NRRC Stakeholders Guidelines

Kingdom of Saudi Arabia

# Development of Security Plan for Radioactive Material

NRRC-SG-001

2023

هيئة الرقابة النووية والإشعاعية
Nuclear and Radiological Regulatory Commission

**Stakeholder Guideline**

Development of Security Plan for Radioactive Material

2023

NRRC-SG-001

## Preamble

In accordance with the provisions of the NRRC's approved Regulations, this stakeholder guideline describes criteria and/or techniques that are considered appropriate for satisfying the requirements stipulated in the NRRC's regulations.

This stakeholder guideline has been prepared on the basis of International Atomic Energy Agency (IAEA) standards, as well as the and the international best practices and the experiences of similar international regulatory bodies, and in accordance with the Kingdom's international commitments, and it has been approved by the NRRC's CEO resolution No. 1111 , dated 03/04/2023.

# Contents

## 1. Purpose

Nuclear and Radiological Regulatory Commission (NRRC) has developed an effective regulatory framework for the safe and secure of radioactive material throughout their life cycle against unauthorized removal and sabotage. Under this regulatory framework, the prime responsibility for safety and security of radioactive material lies with the authorized person. The purpose of this guideline is to guide the authorized person or applicant to develop and maintain security plan for security of radioactive material.

The NRRC ensures security of radioactive material in the Kingdom through provision of requirement for a security plan and regulatory oversight to the authorized person. – It is indicated in Article 37 of Regulation on Security of Radioactive Materials (NRRC-R-17) that "the authorized person for radioactive material of categories 1, 2, and 3 shall submit a security plan for approval by the NRRC as part of the authorization requirements".

## 2. Scope

This is a guideline for development of a security plan that is applicable to the security of radioactive material, associated activity, and associated facility, having Categories1, 2 and 3 radioactive sources throughout their life cycle within the Kingdom.

The security measures for materials of Category 4, and 5 can be applied based on safety measures prescribed in Regulation on Radiation Safety (NRRC-R-01) that are sufficient to address the desired security measures. Nevertheless, the authorized person or applicant may develop a security plan for category 4, and 5 of radioactive sources as a good practice by using the relevant sections in this regulatory guideline.

## 3. General Security Measures

The security plan should include all security measures concerning the detection, delay, and response against unauthorized removal and sabotage in accordance with Regulation on Security of Radioactive Materials (NRRC-R-17).

The authorized person or applicant should develop and maintain a security plan for security of radioactive material under its jurisdiction based on the threat and risk assessment to determine vulnerabilities in the existing physical protection systems designed to protect against the loss, sabotage, illegal use, illegal possession, or illegal removal radioactive sources throughout their life cycle. Additionally, the security plan should be reviewed annually and updated as the level of threat changes in response to evolving threats.

The degree of rigor of a threat and risk assessment should be evaluated following the graded approach and should be commensurate with the category and risks associated with the radioactive material. This threat and risk assessment may be incorporated into existing assessments.

### 3.1 General Instructions for Security Plan

These general instructions should be followed by the authorized person or applicant while developing a security plan for security of radioactive material:

- The security plan should be part of the facility's overall management system.
- The security plan should be prepared by the authorized person in consultation with concerned security elements.

- The security plan should provide clear, concise and up to date information.
- The security plan should include a table of contents.
- Definitions and abbreviations (if necessary) should be consistent throughout the document.
- Duplication of information should be avoided. In case where necessary, reference to relevant section should be made.
- Legible drawings, diagrams, maps, annexes and tables should be added wherever necessary with proper reference.
- The security plan should be signed by the authorized person and each page of the security plan should contain a page number, a revision number (if applicable) and date.
- The security plan and related records should be protected against unauthorized disclosure.

## 4. Format and Content of Security Plan

The following sections and subsections describe the content and level of details that should be included within the security plan, and guidance checklist for development of the security plan that is illustrated in Annex-I:

### 4.1. Introduction

In the Introduction section, the authorized person or applicant should describe the purpose of the facility, operations and na-

ture of activities that involve radioactive materials. The authorized person or applicant should also describe the scope and objectives of its security plan.

