



اوتوريتي كبحسائن كسلامتن
كصيجتن. دان عالم سكيتر
Safety, Health and Environment
National Authority

GUIDELINES ON SECURITY OF RADIOACTIVE MATERIAL PROGRAMME (SRMP) REQUIREMENTS



DOCUMENT HISTORY

DOCUMENT TITLE	GUIDELINES ON SECURITY OF RADIOACTIVE MATERIAL PROGRAMME (SRMP) REQUIREMENTS
DOCUMENT NUMBER	SHENA / CID / GUI / 4-203
AUTHOR	COMPLIANCE AND INTERNATIONAL AFFAIRS DIVISION (CID)
ISSUE DATE	01 JULY 2023
NEXT REVIEW DATE	30 JUNE 2025
DISTRIBUTION	SHENA WEBSITE & SOCIAL MEDIA

REV	REVISION DESCRIPTION	NAME	ENDORSER	DATE
0	Draft for review	Radiation Team	Director of CID	April 2023
1	First Issue	Compliance and International Affairs Division	Interim Chief Executive Officer <i>Zm</i>	July 2023

DISCLAIMER

This document is the property of the Safety Health and Environment National Authority (SHENA), Brunei Darussalam. Circulation is restricted to SHENA and its designated associates. It must not be copied or used for any other purpose other than which it is supplied, without the expressed written authority of SHENA.

SHENA disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party. Any misuse of the document is not supported by SHENA.



CONTENTS

1. INTRODUCTION	3
2. OUR VISION, MISSION, KEY PRINCIPLES AND VALUES	3
3. PURPOSE	4
4. SCOPE	4
5. DEFINITIONS AND ABBREVIATIONS	5
6. BASIC ELEMENTS OF A SECURITY OF RADIOACTIVE MATERIAL PROGRAMME	5
PART 1: INTRODUCTION	5
PART 2: SECURITY MANAGEMENT	6
PART 3: SECURITY POLICY	6
PART 4: SECURITY PROCEDURES	7
PART 5: FACILITY AND STORAGE	7
PART 6: SITE PLAN	7
PART 7: SECURITY PERIMETER	8
PART 8: ACCESS CONTROL	8
PART 9: TRANSPORTATION	8
PART 10: SECURITY OF INFORMATION	9
PART 11: MAINTENANCE, TESTING, AND EVALUATION	9
PART 12: CONTIGENCY AND RESPONSE PLAN	9
PART 13: SECURITY AWARENESS PROGRAMME	10
PART 14: REFERENCE DOCUMENT	10
7. EFFECTIVE DATE	10
8. REFERENCES	11
APPENDIX A	12
APPENDIX B	13
APPENDIX C	14
APPENDIX D	19



1. INTRODUCTION

The Safety, Health and Environment National Authority (**SHENA**) is a statutory body set up under the Safety Health and Environment National Authority Act, Chapter 227. The Authority acts and enforces all matters relating to workplace safety, health and the environment as well as radiation within Brunei Darussalam. SHENA is headed by a Chief Executive Officer (CEO) reporting directly to the Minister in Charge (Minister at Prime Ministry Office) and responsible for the administration of the SHENA Act, Chapter 227.

2. OUR VISION, MISSION, KEY PRINCIPLES AND VALUES

2.1 SHENA Vision Statement

We are committed to making a difference and ensuring Brunei Darussalam is a safe place to work and live.

2.2 SHENA Mission Statement

We will maintain a robust fit for purpose national safety, health and environmental regulatory framework and ensure that the risks to people, assets and the environment are controlled in compliance with laws and regulations, set by the government, and implemented by those who create the risk and underpinned by continuous improvement.

2.3 Principles

Our operational philosophy is governed by four key principles:

- a) Structured
- b) Auditable
- c) Focused
- d) Engaged

In all our activities we will ensure a transparent and open dialogue with all our stakeholders. Our stakeholders include industry, government, and the general public and our key principles apply equally to all.

2.4 Values

All our employees are expected to adopt key values in their day-to-day engagements. Our employees will demonstrate the following values in all aspects of our activities:

- a) Integrity
- b) Respect
- c) Reasonability
- d) Professionalism



3. PURPOSE

This document is created as guidelines on the development of a Security of Radioactive Material Programme (**SRMP**) for licensees and new applicants in accordance with Section 8 of the Radiation Protection Act (**CAP 228**).

