source location. The measures should include identification and verification of authorized personnel such as key, card, personal identification number, biometric device or a combination.

Access controls should effectively restrict unescorted access to radioactive sources to authorized persons only. It may be noted that verification of the identity of authorized personnel is mandatory for Category 1 radioactive sources.

5.9 Response Arrangements Against Security Events

The applicant or licensee should identify all possible security events and

describe response capabilities to interrupt and neutralize the adversary. The security events may include at least the following:

i. Attempted or successful unauthorized removal or loss of radioactive sources;
ii. Attempted or actual sabotage;
iii. Unauthorized transfer or transport of radioactive sources;
iv. Unauthorized access to secured area;
v. Failure or loss of a security system or failure of multiple systems that are essential for the security of radioactive sources;
vi. Loss or unauthorized disclosure of sensitive information; and
vii. Other malicious acts related to radioactive source (such as theft/loss of keys or access control card, suspected tampering with security system, discovery of prohibited items, forceful stopover of transport vehicle, etc.).

In case of security event, the applicant or licensee should describe arrangements for coordination and liaison with relevant local law enforcement agencies such as police including coordination with other relevant national response organizations having their role in response to contingencies such as Strategic Plans Division (SPD), PNRA, National Disaster Management Authority (NDMA), Fire Brigade, Rescue 1122, Civil Defence, etc.

5.10 Security Event Reporting

For security events identified in section 5.9, the applicant or licensee should describe mechanism for notification and reporting security events to PNRA and information to local law enforcement agencies (such as Police). As a regulatory requirement, the licensee is bound to notify security event to PNRA within twenty four (24) hours. The format for security event notification is given at Annex II.

The applicant or licensee should also identify personnel with responsibilities for security event documentation and subsequent notification and reporting.

5.11 Safety and Security Interface

The applicant or licensee should address arrangements for establishing and maintaining an effective interface between safety and security in such a way that they are mutually supportive.

Safety and security measures should be designed in such a manner that safety measures do not compromise security and security measures do not compromise safety. Due weightage for safety should be ensured. Possible conflicts of safety and

security measures should be managed through compensatory and mitigating actions. Any proposed changes to either safety or security should be reviewed before they are implemented to ensure that changes do not result in the unintended degradation of arrangements in the other area.

Following are some examples of safety and security interface areas for which licensee may describe its arrangements:

i. Access control arrangements to ensure easy entry and exit in case of radiological emergencies while ensuring prevention of unauthorized access to secured areas;

ii. Radioactive sources inventory management after every use in the field and in case of transportation to prevent loss of radioactive source and undue radiation exposure;

iii. Consideration of the radiation protection program and emergency plan in the development of the physical protection plan in order to ensure compatibility and consistency;

iv. Developing and conducting regular integrated safety and security exercises to test coordination in associated plans and arrangements;

v. Consideration of safety and radiation protection requirements in designing security system (e.g. lead lined door vs. robust security door);

vi. Change, modification and maintenance management from both safety and security point of view to avoid intentional or unintentional radiation exposure;

vii. Security staff should have adequate knowledge of radiation protection, and similarly, safety staff should be familiar with those security measures so that the interfaces between safety and security are well understood and managed;

viii. Liaison between safety and security personal to ensure coordination and integration of physical protection plan with emergency plan;

ix. Dissemination of information at various management and staff levels for safety and security related activities to ensure transparency of information pertaining to safety issues while ensuring confidentiality of security-sensitive information; and

x. Establishing and maintaining the integration of safety and security cultures.

5.12 Training Program

The applicant or licensee should describe training and retraining program for its personnel having security related responsibilities.

5.13 Maintenance Program

The applicant or licensee should describe its arrangements for corrective and preventive maintenance of installed security systems and ensure that it is in line with management system or Quality Assurance Program (QAP), as appropriate.

5.14 Drills and Exercises

The applicant or licensee should describe its arrangements for drills and exercises to test the effectiveness of security measures and appropriate response measures against security events mentioned in section 5.9.

This section should also include the frequency for such drills and exercises. The relevant procedure of licensee should also address notification to National Radiation Emergency Coordination Centre (NRECC) for such drills and exercises. Address and contact details of NRECC are given at Annex II.

5.15 Implementing Procedures

The applicant or licensee should prepare and implement operating procedures for the implementation of its physical protection plan. The applicant or licensee should provide only the list of its approved procedures with its physical protection plan. The procedures may include the following:

i. Access authorization;
ii. Key and lock control;
iii. Alarm assessment and initiation of response;
iv. Physical verification of inventory;
v. Receipt, transfer and transport of radioactive sources;
vi. Operation and maintenance of security systems;
vii. Coordination and communication with relevant organizations in case of security event;
viii. Security event reporting;
ix. Drills and exercises for evaluation of security system effectiveness; and
x. Protection of sensitive information.