## 4.2. Facility Description

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

a. Location (address);

b. Relevant departments where the radioactive materials are either manufactured, used or stored including their details;

c. Facility working hours; and

d. Number of personnel visiting the facility (employees, general public, etc.).

## 4.3. Radioactive Source Description, Categorization, and their Corresponding security Levels

The authorized person or applicant should provide details of radioactive sources such as radionuclide's reference activity (mentioned on source certificate), identification number of source, physical form, quantity, serial number and other information that may be prescribed by the NRRC in compliance with Regulation on Radiation Safety (NRRC-R-01), for each category specified in Regulation on Security of Radioactive Materials (NRRC-R-17).

## 4.4. Map of the Secured Area

In this section, the authorized person or applicant should provide a map or layout of the secured area, locations of radioactive sources and associated entry and 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 4.8.

## 4.5. Organizational Structure and Responsibilities

The authorized person or applicant should provide information about the security assigned responsibility and its relationship with the overall organizational structure of the activity or facility. Security related responsibilities and clear lines of authorities of management, operating personnel and security personnel of the authorized activity or at the facility, 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 authorized person or applicant should provide details of designated contact person travelling with the vehicle and describe responsibilities of all the individuals involved in the transportation. This includes transfer of responsibilities when a radioactive source is moved from origin to destination.

### 4.6. Personal Trustworthiness and Reliability

The authorized person or applicant's trustworthiness verification program should ensure that individuals who have unescorted access to high-risk radioactive sources are trustworthy and reliable, and do not pose an unreasonable risk to the health and safety of persons and security. The authorized person or applicant should obtain a record from the relevant competent security agencies showing the result of a criminal record on the persons. The authorized person or applicant should maintain copies of all documents provided and ensure that they have been verified as original. The trustworthiness verification program should be reviewed on a regular basis.

The trustworthiness verification program should apply to:

- Individuals with unescorted access to Categories 1, 2 and 3 sources.
- Vehicle drivers and those accompanying the transport of Categories 1, 2 and 3 sources.
- Any individual whose assigned duties provide access to prescribed and/or sensitive information or the handling of Categories 1, 2 and 3 sources (including onsite security officers).

The trustworthiness verification program identifies past actions to help determine an individual's past and current character and reputation in order to provide reasonable assurance of that individual's future reliability. Some indicators that authorized person or applicants may consider while verifying trustworthiness and reliability include:

- Conviction for a serious crime within the past five (5) years (including murder, attempted murder, or indictable offences involving violence).
- Impaired performance or dangerous behavior attributable to psychological or other disorders.
- Misconduct that warrants criminal investigations or results in arrest or conviction.
- Indication of deceitful or delinquent behavior.
- Attempted or threatened destruction of life or property.
- Illegal drug use, abuse or distribution.
- Alcohol abuse disorders.
- Failure to comply with work directives.
- Hostility or aggression toward fellow workers or authority.
- Uncontrolled anger.
- Violation of safety or security procedures.

### 4.7. Protection of Sensitive Information and Computer System

The authorized person or applicant should identify and classify sensitive information (both in hard and electronic forms) and should describe the measures for its protection.The authorized person or applicant should also describe cyber security measures for computer systems important to safety and security.

Cyber security enables the authorized person or applicants 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 authorized person or applicant should consider cyber security for the following categories:

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

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

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

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

For effective cyber security of computer and computer-based system, the authorized person or applicant should ensure the following measures at least

a. Restricting the number of personnel granted administrative rights or accounts on each computer.

b. Taking other types of controls beyond physical controls for protecting digital assets. This may be technical (e.g. firewalls, account passwords, antivirus software) or administrative (e.g. policies, procedures, guidelines, trainings).

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

d. Disabling wireless interfaces when they are not needed.

e. Disabling all open and unused network ports.

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

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

## 4.8. Security System and Measures

The authorized person or applicant should include the description of the security system and measures designed (detection, delay and access control), installed and implemented in order to protect radioactive sources in accordance with the regulatory requirements mentioned in Regulation on Security of Radioactive Materials (NRRC-R-17). The details should be described as per following subsections:

### 4.8.1 Detection

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

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

b. The measures used to detect unauthorized removal of radioactive sources either by electronic tamper detection device or operating personnel, as applicable.