The SRMP is required to be developed by the licensee and new applicants handling category 1 and 2 radioactive materials according to the categorisation of radioactive materials that appear in [Appendix A](#) and [Appendix B](#).

4. SCOPE

These guidelines outline the minimum legal and regulatory requirements in developing the SRMP in accordance with CAP 228, comprising the security measures such as detection, delay and response elements and necessary arrangements required to be provided as well as implemented by the licensee to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of radioactive material during their entire lifecycle, including while they are in storage or transport, or being stored during transportation.

In preparation for the SRMP, licensee and new applicants must:

- (i) Ensure the type of radiation activity, radioactive material(s) and location(s) to be engaged are clearly identified and aligned with the Radiation Protection Programme (RPP);
- (ii) Elaborate the standard operating procedures (SOPs) on the radiation activity to be conducted to ensure the security of radioactive material is in place;
- (iii) Ensure risk assessment (potential threats, vulnerabilities on-site and/or off-site, potential consequences and the likelihood of malicious acts) is developed;
- (iv) Ensure security measures related to detection, delay and response to security events are carefully determined and implemented according to the recommended security level and security objectives that appear in [Appendix C](#);
- (v) Ensure the SRMP to be submitted to SHENA is endorsed by the Radiation Protection Officer (RPO) and the licensee;
- (vi) Ensure the SRMP is reviewed at least once in two years, OR when there are changes made to particulars OR as directed by SHENA; and



- (vii) Ensure the cover page of SRMP carries the information required by SHENA that appears in [Appendix D](#).

These guidelines may be amended or varied by SHENA from time to time.

5. DEFINITIONS AND ABBREVIATIONS

In this guideline, the abbreviations commonly used are as follows:

- (i) CCTV - Closed-Circuit Television
- (ii) PIDS - Perimeter Intrusion Detection System
- (iii) RPP - Radiation Protection Programme
- (iv) SRMP - Security of Radioactive Material Programme

6. BASIC ELEMENTS OF A SECURITY OF RADIOACTIVE MATERIAL PROGRAMME

A Security of Radioactive Material Programme is expected to be comprehensive and comprises (but not limited to) the following basic elements:

- (i) Introduction;
- (ii) Security Management;
- (iii) Security Policy;
- (iv) Security Procedures;
- (v) Facility and Storage;
- (vi) Site Plan;
- (vii) Security Perimeter;
- (viii) Access Control;
- (ix) Transportation;
- (x) Security of Information;
- (xi) Maintenance, Testing and Evaluation;
- (xii) Contingency and Response Plan;
- (xiii) Security Awareness Programme; and
- (xiv) Reference Documents.

These basic elements are further described as follows:

PART 1: INTRODUCTION

This Part is expected to briefly describe the business entity, the type of radiation activity involved, the premises, the number of employee(s) and the location(s) whereby the following information is required to be provided:

- (i) Background of business entity and premises;



- (ii) Objective(s) of the security programme; and
- (iii) Organisation chart and departments (including contact details) dealing with the security of radioactive materials.

PART 2: SECURITY MANAGEMENT

This part should describe the security management measures in place whereby the following information is required to be provided:

- (i) Roles and responsibilities of each personnel in the security management measures.
 - The licensee should identify the personnel from senior management, radiation worker(s) and other personnel responsible for the security of radiation activity, including the designation of an individual responsible for maintaining the site security plan.
- (ii) Background checks to determine trustworthiness and reliability.
 - This section should describe the arrangement for verifying the identity of all personnel, including worker(s) and external contractor(s) to ensure the trustworthiness and reliability of all designated personnel authorised for unescorted access to radioactive material(s) and/or for access to sensitive information.
- (iii) Accounting and inventory of radioactive material(s).
 - The licensee should establish and maintain an inventory of radioactive material(s) under its responsibility. In the event of information required and/or inspection conducted by the Authority, the licensee should be able to verify that the inventory is accurate, and that radioactive material(s) is present at its authorised location.
- (iv) Potential security threat.
 - Licensee should identify and list potential threat events while considering all activities, for example, during transportation, storage, on-site, etc.

PART 3: SECURITY POLICY

This part should describe the company's corporate security policy, including commitments to ensure that security management measures are in place.