5.16 Review and Revision of Physical Protection Plan

The applicant or licensee should describe the process for periodic review and revision of its approved physical protection plan. The basis for revision of physical protection plan could be the following:

i. Whenever, there is a change in application or location of radioactive sources;
ii. To address new threat information;
iii. Changes in the regulatory requirements;
iv. After testing and evaluation of physical protection plan;
v. Prescribed interval defined in physical protection plan; or
vi. As deemed necessary by PNRA.

5.17 Transport of Radioactive Sources

In addition to the applicability of above mentioned sections, following information should be included in the physical protection plan for transport of radioactive sources:

5.17.1 Description of the Shipment

The licensee should address description of shipment (type & category of package, number of packages in a consignment, transport index, etc.), mode of shipment (road, rail, air or water) and description of carrier (vehicle, rail, aircraft or ship).

The licensee should provide details of dedicated transport vehicle. The dedicated transport vehicle should comply with security requirements including securing mechanism of source (e.g. chain/tie-downs, locks, and seals), reliable communication means, tracking system (for Category 1 sources), etc.

The licensee should also specify primary & alternate routes, where applicable, and associated in-transit storage.

5.17.2 Advance Notification to PNRA

The licensee should describe the methods and arrangements for advance notification and route information to PNRA for each transportation of radioactive sources. The licensee should provide notification as per format given at Annex III.

5.17.3 Communication and Tracking Arrangements

The licensee should provide details of primary and alternate communication arrangements during transport. The licensee should also describe the measures for tracking of vehicle carrying Category 1 radioactive sources.

Note: For frequently transported radioactive sources (e.g. Industrial radiography, Oil well logging, etc.), the licensee should submit physical protection plan to PNRA for one time approval that will apply for each transportation thereafter (unless plan is revised based on section 5.16).

For radioactive sources which are not frequently transported (e.g. Teletherapy, Irradiators, Industrial gauges, etc.), physical protection plan for each transportation should be submitted to PNRA for approval.

5.18 References, Abbreviations, Tables and Annexes

Applicant or licensee should include all applicable references, abbreviations, tables and annexes necessary for its physical protection plan.

6. REFERENCES

[1]. Regulations on Security of Radioactive Sources – (PAK/926).

[2]. Regulations on Licensing of Radiation Facility(ies) other than Nuclear Installation(s) – (PAK/908) (Rev.1).

[3]. Regulations on Management of a Nuclear or Radiological Emergency – (PAK/914).

[4]. IAEA Code of Conduct on the Safety and Security of Radioactive Sources.

[5]. Implementing Guide on Security of Radioactive Material in Use and Storage and of Associated Facilities – IAEA Nuclear Security Series No. 11-G (Rev. 1).

[6]. Implementing Guide on Security of Radioactive Material in Transport – IAEA Nuclear Security Series No. 9-G (Rev.1).

7. GLOSSARY

i. *"Applicant"* means a person who has applied to the Authority for a license or an authorization.

ii. *"Authority"* means the Pakistan Nuclear Regulatory Authority established under section 3 of the Ordinance.

iii. *"Background Checks"* means a process which includes confirmation of identity, financial/criminal record, moral conduct, motivation, verification of references, and employment history to determine the integrity, character and reliability of an individual.

iv. *"D Value"* means the activity of a radioactive source above which it is considered to be a dangerous source.

v. *"Delay"* means a function of security system, occurring between detection and response, designed to increase adversary's penetration time towards the radioactive source locations.

vi. *"Detection"* means a function of security system that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm.

vii. *"Licensee"* means the holder of a valid license issued by the Authority.

viii. *"Operating Personnel"* means individual workers engaged in the operation of a licensed radiation facility.

ix. *"Physical Protection Plan"* means a document prepared by the licensee and required to be reviewed by the Authority that presents a detailed description of the security arrangements in place at a facility.

x. *"Radiation Facility"* means any premises where radiation source (radioactive material or radiation generator) is acquired, produced, manufactured, processed, reprocessed, repaired, used, handled, extracted, imported, exported, stored, installed, operated, maintained and converted.

xi. *"Radioactive Source"* (also called as sealed radioactive source) means radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form.

xii. *"Response Organization"* means an organization designated or otherwise recognized as being responsible for managing or implementing any aspect of an emergency response.

xiii. *"Response Personnel"* means persons, on-site or off-site, who are appropriately equipped and trained to counter an attempted unauthorized removal of radioactive sources or an act of sabotage.

xiv. *"Sabotage"* means a deliberate act directed against a radioactive source in use, storage or transport that could directly or indirectly endanger the health and safety of personnel, the public or the environment by

exposure to radiation or release of radioactive material.

xv. *"Secured Area"* means designated area containing radioactive source to which access is limited to authorized personnel only and controlled for security purposes.

xvi. *"Security Culture"* means the assembly of characteristics, attitudes and behaviors of individuals, organization and institutions that serve as a means to support and enhance the security.

