

Guidance on the Contents of a Facility Security Plan

The purpose of this document is to provide guidance primarily to operators for the preparation of a facility security plan. This includes the recommended topics, organization and a description of the content for each topic. Users of this guidance should also take into account when drafting a security plan any national or regulatory requirements.

The facility's security plan describes the security system in place to protect the operator's radioactive sources. It provides the means by which the operator integrates all security management elements with the overall security system and with the operator's broader management system to ensure that the security system is effectively operated, reliably maintained and in compliance with applicable regulatory requirements. An effective security plan documents the design, operation and maintenance of the entire security system, as well as the application of the various security management elements and supports the development of an effective security culture. Security plans are facility-specific and an operator with multiple facilities may need to develop individual security plans for each, clearly describing any inter-relationship between them. In order for a security plan to be operationally effective, it should be routinely reviewed, evaluated and updated. This process in turn instills and promotes a strong security culture.

Contents

1.	Introduction.....	2
1.1	Requirements	2
1.2	Objective of the Security Plan	2
1.3	Scope.....	3
1.4	Preparing and Updating of the Security Plan.....	3
2.	Facility Description.....	3
2.1	Overview.....	3
2.2	Radioactive Sources.....	3
2.3	Categorization and Security Level.....	3
2.4	Physical Description	3
2.5	Operational Description	4
2.6	Regulatory Requirements.....	4
3.	Security Management	4
3.1	Roles and Responsibilities	4
3.2	Training and Qualification.....	4
3.3	Access Authorization	5
3.4	Trustworthiness.....	5
3.5	Information Protection	5
3.6	Maintenance Programme	6
3.7	Budget and Resource Planning	7
3.8	Evaluation for Compliance and Effectiveness	8

Workshop for Drafting Site Security Plans Based on Model Security Plan
GUIDANCE ON CONTENTS OF A FACILITY SECURITY PLAN

4.	Security System	8
4.1	Threat Information	8
4.2	Security Assessment Methodology	8
4.3	Security System Design	9
4.4	Access Control	9
4.5	Delay, Detection and Assessment Measures.....	9
5.	Security Procedures	10
5.1	Routine, Off-shift and Emergency Operations.....	10
5.2	Opening and Closing of Facility	10
5.3	Key and Lock Control.....	10
5.4	Accounting and Inventory.....	10
5.5	Acceptance and Transfer.....	11
6.	Response	11
6.1	Security Events	11
6.2	Communications	11
6.3	Security Event Reporting.....	12
6.4	Security during Emergencies and Contingencies.....	12
6.5	Increased Threat Level.....	12
	References	12
	Appendices	12

1. Introduction

This section should describe why the Security Plan is required, what objectives it satisfies and any scope considerations.

1.1 Requirements

Describe the need for the Security Plan considering the particular facility's circumstances, such as: (a) satisfying the need to adequately protect radioactive sources against the threat of unauthorized removal or sabotage; (b) satisfying regulatory requirements; and (c) being part of, and integrated with, the organization's integrated management system.

1.2 Objective of the Security Plan

Describe the objectives to be satisfied by the Security Plan such as: (a) to document the design and operation of the security system and security management measures according to applicable methods, criteria and requirements; (b) to demonstrate regulatory compliance by specifying in each relevant section which particular regulatory requirement is met; and (c) to serve as an operational tool used by management and staff to integrate people, procedures and equipment into an effective security system.

1.3 Scope

Describe the coverage and any limitations of the Security Plan and its relation to other relevant documents or arrangements such as any management, operational, radiation protection or emergency matters. Reference should also be made to areas where security interacts with or impacts other management systems, especially those for safety.

1.4 Preparing and Updating of the Security Plan

Describe the process for developing, approving and updating the Security Plan, as well as its revision history within the organization's document control or quality management system. Describe how this Security Plan is reviewed and updated, at a prescribed interval specified by the regulatory body, as applicable, and as necessary to address new threat information, changes in facility operations, or any other development that could affect the performance of the security system.

2. Facility Description

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.