PART 4: SECURITY PROCEDURES

This part should describe written procedures to provide guidance to personnel for operating and maintaining security management measures such as the following:

- (i) Security procedure for routine, off-shift, and emergency operations.
- (ii) Security procedure to be followed before and after the conduct of any maintenance work.
- (iii) Security procedure for opening and closing of the facility.
- (iv) Key and lock control procedure.
- (v) Accounting and inventory control procedure.
- (vi) Security procedure for acceptance and transfer or movement of the radioactive material(s) from one facility to another.

PART 5: FACILITY AND STORAGE

This part should provide a general description of the company's radiation activity, including a list of the building(s), vessel(s), room(s), or location(s) (by name and number or other means of identification) where radioactive material(s) is(are) involved. The licensee must provide the following information for each of the buildings, rooms, vessels, or locations:

- (i) Type and category of the radioactive material(s).
- (ii) Security arrangements for storage of equipment containing radioactive material(s).
- (iii) Means of detecting unauthorised intrusion either to the equipment or storage location.
- (iv) Process or procedure to access the facility.

The licensee should identify and clearly mark the controlled area (restricted area) limited to authorised personnel and the areas accessible by the public.

The licensee should identify facility management arrangements associated with the security of the facility, especially where radioactive material(s) and associated activities are present.

PART 6: SITE PLAN

This part should provide a layout, drawing, photograph, or other accurate illustration of the associated facility, clearly showing the following:

- (i) All relevant fence lines, boundaries, and facilities.
- (ii) Location of all security systems.
- (iii) Location of all access and egress points.



PART 7: SECURITY PERIMETER

This part should describe the security measures in place on the perimeter, including details of fences, gates, barriers, windows and doors, security lighting, perimeter intrusion detection system (PIDS), closed-circuit television (CCTV), or any other arrangement such as the gatehouse, etc.

The licensee should identify and ensure that the materials and/or system in place on the perimeter are appropriate for such a threat, the nature of the radioactive material(s) being protected, and the classification area (such as controlled area) of the site.

PART 8: ACCESS CONTROL

This part should describe the physical measures for controlling access, such as how personnel and vehicles are physically controlled at each access point to ensure that only individuals with authorized access enter areas containing radioactive material(s), as well as the specific media used to authenticate the identity of authorized individuals and vehicles at the access point, such as a key card, personal identification number, biometric device, or a combination thereof.

This part should also include a description of security arrangements, such as an escort policy for the contractor(s), staff without authorized access, and/or visitor(s) entering the facility and areas containing radioactive material(s).

The licensee should identify the number of personnel with authorised access and the number of personnel without authorised access.

The licensee should identify the process for screening vehicles and searches for weapons and substances prior to entering the facility, if necessary.

The licensee should identify and guarantee that the locks used are of high quality, with characteristics that provide some resistance to forced attack. A key management procedure should be established to control the movement of personnel and prevent unauthorised access or compromise.

PART 9: TRANSPORTATION

The licensee should provide a list and details of the vehicle(s) used for the transportation of radioactive material(s).

The security management measures in place for the transportation of radioactive material(s) should be clearly described, including the following:



- (i) Security precautions for the transportation of radioactive material(s).
- (ii) Means of detecting unauthorised removal of the equipment before arriving at the destination.
- (iii) Transportation security procedure.

PART 10: SECURITY OF INFORMATION

This part should describe the security management measures in place or procedures established including computer security to ensure the confidentiality, integrity, and availability of sensitive information from unauthorised disclosure (or modification, alternation, destruction, or denial of use) is maintained.

The licensee should categorize the sensitive information which contains details such as the following:

- (i) The security arrangements at a facility.
- (ii) The security systems, structures, and components at a facility.
- (iii) The location and details of the transport of radioactive material(s).
- (iv) Details of organisation and background personnel.

PART 11: MAINTENANCE, TESTING, AND EVALUATION

The licensee should conduct an assessment and verify the effectiveness of the security system to ensure that all applicable security requirements are met. In addition, this part should describe the process and arrangement for maintenance, calibration, testing and evaluation of all the security equipment and system in place, including information on compensatory measures, performance testing, quality assurance and the frequency of testing and evaluation.