xvii. *"Security Elements"* means an organization/establishment having its role in the security of radiation facilities.

xviii. *"Security Event"* means an event that has potential or actual implications for security that must be addressed.

xix. *"Security Level"* means protection level for security of radioactive sources, based on graded approach, for determination of security system specifications with respect to corresponding goal.

xx. *"Security Personnel"* means an authorized and security cleared person who is responsible for security relating to patrolling, monitoring, assessing or escorting any individual or transport or controlling access and providing initial response.

xxi. *"Security System"* means an integrated set of security measures.

xxii. *"Sensitive Information"* means information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise security.

xxiii. *"Source location"* means a position of radioactive source inside the secured area.

xxiv. *"Storage"* means the holding of radioactive sources in a facility that provides for their containment with the intention of retrieval.

xxv. *"Transport"* means carriage of radioactive sources by any means of transportation, beginning with the departure from a facility of the shipper and ending with the arrival at a facility of the receiver.

xxvi. *"Unauthorized Removal"* means theft or other unlawful taking of radioactive sources.

ANNEX I

CRITERIA FOR CATEGORIZATION OF RADIOACTIVE SOURCES

Category	Practices	A/D	Security Level
1	Irradiators, Teletherapy	$A/D \geq 1000$	A
2	Industrial radiography, high/medium dose rate Brachytherapy	$1000 > A/D \geq 10$	B
3	Fixed industrial gauges that incorporate high activity sources, Well logging gauges	$10 > A/D \geq 1$	C
4	Low Dose Rate (LDR) Brachytherapy, industrial gauges that incorporate low activity sources, Bone densitometers, Static eliminators	$1 > A/D \geq 0.01$	D
5	LDR Brachytherapy eye plaques and permanent implant sources, X-ray fluorescence devices containing sources, Electron capture devices, Mossbauer spectrometry, check sources.	$0.01 > A/D$ and A > exempt	

ANNEX II

SECURITY EVENT NOTIFICATION FORM

Event Date:	Event Time:
Facility Type: ☐ Irradiators ☐ Teletherapy ☐ Brachytherapy ☐ Industrial Radiography ☐ Industrial Gauges ☐ Oil Well Logging ☐ Calibration Sources ☐ Other _____ (Please specify)	**Nature of Event:** ☐ Source lost or stolen ☐ Attempted or actual sabotage ☐ Unauthorized transfer or transport ☐ Unauthorized access to secured area ☐ Failure of essential security systems ☐ Loss of sensitive information ☐ Other _____ (Please specify)
Name and location of facility/site where incident occurred: _____	
City: _____	Contact No: _____
Incident Summary: (Brief description of event) (Use another sheet, if required)	
Sender details: Name: _____ Designation: _____Contact No: _____ Reporting Time: _____ Signature with date: _____	

Please send filled form to:

National Radiation Emergency Coordination Center (NRECC)

PNRA HQs, Mauve Area, G-8/1, Islamabad.

Telephone	Fax	Email
Primary: 051-9262019 Backup: 051-2289210 Toll Free: 080077766 Officer In Charge: 03008540319 Alternate Officer In Charge: 03345131978	Primary: 051-9260201 Backup: 051-2289233	nrecc@pnra.org

ANNEX III

INFORMATION PROFORMA FOR TRANSPORT OF RADIOACTIVE SOURCES

Name of the Facility:

- ☐ Industrial Radiography
- ☐ Nuclear Gauges
- ☐ Oil Well Logging
- ☐ Other _____
  (Please specify)

License No. _____

Information	Details
Name of the focal person along with contact details who will be responsible to ensure safety and security and coordination with PNRA and other federal agencies	
Planned date & time of radioactive source movement	
Radioisotope(s)	
ID of source(s), type & Sr. No. of container(s) (if applicable)	
Current activity/physical form	
Validity of transport container	
From (Address of site from where the source is to be moved)	
To (Address of site where the source is to be received along with clients contact details)	
Name of the Incharge along with contact details who will receive the source	
Name of designated person along with CNIC and mobile numbers travelling with the vehicle	
Details of vehicle along with its Registration Number	
Transportation route plan (name of the highway/road, etc.)	
In transit storage locations (if applicable)	
Necessary instructions for safety and security during transport provided to the personnel	
Other information, if any.	

Signature and stamp of the licensee: _____

Please send filled Proforma to:

National Radiation Emergency Coordination Center (NRECC)
PNRA HQs, Mauve Area, G-8/1, Islamabad.

Telephone	Fax	Email
Primary: 051-9262019 Backup: 051-2289210 Toll Free: 080077766 Officer In Charge: 03008540319 Alternate Officer In Charge: 03345131978	Primary: 051-9260201 Backup: 051-2289233	nrecc@pnra.org

PAKISTAN NUCLEAR REGULATORY AUTHORITY
P.O. Box 1912, Islamabad
www.pnra.org