2.1 Overview

Describe the purpose or mission of the facility and its operating organization, including the types of practices involving radioactive sources and associated devices or equipment.

2.2 Radioactive Sources

Provide details of the radioactive sources and associated equipment or devices including: radionuclide, activity and reference date, chemical and physical form, serial number, equipment/device brand, model and manufacturer.

2.3 Categorization and Security Level

Identify, and explain the basis for, the categorization of the radioactive sources and the associated security level according to regulatory or other requirements, such as license conditions.

2.4 Physical Description

Describe the physical features of the facility and its surrounding environment, including diagrams and scale floor and building drawings and photographs. These descriptions should include:

- a) the location and layout of the facility, particularly indicating areas accessible to the public; roads and parking areas; nearest public thoroughfares; central security office; building and site perimeter; access points; and physical barriers.
- b) the facility's surrounding environment such as industrial, commercial, residential or other uses; indication of distances to nearest police stations and other response services; proximity to other buildings, roads and other features of security or operational interest, such as other facilities with hazardous materials.

2.5 Operational Description

Provide a description of the facility operations including working and non-working hours; the number and type of staff involved in the facility's operations; the typical number, type, and frequency of other people, such as visitors, public, patients, customers, service personnel or contractors, who may be at the facility during scheduled operations or at any other time.

2.6 Regulatory Requirements

Identify and reference the applicable regulatory requirements based on the type of practice or facility and the type of radioactive sources present. More specific reference to the particular regulatory requirement being satisfied should be given in relevant other sections of the Security Plan by stating the applicable provision of the regulations, license, standards or other requirement.

3. Security Management

This section should describe the security management measures in place and the particular duties of management and staff in ensuring the measures are implemented and effective.

3.1 Roles and Responsibilities

Assign and document all roles and responsibilities with respect to the performance of each security activity and function, including the roles and responsibilities of:

- a. facility leadership, management, supervisors, staff, and contract or casual personnel;
- b. positions directly responsible for facility security;
- c. positions with responsibility for regulatory matters, including any positions prescribed by the regulatory body such as the licensee, radiation safety officer, security personnel, advisers or guards.

Provide an organizational chart, schematic or tables showing the staffing structure with lines of authority and supervision to demonstrate how the security organization and responsibilities fit within the overall facility organization.

3.2 Training and Qualification

Using the information on positions with security responsibility from section 3.1, describe:

- a. establish requirements for qualification of staff with security responsibilities, noting any specific qualifications required by regulations or license conditions;
- b. training to be provided to each individual, including the required initial, specialized, advanced or refresher training for each position with security responsibilities; security awareness training for all staff; and any other relevant specific on-the-job training such as those involving procedures and work instructions;
- c. provider(s) of the identified training and how frequently each piece of training must be conducted;
- d. related training records that document satisfactory completion of all security-related training.

3.3 Access Authorization

Describe the process for authorizing personnel who need unescorted access to the radioactive source location, secured areas, and/or security-sensitive information, in order to perform their duties (which may or may not be directly related to security).

The description should include information on how to:

- a. identify the positions requiring unescorted access
- b. verify that the individuals holding the identified positions are trustworthy (see next section)
- c. verify that the individuals holding the identified positions have the necessary qualifications and training (see previous section)
- d. perform the timely withdrawal of access for individuals who no longer require it
- e. conduct periodic review and re-evaluation for particular circumstances, such as withdrawing access authorization when personnel or positions no longer have need for unescorted access, transfer of job responsibilities or termination of employment
- f. maintain up-to-date records of personnel authorized for unescorted access.

3.4 Trustworthiness

Describe the process to evaluate the trustworthiness and reliability of personnel in order to determine whether they should be granted unescorted access to radioactive sources, secured areas and/or security-sensitive information.

The process should also indicate requirements for periodic review and any re-evaluation for particular circumstances.

The description should:

- a. identify the individuals whose trustworthiness must be evaluated based on the section above for access authorization
- b. identify the applicable requirements regarding trustworthiness in regulations for the security of radioactive sources, license conditions, or elsewhere, including any requirements that vary depending on security level or other factors
- c. indicate the method by which each individual is evaluated
- d. state what records are maintained and kept confidential as part of the trustworthiness evaluation.