PART 12: CONTINGENCY AND RESPONSE PLAN

This part should describe the contingency and response plan for all potential security events, such as unauthorized access to a location containing radioactive material(s), attempted or successful unauthorized removal, loss, and destruction of radioactive material(s), sabotage, cyber-attack, and any other scenario involving the security of radioactive material(s) and/or facility that may be considered and addressed in the plan.

The plan should provide procedures for responding to the security event(s), including reporting to the relevant Authority and emergency response agencies following the event(s), and actions required.

The list of emergency and other relevant phone numbers shall be provided in a separate attachment. The list shall include, but not be limited to, police and fire



department, ambulance, Radiation Protection Officer (RPO), and SHENA radiological emergency phone number.

The licensee should also specify compensatory measures that will be implemented when physical protection barriers deteriorate or equipment fails, as well as improvements to the procedures that will be implemented in the case of an increase in the overall level of threat.

The licensee should ensure that the contingency and response plan is coordinated with the radiological emergency preparedness and response plan stated in the Radiation Protection Programme (RPP).

PART 13: SECURITY AWARENESS PROGRAMME

This part should describe the security awareness training programme provided to employees and other personnel (for example, contractors, building maintenance staff, and temporary employees), which should contain the following:

- (i) Instructions and information on security measures.
- (ii) Security culture within the organisation.
- (iii) Any restrictions concerning access, use, storage and/or transportation of radioactive material(s).
- (iv) Threats and security concerns, methods to address such concerns and actions to be undertaken in the event of a security incident.

The licensee should ensure that all personnel whether they are engaged in radiation activity or not receive general security awareness and are recorded accordingly.

PART 14: REFERENCE DOCUMENT

The licensee should provide information on reference documents used in the development of the security of radioactive material programme (SRMP) including existing regulations or standards, policies, procedures, and operating manuals.

7. EFFECTIVE DATE

These guidelines take effect immediately upon the date of release and when they are published on the SHENA website at www.shena.gov.bn. For further questions regarding this guideline, the licensees and new applicants can contact the Authority at:

Safety Health and Environment National Authority (SHENA)
Level 6, Knowledge Hub Building,
Simpang 32-37, Kg Anggerek Desa,



اتوريٲى كبحسان كسلامن
كصيتن دن عالم سكيتن
Safety, Health and Environment
National Authority

Bandar Seri Begawan BB3713
Brunei Darussalam

Operating hours : Mon – Fri 8:00am – 11:30am; 2:00pm – 4:00pm
Office telephone no. : +673 2382000
Email address : radapplication@shena.gov.bn

8. REFERENCES

- (i) Radiation Protection Act, Chapter 228.
- (ii) International Atomic Energy Agency (IAEA) (2005) “Categorization of Radioactive Sources” IAEA Safety Standards Series RS-G-1.9 ISBN 92–0–103905–0.
- (iii) International Atomic Energy Agency (IAEA) (2019) “Security of Radioactive Material in Use and Storage and of Associated Facilities” IAEA Nuclear Security Series No. 11-G (Rev. 1).
- (iv) International Atomic Energy Agency (IAEA) (2008) “Security in the Transport of Radioactive Material” IAEA Nuclear Security Series No. 9.
- (v) International Atomic Energy Agency (IAEA) (2011) “Nuclear Security Recommendations on Radioactive Material and Associated Facilities” IAEA Nuclear Security Series No. 14.



CATEGORISATION OF RADIOACTIVE MATERIAL

CATEGORY	SOURCES USED AND/OR PRACTICES
1	<ul style="list-style-type: none"> • Radioisotope Thermoelectric Generators (RTGs) • Irradiator sources • Teletherapy source • Multi – Beam Teletherapy (Gamma Knife) sources
2	<ul style="list-style-type: none"> • Industrial Gamma Radiography sources (Non-Destructive Testing) • Brachytherapy sources • Calibration sources (⁶⁰Co)
3	<ul style="list-style-type: none"> • Industrial level gauges • Conveyor gauges • Well-logging gauges • Security Purpose that used Radioactive Material • Calibration sources (²⁴¹Am) • Blast furnace gauges • Spinning pipe gauges (¹³⁷Cs)
4	<ul style="list-style-type: none"> • Thickness gauges • Fill level gauges • Calibration sources (⁹⁰Sr, ¹³⁷Cs, ⁵⁷Co) • Moisture detectors (²⁴¹Am/Be) • Density gauges (¹³⁷Cs) • Static Eliminators sources • Bone Densitometers sources • X-ray Fluorescence (XRF) analyser sources (⁵⁵Fe) • Electron capture detector sources • Medical unsealed sources • Tritium targets (³H) • PET check sources (⁶⁸GE) • Mossbauer spectrometry sources (⁵⁷Co) • Naturally Occurring Radioactive Material (Norm) • Technologically enhanced naturally occurring radioactive material (TENORM) • Thorium Blanket (²³²Th)