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

d. The measures of communication to response personnel such as telephone, cell phone, walkie-talkie, etc.

e. The measures of physical verification of radioactive sources on periodic basis (such as fortnightly basis for Categories 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.

f. Continuous visual surveillance by operating personnel as a detection measure for mobile and/or portable radioactive sources in use.

For detection of unauthorized access, failure or tampering, the alarm system should:

- activate immediately upon detecting an intrusion or tamper event;
- stay in an alarmed state until acknowledged by an authorized person;
- use more than one sensor or sensor type in order to provide redundancy;
- include overlapping sensor detection areas.

### 4.8.2 Delay

The authorized person or applicant should describe the 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 Categories 1 and 2 radioactive sources.

Guidance for delay measures is illustrated in the following subsections:

#### 4.8.2.1 Locking hardware and key control

If keys are used, the authorized person or applicant should implement a key control policy that:

- restricts the number of individuals with keys;
- restricts the number of master keys;
- prohibits employees from duplicating keys;
- uses a patented key or dedicated keyway to prevent unauthorized duplication of keys;
- includes a provision for employees to return keys when access is no longer required; and
- ensures that key blanks are stored securely.

For key control, the authorized person or applicant should:

- conduct a review of the key inventory and keyholders on a regular basis;
- note changes and additions to the key inventory and key-holders in their records;
- maintain accountability for all keys that have been issued and keys reported lost or stolen.

When conventional locks and keys are used, they should be of high quality or from a high- security lock series. Key management procedures should be designed to prevent unauthorized access or compromise. The locks should have shielded shackles, to prevent cutting of the lock.

**4.8.2.2 Physical barriers**

Traditional barriers such as chain-link fences, locked doors, grilled windows, masonry walls and vaults are commonly used for storage of radioactive sources. Barriers should be considered in relation to an adversary's objectives.

The authorized person or applicant should implement multiple physical barriers to protect the radioactive sources. Multiple barriers potentially force an adversary to bring a variety of tools to defeat each individual barrier, thereby delaying the adversary and providing the response personnel with time to intervene.

For example, multiple barriers may include:

- A portable device (e.g., portable gauge, exposure device) stored inside a vault or safe that is bolted to the floor and capable of resisting common attack tools.

- A mobile device (e.g., a brachytherapy unit) that may be chained to the floor within the storage area. The chain is made of material that is resistant to common attack tools and is secured with a high-quality padlock that has the same level of robustness (e.g., shielded shackles).

- A solid-core door made of wood or metal, installed with non-removable screws, pinned door hinges, a latch protector and an automatic door closer.

- A window equipped with laminated window-film resistant to burglar attacks.

#### 4.8.2.3 Secure container

The storage location and/or container should be:

- Secured with a locking mechanism or have other measures to prevent unauthorized removal;

- Secured when left unattended;

- Equipped with an alarm system to detect unauthorized entry or access; and

- Sufficiently robust to resist common attack tools (e.g., crowbar, drill, blowtorch).

### 4.8.3 Access Control

The authorized person or applicant should describe the 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 access to a person with authorized access only.

The authorized person or applicant should consider the following measures in controlling access to the radioactive sources based on a graded approach:

- Monitoring and maintaining records of all personnel with access to secure storage areas, and transport points through the use of a logbook or an access control system with tracking capabilities.
- Implementing effective access control measures such as manually activated locking devices, padlocks, card reader access, biometric devices/systems, and "controlled" entry points.
- Ensuring the access control system incorporates measures to prevent unacceptable practices such as "pass back" or "tailgating".
- Assigning individual personal identification number (PIN) codes if used in conjunction with an access control system.
- Removing access rights for individuals as soon as access is no longer required.
- Restricting access rights to the access control management system and software, to prevent unauthorized in-

terference with the system database (hacking, software sabotage).

- Implementing a means of duress signaling near the source storage, to provide notice to the alarm monitoring company or response personnel.

- Implementing a local alarm that triggers in the vicinity of the storage area, to alert nearby personnel of an intrusion or other problem in the source storage area.

