

UNITED REPUBLIC OF TANZANIA



MINISTRY OF EDUCATION
SCIENCE AND TECHNOLOGY

TANZANIA ATOMIC ENERGY COMMISSION



PROPOSED GUIDANCE ON SITE SECURITY PLAN PREPARATION

Document Title:	Guide for Site Security Plan Preparation		
Document Number	TAEC/RCD/103	Version No:	1.0
Issue Date:	August 2026	Review Date:	July 2029

FOREWORD

Tanzania Atomic Energy Commission, established under the Atomic Energy Act No. 7 of 2003 (here in after called "the Act") of The United Republic of Tanzania, is the official government body responsible for regulating the peaceful use of atomic energy in the country. Under section 6 (c) and (e) of the Act, Tanzania Atomic Energy Commission (TAEC) is authorised to establish or adopt in consultation with a competent body inside and outside the country, Guides of Safety for the protection of health and minimization of danger to life and property; and to provide for the applications and supervision of these guides in all undertakings or practises involving the use of atomic energy and radiation sources.

This Guide was developed to assist the Registrants/Licensees/operators for preparation of Site Security Plan (SSP). This guide includes the recommended structure and content for each topic. Users of this guidance should also ensure adherence to the requirements of the Atomic Energy (Security of Radioactive Sources, Nuclear Materials and Nuclear Facilities) Regulations 2022. The Guide was prepared by the Tanzania Atomic Energy Commission with the assistance of the International Atomic Energy Agency. For its effective operation, this Guide will be revised as and when necessary in the light of experience and feedback from users as well as new developments in the field.

EXECUTIVE SUMMARY

This Guide was prepared to provide guidance to operators for preparation of Site Security Plan (SSP) for security of radiation sources in their facilities and has contained the recommendations that can be used in establishing, implementing and maintaining nuclear security regime at their sites. The guide was prepared to comply with International Code of Conduct on the Safety and Security of radioactive sources, Nuclear Security Recommendations on radioactive material and associated Facilities (IAEA Nuclear Security Series No. 14), Security of Radioactive Material in use and storage and Associated Facilities (IAEA Nuclear Security Series No. 11-G) and the Atomic Energy (Security of Radioactive Sources, Nuclear Materials and Nuclear Facilities) Regulations 2022. The aim is to ensure that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts/use.

For effective security plan, this Guide requires documentations of the design, operation, and maintenance of the entire security system as well as application of the various security management elements and supports the development of an effective security culture. Security plans are site-specific and therefore an operator with multiple facilities may be needed to develop individual security plans for each, clearly describing any inter-relationship between them. To be operationally effective, the security plan should be routinely reviewed, evaluated, and updated.

The guidance on site security preparation is intended only for all persons/organizations involved in the use/handling of sealed and unsealed radioactive materials in medical diagnosis, therapy, radioactive waste Management facilities and research facilities.



.....
Prof. Najat K. Mohammed
Director General

Contents

1. Introduction.....	6
1.1 Requirements	6
1.2 Objective of the Security Plan.....	6
1.3 Scope	6
1.4 Preparing and Updating of the Security Plan.....	7
2. The Facility	7
2.1 Overview	7
2.2 Radioactive Sources	7
2.3 Categorization and Security Level	8
2.4 Physical Description.....	8
2.5 Operational Description	9
3. Security Management.....	9
3.1 Roles and Responsibilities	9
3.2 Training and qualifications.....	9
3.3 Access Authorization.....	10
3.4 Trustworthiness	10
3.5 Information Protection.....	11
3.6 Maintenance Program.....	11
3.7 Budget and Resource Planning	12
3.8 Evaluation for Compliance and Effectiveness	12
4. Security System	12
4.1 Threat Information.....	13
4.2 Security Assessment Methodology.....	13
4.3 Security System Design.....	13
4.4 Access Control.....	13
4.5 Detection, Assessment, and Delay Measures.....	14
5. Security Procedures.....	14
5.1 Routine, Off-shift, and Emergency Operations	14
5.2 Opening and Closing of Facility	14
5.3 Key and Lock Control.....	15
5.4 Accounting and Inventory	15
5.5 Acceptance and Transfer.....	16
6. Response.....	16
6.1 Security Events.....	16
6.2 Communications.....	17
6.3 Security Event Reporting.....	17

6.4	Security during Emergencies and Contingencies.....	17
6.5	Increased Threat Level	17
7.	Management of Disused sources	18
7.1	Regulatory requirements	18
7.2	Planned disposition.....	18
7.3	Storage pending disposal.....	19
8.	References.....	19
9.	Appendices	19

1. Introduction

This section should describe why security plan is required, what objectives it satisfies and any scope consideration. The section shall cover three subsections 1.1 - 1.4 below.

1.1 Requirements

This section should describe the regulatory requirements to be satisfied by the site security plan, such as:

- a) adequately protecting radioactive sources against unauthorized removal and sabotage;*
- b) Meeting regulatory requirements; and*
- c) Integrating with organizations general requirement system.*

1.2 Objective of the Security Plan

This section should describe the objectives to be met by the security plan, such as:

- a) document the design and operation of the security system;*
- b) document the design and operation of the security management measures;*
- c) demonstrate regulatory compliance; and*
- d) provide operational requirements and guidance from management and staff.*

1.3 Scope

This section should describe the coverage of and any exclusion from the security plan and shall explain the relationship of the security plan to other related documents or arrangements such as:

- a) management systems;*
- b) facility operations;*
- c) radiation protection; and*
- d) emergency preparedness and response.*

1.4 Preparing and Updating of the Security Plan

This section should state the frequency and reasons for reviewing and /or updating the security plan.

Example: -

- a) at a review interval prescribed by Atomic Energy (security of radioactive materials, nuclear materials and Nuclear facilities) Regulations 2022; and*
- b) as necessary to address the threat information, changes in facility operations and any other developments that could affect the performance of the security system.*

2. The Facility

This section should describe the radioactive sources(s) and their location(s) that need protection, the level of protection required, and the physical and operational environment that affects such protection. The section shall be divided into subsection 2.1- 2.5 as shown bellow

2.1 Overview

This section should describe the purpose or mission of the facility and its operating organization. It should include the following:

- a) types of practices involving radioactive sources; and*
- b) associated devices or equipment.*

2.2 Radioactive Sources

This section should provide details of radioactive sources and associated equipment or devices, including the following:

- a) radionuclide, activity and reference date;*
- b) chemical and physical form; and*
- c) serial number, brand, model and manufacturer.*

Example of the table showing the list of radioactive sources

Source	Activity (TBq)	Activity Date	IAEA Category	Description/Location
⁶⁰ Co	227	12/101/2011	1	Leksell Gamma knife 24001, research building wing 2

2.3 Categorization and Security Level

This section should identify and explain the basis for categorization of radioactive sources and their security level in line with the requirements of Atomic Energy (security of radioactive materials, nuclear materials and nuclear facilities) Regulations 2022.

Example of the table showing source category and security level

Category	A/D	Practice/equipment	Security level
1	$A/D \geq 1000$	a) Radioisotope thermoelectric generators b) Irradiators c) Teletherapy	A
2	$1000 > A/D \geq 10$	a) Industrial gamma radiography b) High dose brachytherapy	B
3	$10 > A/D \geq 1$	a) Fixed industrial gauge with high activity sources b) Well-lodging gauges	C

2.4 Physical Description

This section should describe the physical features of the facility diagrams maps and photograph. It should include the following: -

- a) location and layout of the facility including the location of sources;
- b) surrounding environment such as industrial, commercial, residential or other uses;

- c) distance to nearest police stations and other services; and*
- d) proximity to buildings, roads and other features of security or operational interest.*

Note to include the layout structure/diagram of the facility

2.5 Operational Description

This section should provide a description of the facility operations that include: -

- a) facility working and non-working hours;*
- b) the number and type of staff involved in the facility operations; and*
- c) typical number and type of other people like visitors, public, customers, service personnel or contractors who may be at the facility during scheduled operations or at any other time.*

3. Security Management

This section should describe the facility's security management measures for radioactive sources. The section should be divided into section 3.1 - 3.8 as shown below:

3.1 Roles and Responsibilities

This section should identify positions within the organization that have general or specific responsibilities for security. Should also describe their roles and responsibilities to included:

- a) leadership, management, and supervisors;*
- b) positions for which the security of radioactive sources is the main job e.g. Guards;*
- c) positions with responsibility for regulatory matters like medical technicians etc.; and*
- d) positions responsible for information security and network infrastructures.*

Note to use organization chart or tables

3.2 Training and qualifications

Use the information provided in 3.1 to describe the following: -

- e) the qualification of staff in the security roles;*
- f) Initial and refresher courses/training needed to be provided - **should indicate who provides the training and at what frequencies;** and*
- g) records that documents satisfactory completion of training.*

3.3 Access Authorization

This section should describe the process for authorizing personnel for unescorted access to secured areas or security sensitive areas:

The section shall include the description for:

- a) Identifying the positions requiring unescorted access;*
- b) identifying positions requiring access to component and network segments associated with physical protection system (PPS);*
- c) confirming trustworthiness of staffs has been verified;*
- d) Verify individuals have the necessary qualifications and training;*
- e) Maintaining up to date records of personnel authorized for unescorted access; and*
- f) withdrawing access authorization when personnel no longer have need for unescorted access, such as transfer of job responsibilities, or termination of employment.*

3.4 Trustworthiness

This section should describe the process to evaluate trustworthiness to determine whether they should be granted unescorted access to radioactive sources, secured areas, and/or security-sensitive information as per the requirements of the Atomic Energy (security of radioactive materials, nuclear materials and Nuclear facilities) Regulations 2022

The process should indicate requirements for periodic review and any re-evaluation for particular circumstances, the method by which each individual is

evaluated and may include referral to law enforcement or other external agencies.

- a) should identify applicable requirements regarding trustworthiness;*
- b) indicate the evaluation method used; and*
- c) state what record are maintained and kept confidential as part of trustworthiness evaluation.*

3.5 Information Protection

This section is potential to compromise security if information is disclosed to non-authorized person. The section should describe:

- a) information that require protection (hard copy and digital);*
- b) specific forms of protected information (paper, electronic, media etc.);*
- c) how protected information is marked, handled and stored;*
- d) who has access to particular information and how this access is determined;*
- e) protection measures used to prevent unauthorized access;*
 - ◆ *when information is being used or stored*
 - ◆ *when information is being produced or transmitted*
- f) how potential information destroyed when no longer required.*

3.6 Maintenance Program

This section should describe the maintenance program that will include:

1. Approaches used to:

- a) contract with outside vendor;*
- b) use qualified facility technicians; and*
- c) use combination of facility technician and outside vendors.*

2. Chosen approach practicability and cost effectiveness based on:

- a) roles and responsibilities of staff and contractor;*

- b) master equipment and spare parts list with warranty information;*
- c) Schedule of preventive maintenance activities;*
- d) plans for dealing with component failures including response times and identification of compensatory measures;*
- e) maintenance records ;*
- f) equipment replacement planning; and*
- g) program for Cyber hygiene.*

3.7 Budget and Resource Planning

This section should describe the process to budget for all security activities and elements including: -

- a) human resources;*
- b) training;*
- c) technical means of o security-related;*
- d) equipment maintenance; and*
- e) other activities associated with security management.*

3.8 Evaluation for Compliance and Effectiveness

This section should describe the process for periodic evaluation of the security program to assess:

- a) the facility's compliance with Atomic Energy (security of radioactive materials, nuclear materials and Nuclear facilities) Regulations 2022, license conditions and other regulatory requirements;*
- b) effectiveness of security system in protecting radioactive sources;*
 - ◆ *detecting weakness through performance tests and other means*
 - ◆ *how identified weaknesses are addressed*

- c) *the section should also include the description of frequency, scope and record keeping practices.*

4. Security System

This section should describe how the current security system was designed and is being implemented to comply the established law. This section should include: -

4.1 Threat Information

- a) *This section should describe how the facility obtains and uses threat assessment information;*
- b) *Describe the information in sufficient detail to indicate how the security system is designed to protect against both external and insider threats, as applicable; and*
- c) *Should provide information on who is responsible for receiving threat information, including notification and how such information is appropriately shared with site personnel who have a need to know.*

4.2 Security Assessment Methodology

- a) *This subsection should describe the process or methodology used to evaluate the security system and assess its vulnerabilities;*
- b) *Should indicate the results of the initial security assessment as input to the security system design (see previous section); and*
- c) *Should the periodic updates as part of the security plan review and licensing requirements, and modifications when necessary to address new threat information, changes in site operations, or any other development that could affect security system performance or vulnerabilities.*

4.3 Security System Design

This section should describe how the security system has been designed to provide the required level of protection including the application of the graded approach, defense in depth and balanced protection:

- a) *Should describe also security layers and associated measures for access control, delay and detection and measurement.*

4.4 Access Control

This section should describe the *physical measures for controlling access* indicating: -

- a) *How personnel are physically controlled at each control point to limit unescorted access only to authorized persons; and*
- b) *Specific means used to authenticate the identity of authorized persons*

4.5 Detection, Assessment, and Delay Measures

For each secured area should describe

- a) *Barriers (delay measures) to increase adversary task time relative to response timeline;*
- b) *Means of detection at each barrier, including intrusion detection system and observation by personnel as applicable; and*
- c) *Method of assessment including people and equipment including the people and equipment supporting the assessment, such as:*
 - i. *CCTV camera monitoring and switching systems;*
 - ii. *Central alarm stations;*
 - iii. *Guard or response forces both internal and external;*
 - iv. *Computer and recording systems;*
 - v. *Security lighting;*
 - vi. *Electrical and back-up power sources.*

Note to describe and map the integration with physical protection measures

5. Security Procedures

This section should describe the written procedures to be followed by responsible personnel (actual procedures should be standalone documents and could be included in an appendix). It should contain 5.1-5.5 sections as shown below.

5.1 Routine, Off-shift, and Emergency Operations

This section should describe how assigned personnel, such as staff and contractors, must operate security systems and discharge other security-related responsibilities during:

- a) Routine operations;*
- b) Off-shift (after-hours) operations when staff are not ordinary present; and*
- c) Emergency operations when a security-related or other emergency occurs.*

5.2 Opening and Closing of Facility

This section should describe procedures for opening and closing secured such as:

- a) Unlocking and locking doors;*
- b) Communications with alarm station to deactivate detection systems; and*
- c) The procedure should also include who is responsible, and should take action to be to validate that other delay mechanisms have been appropriately secured.*

5.3 Key and Lock Control

This section should describe the procedures used for control of all keys, locks, combinations, passwords, and related measures for controlling access to secured areas and security systems.

The procedure should specifically describe the following:

- a) Specific conditions that require access control measures to be changed, such as compromise of a combination of password, or loss of a key; and*

- b) Who is responsible for making such changes*

5.4 Accounting and Inventory

This section should describe how periodic accounting for each radioactive sources is performed, including:

- a) frequency of inventory and accounting activities;*
- b) accounting method used, such as a physical check, examination of seals or radiation measurements;*
- c) records generated, indicating results of each verification, when, by whom, and by what method; and*
- d) arrangements for corrective actions and reporting if the presence of radioactive sources cannot be verified.*

The section should also describe how the inventory of radioactive sources maintained with the following:

- a) Details of radioactive sources and associated equipment;*
- b) Use history;*
- c) Receipt, transfer, or disposal of the source;*
- d) Notifying the regulatory authority of inventory changes; and*
- e) Reporting to the regulatory authority at prescribed intervals.*

5.5 Acceptance and Transfer

This section should describe the procedures to be followed to ensure proper security during acceptance and transfer of radioactive sources including:

- a) Prior approval for transfer and shipping sources; and*
- b) Security measures while the source is moved through the facility for shipment nor acceptance.*

6. Response

This section should describe arrangements for responding to a security events. Sections 6.1-6.5 should describe arrangements for responding to a security event as follows.

6.1 Security Events

This section should describe arrangements with designated response authority for responding to a security event, including:

- a) responsible person within the operator organization for making such arrangements;*
- b) designated responsible authority such as local law enforcement;*
- c) confirmation of a visit by responsible authority to become familiar with radioactive sources, associated equipment and devices, security system and security management measures;*
- d) means to notify response authority following detection and assessment of an alarm;*
- e) confirmation that response authority understands threats responders should be prepared to encounter;*
- f) estimated response time obtained from the response authority;*
- g) any resulting modifications to the security system to provide sufficient delay to enable a timely response;*
- h) any specific actions to be taken by staff to facilitate a response based on the agreement with the response authority;*
- i) arrangements for response exercise, with participation of the operator. Response authority and regulatory authority; and*
- j) how the site information technology staff will assess network intrusion detection events or unusual network activity to determine potential threat.*

6.2 Communications

This section should describe arrangements available with response authority, including:

- a) means of communication, such as mobile duress buttons, fixed duress switches, radios, landline telephones, cellphones, network, etc.; and*
- b) programming for immediate communication to response authority's;*
- c) testing and maintenance to ensure effective operability.*

6.3 Security Event Reporting

This section should describe how security events are documented in a report to the regulatory authority after they occur, including:

- a) who is responsible for preparing the reported;*
- b) time by which the report must be submitted to TAEC; and*
- c) how the security system, security management measures, and response management are reviewed to determine cause of event, identify weaknesses, or vulnerabilities and make any necessary improvements.*

6.4 Security during Emergencies and Contingencies

This section should describe how sources are secured in a non-security emergency such as fire, earthquake, flood, or hurricane, including arrangements:

- a) to evaluate status of the security system;*
- b) to implement compulsory measure in the event of security system failures; and*
- c) to avoid endangering personnel safety.*

6.5 Increased Threat Level

This section should describe plans for addressing an increased threat level, including:

- a) *immediate measures, such as deploying additional guards, changing key codes, alerting staff to additional risks, testing security equipment, and meeting with response authority to review response arrangements; and*
- b) *modification of the system, such as installing additional security cameras, new/additional locks, new/additional alarm systems, or structural changes to the facility.*

7. Management of Disused sources

This section should describe arrangements for managing the facility and radioactive sources when they become disused, including:

7.1 Regulatory requirements

This section should describe the requirements of Atomic Energy (Security of Radioactive Materials, Nuclear materials and Nuclear facilities) Regulations 2022, license conditions for managing the facility's radioactive sources once they become disused, and briefly indicate how they are being addressed:

- a) *permissible/preferred disposition pathways including returning to supplier, reuse/recycle or long term storage and disposal;*
- b) *require to have financial and contractual arrangements;*
- c) *required to have financial and contractual arrangements; and*
- d) *set limits on short term storage duration and location.*

7.2 Planned disposition

This section describe arrangements for offsite disposition for each radioactive source once becomes disused, including the following:

- a) *Planned dates (circumstances) when sources will no longer be used;*
- b) *Disposal pathways;*
- c) *Financial arrangements (how disposal will be paid for);*
- d) *Contractual arrangements; and*
- e) *Transport arrangements.*

7.3 Storage pending disposal

Describe how each source will be arranged once it becomes disused but before its disposition (as applicable):

- a) State the short term storage location i.e. if same location where source was used or dedicated short term storage onsite or others;*
- b) Specify security measures will be applied; and*
- c) State the planned duration of short term storage.*

8. References

List any documents referred to in the security plan or that are needed to explain or expand on details in the plan, such as

- a) specific regulations;*
- b) regulatory license;*
- c) operating manuals;*
- d) organizational policies and manuals.*

9. Appendices

Provide list of procedures stated in the security plan, including their dates and version.