APPENDIX B

CATEGORISATION OF RADIATION ACTIVITIES REQUIRING SRMP

NO.	RADIATION ACTIVITIES	REQUIREMENT	
		RPP	SRMP
1	Sales of any controlled apparatus.	Yes	No
2	Sales and maintenance of any controlled apparatus.	Yes	No
3	Sales and transport of any controlled apparatus.	Yes	No
4	Use of Controlled Apparatus.	Yes	No
5	Sales of any radioactive materials.	Yes	No
6	Sales and maintenance of any radioactive materials (Category 1 and 2).	Yes	Yes
7	Sales and transport of radioactive materials (Category 1 and 2).	Yes	Yes
8	Sales and transport of radioactive materials (Category 3,4 and 5).	Yes	No
9	Use of radioactive materials (Category 1 and 2).	Yes	Yes
10	Use of radioactive materials (Category 3,4 and 5).	Yes	No
11	Use of check source for education purpose.	Yes	No
12	Transport of radioactive materials (via land) (Category 1 and 2).	Yes	Yes
13	Transport of radioactive materials (via land) (Category 3, 4 and 5).	Yes	No
14	Transport of radioactive materials (via sea) (Category 1 and 2).	Yes	Yes
15	Transport of radioactive materials (via sea) (Category 3,4 and 5).	Yes	No
16	Transport of any radioactive materials (via air).	Yes	No
17	Permanent or temporary storage of radioactive materials (Category 1 and 2).	Yes	Yes
18	Permanent or temporary storage of radioactive materials (Category 3,4 and 5).	Yes	No
19	Permanent or temporary storage of any controlled apparatus.	Yes	No



RECOMMENDED SECURITY LEVEL AND SECURITY OBJECTIVES

Security Programme Sub-sections	Category 1 – High-risk	Category 2 – High-risk	Category 3 – Medium risk	Category 4 and 5 – Low-risk
Access control	<ul style="list-style-type: none"> Restrict access to authorised users only. Two-person rule (optimal). Visitors, students, contractors must be escorted at all times by an authorised users. 	<ul style="list-style-type: none"> Restrict access to authorised users only. Visitors, students, and contractors must be escorted at all times by an authorised users. 	<ul style="list-style-type: none"> Restrict access to authorised users only. Visitors, students, and contractors must be escorted at all times by an authorised users. 	<ul style="list-style-type: none"> Source should be protected against unauthorized access and removal.
Intrusion detection system	<ul style="list-style-type: none"> The licensee should provide immediate detection and be linked to a control room monitored by operator personnel 24/7 or an equivalent mechanism (i.e., continuous surveillance by operator personnel) for detection, assessment, and communication with response personnel in case of a security event. 			
Perimeter and/or	<ul style="list-style-type: none"> Radioactive material must be protected with at least two physical barriers (i.e., walls, cages, secure containers) to separate the source from unauthorised 			



Security Programme Sub-sections	Category 1 – High-risk	Category 2 – High-risk	Category 3 – Medium risk	Category 4 and 5 – Low-risk
physical barrier	personnel and provide a sufficient delay to allow for immediate detection, and for response personnel to intervene before the adversary can remove the source.			
Security of storage	<ul style="list-style-type: none"> Secured with high-quality padlock, high-security lock or equivalent security system. Equipped with a minimum of one intrusion detection system or equivalent. Secured containers must be able to resist an attack by handheld tools. 	<ul style="list-style-type: none"> Secured with high-quality padlock, high-security lock or equivalent security system. Equipped with a minimum of one intrusion detection system or equivalent. 	<ul style="list-style-type: none"> Should be stored in a secure container or location. 	
Response protocol	<ul style="list-style-type: none"> Specific response protocol and contingency plan. Contact local law enforcement. Effective response time. Must develop a procedure in case of lost, stolen or malicious acts involving radioactive material. 	<ul style="list-style-type: none"> Generic response protocol and contingency plan. Must develop a procedure in case of lost, stolen, or malicious acts 	<ul style="list-style-type: none"> Source should be protected against unauthorized access and removal. 	