### 4.8.4 Response

The authorized person or applicant 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:

a. Attempted or successful unauthorized removal or loss of radioactive sources;

b. Attempted or actual sabotage.

c. Unauthorized transfer or transport of radioactive sources.

d. Unauthorized access to secured area.

e. Failure or loss of a security system or failure of multiple systems that are essential for the security of radioactive sources.

f. Loss or unauthorized disclosure of sensitive information.

g. 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.).

## 4.9. Security Event Reporting

For security events identified in section 4.8.4, the authorized person or applicant should describe the mechanism for notification and reporting security events to the NRRC in accordance with Regulation on Security of Radioactive Materials (NRRC-R-17) as well as the information of local law enforcement agencies (such as Police). The format for security event notification is given at Annex-II.

## 4.10. Safety and Security Interface

The authorized person or applicant should address the 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 authorized person or applicant may describe its arrangements:

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

b. 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.

c. Consideration of the radiation protection program and emergency plan in the development of the security plan in order to ensure compatibility and consistency.

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

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

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

g. 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.

h. Liaison between safety and security personal to ensure co-ordination and integration of security plan with emergency plan.

i. 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.

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

## 4.11. Training Program

The authorized person or applicant should describe the training and retraining program (i.e., annual retraining) for its personnel having security related responsibilities.

Guidance for training program is demonstrated in the following subsections:

### 4.11.1 Security Officer

Security officers should be properly equipped and trained. A formal training program should be established that is specific to the security officers. The training program should include:

- Requirements of local rules/ regulations (if applicable).
- Legislation and authorities.
- Knowledge of the site.

- Roles, responsibilities, and functions.
- Radiation protection emergency procedures and response protocols.
- First-aid training techniques.

For security officers, the authorized person or applicant should establish and maintain an overall training policy as well as initial and continuing training programs, based on the long-term qualifications and competencies required for performing the job, and training goals that acknowledge the critical roles of safety and security.

**4.11.2 Security Awareness Program**

The security awareness training should include instructions on security practices/procedures to protect radioactive materials and prescribed information, and on reporting suspicious events or security incidents (including during transport).

At a minimum, the security awareness program should:

- Ensure that staff understand their roles and responsibilities for security.
- Ensure that staff are trained to recognize and report suspicious activity, for example:
  - o using false identification
  - o individual exhibiting suspicious behavior
  - o individual causing an alarm without authorization.

o lost or stolen uniforms or material within the organization

o unsafe behavior at the workplace

- Ensure protection of prescribed and/or sensitive information
- Include training on measures for identifying suspicious activity and/or behavioral changes in personnel or contractors/ subcontractors.

## 4.12. Maintenance Program

The authorized person or applicant should describe the 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.

The authorized person or applicants should ensure reliability through a preventive maintenance program that tracks detection device deficiencies. When the device is out of service for repair or replacement, compensatory measures must be implemented.

## 4.13. Drills and Exercises

The authorized person or applicant should describe the arrangements for drills and exercises to test the effectiveness of security measures and appropriate response measures against security events mentioned in section 4.8.4. This section should also include the frequency of such drills and exercises that depends on the category and risks associated with the radioactive material (e.g., quarterly, or annually).

## 4.14. Implementing Procedures

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

a. Access authorization;

b. Key and lock control;

c. Alarm assessment and initiation of response;

d. Physical verification of inventory;

e. Receipt, transfer and transport of radioactive sources;

f. Operation and maintenance of security systems;

g. Coordination and communication with relevant organizations in case of security event;

h. Security event reporting;

i. Drills and exercises for evaluation of security system effectiveness; and Protection of sensitive information.

## 4.15. Review and Revision of Security Plan

The authorized person or applicant should describe the process for periodic review and revision of its approved security plan. The basis for revision of security plan could be the following:

a. Whenever, there is a change in the application or location of radioactive sources;

b. To address new threat information;

c. Changes in the regulatory requirements;

d. After testing and evaluation of the security plan;

e. Prescribed interval defined in the security plan; or

f. As deemed necessary by the NRRC.

### 4.16. Transport of Radioactive Sources

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

- The authorized person or applicant should address the description of shipment (type and 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 authorized person or applicant should provide details of the dedicated transport vehicle. The dedicated transport vehicle should comply with security requirements including securing mechanism of source, reliable communication means, tracking system etc.

- The authorized person or applicant should also specify primary and alternate routes, where applicable, and associated in-transit storage.

- The transport security plan should include; where applicable with each category specified in Regulation on Security of Radioactive Materials (NRRC-R-17), the following general information:

a. Contact information for the authorized person or applicant including the following.

- The complete legal name and business address of the authorized person or applicant who is submitting the plan.
- All relevant contact information, such as telephone number, mobile phone number, and email address.

b. The name, quantity, chemical and physical characteristics of each of the radioactive sources being transported including the following:

- A description of the radioactive source and device.
- The category and quantity of the radioactive source being transported.

c. Roles and responsibilities of the authorized person or applicant's personnel, consignors, and carriers taking the following into consideration:

- A description of who is responsible for security and the transport security plan (name and title)
- Ensuring that security-related information is communicated to the consignors and carriers engaged in the transport of the radioactive source(s). If transport is subcontracted, the authorized person or applicant should ensure contractual arrangements exist for developing the security plan.

d. Mode(s) of transport including the following:

- A description of all types of transport used to convey the radioactive source(s) from the time the shipment leaves its originating location until it is delivered at its intended destination.

- Includingthe date, time and location of any planned transfers and the contact information (name, job title, and telephone number) for all persons responsible for ensuring the successful transfer of the radioactive sources and for verifying the integrity of the associated shipments.

e. The proposed security measures including the following:

- A description of the measures used to monitor the movement of packages and/or conveyances containing radioactive sources (e.g., global positioning system, vehicle or package tracking and monitoring system)

- A description of the measures used for escort, security searches, and procedures with response force in case of breakdown or a failure of the shipment to arrive at its destination at the expected time.

- A description of the procedures to be followed during any schedule stop, or unscheduled delay during transport.

f. Measures to monitor the location of the shipment.

g. Provisions for information security

- A description of how the information will be protected.
- A description of how this information will be communicated to individuals who need to know this information to perform their duties.

h. The communication arrangements made between the authorized person or applicant, the carrier, and the consignee including the following:

- A description of the communication arrangements between the authorized person or applicant, the consignor, the operator of the vehicle transporting the radioactive source, and the response force along the transport route.
- A description of how the authorized person or applicant plans to ensure that communication coverage is adequate along the entire route.
- Indicate the action to be taken if communication contact with a vehicle carrying a radioactive source is lost.

i. Communication arrangements made with any police agency along the transportation route taking the following into consideration:

- The authorized person or applicant should ensure that all responsible police agencies along the transportation route are notified prior to transporting the shipment.

- The consignor should notify the consignee, in advance, of the shipment's departure time, the mode of transport, the expected delivery time and the allowable delivery period around that delivery time

- The consignee should notify the consignor of receipt non-receipt of the shipment within the expected delivery period.

j. The planned route including the following:

- If the proposed route is to pass through an urban area, the authorized person or applicant should describe the precise route to be taken through the area and how the shipment is to be scheduled to avoid peak traffic times.

- Include alternate routes to be used in case of an emergency.

## 4.17. Documentation and Records

The authorized person or applicant should maintain proper documentation and records for all security related information. The documentation and records should be made available based on the need-to-know basis within the authorized activity and or facility that are defined by security arrangement and procedures.

Documentation and records will also be a compliance reference between the authorized person or applicant and the NRRC.

## 5. Related Documents and Files

| ABBREVIATION | DEFINITION | Document Number | Relation to the Procedure |
|---|---|---|---|
| Regulation on Radiation Safety | Technical Regulation | NRRC-R-01 | Sets out the general safety requirements in ensuring the protection of people and the environment against the harmful effects of ionizing radiation and for the safety of radiation sources. |
| Regulation on Security of Radioactive Materials | Technical Regulation | NRRC-R-17 | Presents the requirements for the security of radioactive materials throughout their life cycle against unauthorized removal of the radioactive material and sabotage |

## Annex-I: Guidance Checklist for Development of Security Plan for Radioactive Material

| Guidance Checklist for Development Of Security Plan for Radioactive Material | | | | |
|---|---|---|---|---|
| **No** | **Item** | **Yes** | **No** | **Notes** |
| 1. | Facility Description | | | |
| 2. | Radioactive Source Description, Categorization, and their Corresponding Security Levels | | | |
| 3. | Map of the Secured Area | | | |
| 4. | Organizational Structure and Responsibilities | | | |
| 5. | Personal Trustworthiness and Reliability | | | |
| 6. | Protection of Sensitive Information and Computer System | | | |
| 7. | Technical Security Measures | | | |
| 8. | Detection Measures | | | |
| 9. | Delay Measures | | | |
| 10. | Response Measures | | | |
| 11. | Access Control | | | |
| 12. | Security Event Reporting | | | |
| 13. | Safety and Security Interface | | | |

| Guidance Checklist for Development Of Security Plan for Radioactive Material | | | | |
|---|---|---|---|---|
| **No** | **Item** | **Yes** | **No** | **Notes** |
| 14. | Training/ Retraining Program | | | |
| 15. | Maintenance Program | | | |
| 16. | Drills and Exercises | | | |
| 17. | Implementing Procedures | | | |
| 18. | Review and Revision of Security Plan | | | |
| 19. | Transport of Radioactive Sources | | | |

# Annex-II: Nuclear Security Event Notification Form

**نموذج إشعار بالحوادث الأمنية النووية**
**NUCLEAR SECURITY EVENT NOTIFICATION FORM**

**Date:** **التاريخ:** **Event time:** **وقت الحادثة:**

**الجزء الأول: المعلومات الأساسية والمواد المتعلقة بالاشعار**
**Part-I: Basic Information and Materials Involved**

| | | | |
|---|---|---|---|
| **اسم المرخص له** Licensee Name | | **رقم الرخصة** License Number | |
| **تاريخ الحادثة** Incident Date | | **المنطقة** Region | |
| **المدينة** City | | **نوع الاستخدام** Use | |
| **نوع المنشأة** Facility Type | ☐ Irradiators التشعيع<br>☐ Radiotherapy: العلاج الإشعاعي<br>☐ Brachytherapy العلاج الإشعاعي الموضعي<br>☐ Industrial Radiography التصوير الصناعي<br>☐ Industrial Gauges أجهزة القياس النووية<br>☐ Oil Well Logging سبر غور الابار<br>☐ Calibration Sources مصادر عيارية<br>☐ Other اخرى (Please specify) | **نوع الحادثة** Nature of Event | ☐ Source lost or stolen. فقدان أو سرقة المصدر<br>☐ Attempted or actual sabotage محاولة أو إجراء عمل تخريبي<br>☐ Unauthorized transfer or transport نقل غير المصرح به<br>☐ Unauthorized access to secured area الوصول غير مصرح به إلى المنطقة الأمنية<br>☐ Failure of essential security systems فشل في أنظمة الأمن الداخلي للمنشأة<br>☐ Loss of sensitive information فقدان المعلومات الحساسة<br>☐ Other اخرى (Please specify) |
| **احداثيات الموقع** Location Coordinates | | **أخرى** Other | |
| **تفاصيل الموقع** Location Details | | **تصنيف المادة** Material Classification | **أخرى** Oher |

**Materials involved in the incident** **المواد المتعلقة بالحادثة**

| **النويدة** **Nuclide** | **النشاط الاشعاعي** **Activity** | **معدل الجرعة** **Dose Rate** | **معلومات إضافية** الوصف الكيميائي، الوصف الفيزيائي، الاستخدامات **Additional Details (Description)** | **الفئة** **Category** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

| الجزء الثاني: معلومات إضافية<br>Part-II: Additional Information | |
|---|---|
| Incident Summary ملخص الحادثة | |
| | |
| Additional Information regarding response actions معلومات إضافية بما يتعلق بالإجراءات المتخذة | |
| | |
| Name of Incident Reporter اسم المبلغ | Contact info. معلومات التواصل |
| | |
| Date التاريخ | Signature التوقيع |
| | |

**King Fahd National Library Cataloging-in-Publication Data**

**L.D. no. 1445/24443**
**ISBN: 978-603-92074-6-7**

هيئة الرقابة النووية والإشعاعية
Nuclear and Radiological Regulatory Commission

Kingdom of Saudi Arabia

@saudinrrc

nrrc.gov.sa