3.5 Information Protection

Based on the potential for certain information to compromise security if disclosed to non-authorized persons, describe:

- a. what information requires protection, as defined by the regulatory body or facility management requirements, including:
 - i. location and inventory of radioactive sources
 - ii. access authorization and access control measures

- iii. security system design, equipment details and diagrams
 - iv. lock combinations and key codes
 - v. threat and vulnerability assessment information
 - vi. temporary or longer term weaknesses in the security system
 - vii. security staffing arrangements
 - viii. the means of response to events or alarms
 - ix. planned dates, routes, and mode of shipment or transfer of radioactive sources
 - x. security plan and procedures, contingency plan, response plan and related arrangements and measures; and
 - xi. privacy information relating to individuals' background checks.
- b. how the protected information is identified such as the use of markings or other designators that will ensure all users of this information recognize it as requiring protection
 - c. the particular forms of the protected information such as paper documents, electronic media, CCTV recording, etc.
 - d. where the protected information is stored and who has custody of it
 - e. who has access to sensitive information and how is that access determined e.g., required to perform job, appropriate level of trustworthiness; see sections 3.3, 3.4
 - f. what protection measures are in place to prevent unauthorized access when the information is being used or is being stored e.g. physical protection, encryption
 - g. what requirements are in place for preventing unauthorized access when the protected information is being reproduced or transmitted within or outside the facility
 - h. how the protected information is destroyed to prevent recovery when no longer needed, including who is authorized to destroy it and by what means the various forms of information will be destroyed.

3.6 Maintenance Programme

Describe the maintenance programme for the security system's equipment to ensure their continuous and reliable operation, including:

- a. The arrangements for performing preventive and corrective maintenance, including the maintenance approach followed, that is, use of: (1) outside security vendors, (2) qualified facility technicians or (3) a combination.
- b. Roles and responsibilities of contractors and facility staff (noting these will be determined by maintenance approach). Specify the roles and responsibilities of facility staff in the maintenance of security equipment. The description of roles and responsibilities should state who has overall responsibility for maintenance as well as who has the responsibility for conducting each particular type of maintenance. If a contractor is employed for the maintenance of security equipment, the description should identify the contract and those major tasks the contractor is required to perform. If a hybrid maintenance approach is used, then this section should describe explicitly who does what.

- c. Master equipment and spare part list, with warranty information. Describe those critical subsystems or components that, in the event of failure, require a long time to procure and would therefore create a vulnerability. The definition of criticality of subsystems or components should be determined by factors such as cost, procurement lead time and resulting degree of security system vulnerability when the subsystem or component is non-operational.
- d. The schedule of preventive maintenance activities for each subsystem or component.
- e. Arrangements for dealing with component failures, including corrective maintenance response time, and identification of compensatory measures required during inoperability. Describe what actions are taken when a subsystem or component fails during normal operation or during testing. The description should include notification procedures and contractor response time as specified in the applicable contract. The description should also outline compensatory measures such as the employment of additional security personnel and or the modification of operational procedures to offset the loss of a technical security measure.
- f. The records and documents which must be created and retained to verify the existence of an ongoing maintenance programme for security equipment. At a minimum the following records should be kept:
 - Routine preventive maintenance actions;
 - Corrective maintenance actions;
 - Equipment warranty records;
 - Equipment malfunction and replacement;
 - Results of operational testing;
 - Identification of trends – for example, nuisance alarm rates, false alarm rates, alarm failures.
- g. A description of the process for routinely evaluating the security system and projecting the retirement and replacement of security system components or the entire system. This information will inform budget and resource planning. At a minimum, identify:
 - Date when equipment was placed into service;
 - Cost of equipment (procurement and installation), identified at both subsystem and component level;
 - Anticipated effective life of the equipment at subsystem and component level.

3.7 Budget and Resource Planning

Resource planning for security should be conducted and implemented at the security system level and reported at the facility level. Summarize how the following activities are conducted:

- a. Establish goals, strategies, plans and objectives for the security system that are consistent with the policies of the organization
- b. Determine the resources necessary to ensure the effectiveness of the security system and provide resources to carry out the activities of the security system, including:

- i. Human resources
 - ii. Training
 - iii. Operational costs of the security system
 - iv. Equipment maintenance - should incorporate information from section 3.6 above on Maintenance Requirements
 - v. All other security related activities.
- c. Provide the necessary resources as required by the security system
 - d. Establish metrics to ensure the effective use of budget and resources
 - e. Regularly review the expenditure of resources against budget and resource projections and ensure that actions are taken to address deviations.

3.8 Evaluation for Compliance and Effectiveness

Describe the process for independently verifying that the facility is in compliance with all applicable security requirements and assessing the effectiveness of the security system to identify any weaknesses that should be corrected and any opportunities for continuous improvement, including arrangements for performance testing.

4. Security System

This section should describe how the current security system is designed and implemented. This description should follow the standard practice of identifying the specific target (the radioactive sources) to be protected, identifying and assessing the threats which the facility is being protected against, describing the security assessment methodology, and providing information on how the design of the security system achieves the required level of protection based on a graded approach and employing the principles of defense in depth and balanced protection. For example, at a Security Level A facility, NSS No. 11 recommends a requirement for a timely response with sufficient resources to interrupt and prevent unauthorized removal.

4.1 Threat Information

The content and process for providing threat information to a facility will vary according to national law and practice. To the extent that threat information is provided, by the regulatory body or others, describe the information in sufficient detail to indicate how the security system is designed to protect against both external and insider threats, as applicable. Information should also be provided on who is responsible for receiving threat information, including notification by the regulatory body or others of a specific threat or of an increased threat, and how such information is appropriately shared with facility personnel who have a need to know.

4.2 Security Assessment Methodology

Describe the process or methodology used to evaluate the security system of the facility and assess its vulnerabilities taking account of the threat information provided. The description should indicate the results of the initial security assessment as input to the security system design (see previous section), the periodic updates as part of the security plan review and licensing requirements, and changes when

necessary to address new threat information, changes in facility operations, or any other development that could affect security system performance or vulnerabilities.

4.3 Security System Design

Based on the target and threat information, describe how the security system has been designed and integrated at the facility level in order to provide the level of protection required taking into account the graded approach and the principles of defence in depth and balanced protection. Describe the security layers and how each secured area and the associated radioactive sources is protected by detection, delay, and response measures in an integrated and balanced way, particularly indicating the design and function of the structural, technical, personnel and organizational measures. This description should include identification of the type of equipment and systems installed and their location.

4.4 Access Control

Describe the physical measures for controlling access, in particular indicating:

- a) how personnel are physically controlled at each access control point to limit access only to authorized persons according to the access authorization procedure and to prevent unauthorized access
- b) specific media used to authenticate the identity of authorized persons such as key card, personal identification number, biometric device, or a combination; and
- c) procedures to be followed by authorized persons to access a secured area including, where relevant, application of the two-person rule.

4.5 Delay, Detection and Assessment Measures

For each of the controlled or secured areas describe:

- a) the barriers (delay measures) used to increase adversary task time relative to response time. Delay measures could include high-security hardened metal doors, high security locks, reinforced grids on large openings or windows into the controlled or secured areas
- b) the means of detection at each barrier including, as applicable, both intrusion detection systems and observation by facility personnel
- c) the method of assessment, including the people and equipment supporting the assessment, such as:
 - CCTV camera monitoring and switching systems;
 - central alarm stations;
 - guard or response forces both internal and external;
 - computer and recording systems;
 - security lighting;
 - electrical and back-up power sources; and
 - communications measures.

5. Security Procedures

This section should describe the written procedures that provide instructions to the responsible personnel for operating and maintaining the security measures. The actual procedures should be stand-alone documents and could be included individually as appendices to the Security Plan.

5.1 Routine, Off-shift and Emergency Operations

Describe how assigned personnel, such as staff and contractors, will operate security systems and discharge their other security-related responsibilities during periods of:

- routine operations
- off-shift or after-hours operations when staff are not ordinarily present, generally at nights, on weekends, and during holidays
- emergency operations.

5.2 Opening and Closing of Facility

Describe the procedures for opening and closing each secured area within the facility, particularly activities such as the unlocking and locking of doors and other barriers, as well as communications with the alarm station to deactivate and activate detection systems. The procedures should identify who within the organization is responsible for opening and closing these areas and should also include actions to validate that other delay mechanisms (e.g. cages) have been appropriately secured.

5.3 Key and Lock Control

Describe the procedures used for control of all keys, locks, combinations, passwords, and related measures used to control access to secured areas and security systems. The procedures should identify who is responsible for changing these access control measures and the specific conditions which require them to be changed, such as the compromise of a combination or password, loss of a security key or termination of a staff member's access.

5.4 Accounting and Inventory

Describe how periodic accounting for radioactive sources, as prescribed by the regulatory body, is performed including:

- a. accounting method used, such as a physical check, remote video monitoring, examination of seals or other tamper-indicating devices, or radiation measurements;
- b. records generated, indicating the results of each verification, when, by whom, and by what method;
- c. requirements for corrective actions and reporting if the presence of radioactive sources cannot be verified.

Describe how the facility's inventory of all radioactive sources is established and maintained including:

- a. location of the sources;
- b. radionuclide;

- c. radioactivity on a specified date;
- d. serial number or unique identifier;
- e. chemical and physical form;
- f. radioactive source use history and any internal movements, as applicable;
- g. receipt, transfer or disposal of the radioactive sources;
- h. other information, as appropriate, to enable the radioactive sources to be identifiable and traceable;
- i. notifying the regulatory body of changes to the inventory within the prescribed period;
- j. reporting the inventory to the regulatory body at prescribed intervals to verify that it is complete and accurate.

5.5 Acceptance and Transfer

Describe the procedures to ensure that the operator maintains security and control of radioactive sources when it is being received from outside a facility and the procedures to ensure that the facility takes the necessary steps to ensure that radioactive sources are provided only to a person authorized by the regulatory body to receive the radioactive sources.

6. Response

This section should describe the response arrangements for security events including their relationship with emergency situations and other contingency situations.

6.1 Security Events

Describe the arrangements among organizational, local and national response forces and their deployment, including target familiarization, response times, capabilities, strategy and tactics. Include an organization chart or schematic showing the management and organization structure, positions which interface with facility operations and security management, and command and control responsibilities. Describe any compensatory measures planned to be available during security events. Identify how periodic testing, evaluation and updating of the response arrangements are undertaken.

6.2 Communications

Describe the communication methods (radio, land lines, etc.) to be used by response forces in communicating with the alarm monitoring station and in establishing command and control during security events, including:

- a. communication methods to be used for all organizations providing response (dedicated facility guards, police, military, etc.), ensuring redundancy of communication capability;
- b. how communication methods will be appropriately tested and maintained to ensure effective operability;
- c. description of the response force communications network and, as applicable, secure networks and linkages to off-site law enforcement or other organizations with which support agreements exist.

6.3 Security Event Reporting

Describe how security events are reported to the facility security organization. Describe how events are documented, who is responsible to document the event, and subsequent external reporting requirements (e.g. reporting to the regulatory body). Specify how security arrangements are reviewed after an event in order to evaluate the effectiveness of the Security Plan and to identify any corrective actions necessary to optimize their effectiveness.

6.4 Security during Emergencies and Contingencies

Summarize the arrangements and actions to be taken during non-security emergencies or other contingency situations to ensure the protection of the radioactive sources at the facility is maintained.

6.5 Increased Threat Level

Describe how notifications of an increased threat level are addressed by the facility.

References

List any reference documents such as specific regulations, regulatory license, operating manuals, organizational policies and manuals etc. that are referred to in the Security Plan or are needed to explain or expand on any details in the Plan.

Appendices

Provide, or list, the procedures stated in the Security Plan e.g., those in section 5, including their dates and version.