Security Programme Sub-sections	Category 1 – High-risk	Category 2 – High-risk	Category 3 – Medium risk	Category 4 and 5 – Low-risk
			involving radioactive material.	
Maintenance and testing	<ul style="list-style-type: none"> Maintenance and testing of the security system should be conducted at least every six months, and written records must be maintained. 			
Facility security plan	<ul style="list-style-type: none"> Reviewed regularly or when important and significant changes are made at the facility. Classified prescribed and/or sensitive and stored appropriately. Communicated on a need-to-know basis. Indicate measures in case of increased threat. 	<ul style="list-style-type: none"> Reviewed annually or when important changes are made at the facility. Must be classified as prescribed and/or sensitive and stored appropriately. Communicated on a need-to-know basis. 	<ul style="list-style-type: none"> Prudent management practices^a. 	
Personnel trustworthiness or	<ul style="list-style-type: none"> Conduct criminal records name check. Conduct reference, education, and employment verification. 	<ul style="list-style-type: none"> Conduct reference, education, and employment verification. 	<ul style="list-style-type: none"> Conduct reference, education, and employment verification. 	



Security Programme Sub-sections	Category 1 – High-risk	Category 2 – High-risk	Category 3 – Medium risk	Category 4 and 5 – Low-risk
background checks	<ul style="list-style-type: none"> Ensure drivers and contractors (i.e., carriers) with unescorted access to radioactive material must undergo this verification. 		<ul style="list-style-type: none"> Conduct criminal records name check. 	<ul style="list-style-type: none"> Conduct criminal records name check (as part of prudent management practices^a).
Information security	<ul style="list-style-type: none"> All prescribed information should be protected and be shared on a need-to-know basis. 			
Security awareness program	<ul style="list-style-type: none"> All authorised users, including staff who transport radioactive material, should receive security awareness on a regular basis. 			
Vehicle security	<ul style="list-style-type: none"> Vehicle must be equipped with anti-theft or vehicle disabler and intrusion detection system, or equivalent. Vehicle must be equipped with a minimum of two technical barriers to prevent unauthorized removal of the radioactive source/device. Access must be restricted to authorized users only. Install GPS or tracking system. 		<ul style="list-style-type: none"> Vehicle must be equipped with an anti-theft and intrusion detection system or equivalent. Vehicle must be equipped with a minimum of two technical barriers to 	<ul style="list-style-type: none"> Source should be protected against unauthorised access and removal.



Security Programme Sub-sections	Category 1 – High-risk	Category 2 – High-risk	Category 3 – Medium risk	Category 4 and 5 – Low-risk
	<ul style="list-style-type: none"> • Drivers must be equipped with a means of communication in case of emergency. • Two-person rule (optimal). • Drivers and operators must undergo background verification. 		<p>prevent unauthorized removal of the radioactive source/device.</p>	
Transportation security plan	<ul style="list-style-type: none"> • Should develop and submit a specific Transport Security Plan to SHENA for review and approval. 	<ul style="list-style-type: none"> • Should develop and maintain a generic Transport Security Plan. 	<ul style="list-style-type: none"> • Apply prudent management practices^a. 	<ul style="list-style-type: none"> • Source should be protected against unauthorised access and removal.

^a Prudent Management Practices include ensuring that sealed sources are secured to prevent illegal use, theft, or sabotage, and that a periodic inventory is carried out to ensure sealed sources are at their designated location and are secure.



FOR EXTERNAL USE ONLY

**EXAMPLE FOR
THE FRONT PAGE OF SECURITY OF RADIOACTIVE MATERIAL PROGRAMME**

<div style="border: 1px solid black; border-radius: 10px; padding: 5px; display: inline-block;">COMPANY LOGO</div>	
<p>SECURITY OF RADIOACTIVE MATERIAL PROGRAMME</p> <p>Version XXX</p>	
<p>We hereby declare that all information contained in the Security of Radioactive Material Programme is correct and true. We further acknowledge that we understand and agree that the programme will be implemented accordingly.</p>	
RADIATION PROTECTION OFFICER (RPO)	LICENSEE
Signature	Signature
NAME: DATE:	NAME: DATE: