Pursuant to Article 16(2) of the Law on Radiation and Nuclear Safety in Bosnia and Herzegovina ("Official Gazette of BiH" no. 88/07) and Article 61(2) of the Law on Administration ("Official Gazette of BiH" nos. 32/02 and 102/09), the director of the State Regulatory Agency for Radiation and Nuclear Safety issues:

REGULATION ON THE SECURITY OF NUCLEAR MATERIAL AND RADIOACTIVE SOURCES

PART ONE – INTRODUCTORY PROVISIONS

Article 1
(Subject)

This regulation lays down requirements for the authorization holder relating to the security of nuclear material and radioactive sources in use, storage and transport, and as well all other matters relevant for the security of the material and sources.

Article 2
(Objectives of the regulation)

The objectives of this regulation are:

a) Establishment of a security system for nuclear material and radioactive sources during the entire period from their production until the final disposal;
b) Achievement and maintenance of a high level of security of nuclear material and radioactive sources, commensurate with the potential risk;
c) Prevention of unauthorized access and unauthorized removal of nuclear material and radioactive sources;
d) Enhancing protection of the population against the ionizing radiation that may result from unauthorized use, storage and transport of nuclear material and radioactive sources.

Article 3
(Application)

This regulation shall apply to nuclear material and radioactive sources in use, storage and transport.

Article 4
(Definitions)

The terms, as used in this regulation, mean:

a) **Background check:** The process conducted by a competent authority that is obligated to determine any possible security concerns relating to job performance before a person enters the job at which that person will or could have insight into sensitive information.

b) **Secured area:** A temporary or permanent area established by the authorization holder for the purpose of security of nuclear material and radioactive sources.

c) **Security functions**: Functions of a system for detecting malicious acts involving nuclear material and radioactive sources, a system for delaying such illegal acts, a system of response to illegal acts involving nuclear material and radioactive sources, and a security management system for nuclear material and radioactive sources.

d) **Nuclear security event:** An event that is assessed as having implications for the security of nuclear material and radioactive sources. It is any event that could raise suspicion that the security of nuclear material and radioactive sources is compromised, such as: discrepancy of record data; suspected or confirmed theft of nuclear material and radioactive sources; unauthorized entry into a store of nuclear material and radioactive sources; discovery of suspected or actual explosive device near or in a store of nuclear material and radioactive sources; loss of control over nuclear material and radioactive sources; unauthorized access or use of nuclear material and radioactive sources; failure or loss of security systems, and any other event that could indicate planning a sabotage or unauthorized removal of nuclear material and radioactive sources.

e) **Security plan:** A document of the authorization holder containing a detailed description of the security measures implemented in an associated facility used by the authorization holder to carry out a practice.

f) **Information security:** Preserving the sensitivity, integrity and usability of information.

g) **Security of nuclear material and radioactive sources:** Measures taken with the aim of preventing unauthorized access, unauthorized removal, sabotage or other actions intended to commit a malicious act involving nuclear material, radioactive sources and facilities.

h) **Detection function:** Measures taken to discover a potential adversary during attempted or completed illegal act of unauthorized access to nuclear material and radioactive sources, unauthorized removal or sabotage.

i) **Response function:** Measures taken to assess and respond to an event that compromises the security of nuclear material and radioactive sources.

j) **Delay function:** Impeding a potential adversary to gain unauthorized access, remove or sabotage nuclear material or radioactive sources, generally implemented through physical barriers.

k) **Graded approach**: The application of nuclear security measures by the authorization holder commensurate with the potential consequences of malicious acts involving nuclear material and radioactive sources.

l) **Isolation of the radioactive source:** Protection of radioactive sources by allowing access to the secured areas through established access control points.

m) **Category 1 radioactive sources:** Radioactive sources the activity of which is equal to or greater than the value for Category 1 shown in table 2 of Annex II. If not safely managed or securely protected, Category 1 sources could cause a permanent injury to a person who handled them or was in contact with them for more than a few minutes. It would probably be fatal to be close to such unshielded material for a period between a few minutes and an hour. These sources are used in radiation teletherapy.

n) **Category 2 radioactive sources:** Radioactive sources the activity of which is equal to or greater than the value for Category 2 but less than the value for Category 1 shown in table 2 of Annex II. If not safely managed or securely protected, Category 2 sources could cause a permanent injury to a person who handled them or was in contact with them between several minutes and one hour. It could be fatal to be close to such unshielded material between several hours and several days. These sources are used in industrial radiography, high-dose and medium dose rate brachytherapy.

o) **Category 3 radioactive sources:** Radioactive sources the activity of which is equal to or greater than the value for Category 3 but less than the value for Category 2 shown in table 2 of Annex II. If not safely managed or securely protected, Category 3 sources could cause a permanent injury to a person who handled them or was in contact with them for several hours. It could – although it is unlikely – be fatal to be close to such unshielded material for a period of several days to several weeks. These sources are used in fixed gauges with high activity (level gauges, well logging).

p) **Category 4 radioactive sources:** Radioactive sources the activity of which is equal to or greater than 0.01 D up to 1 D, and less than the value for Category 3 shown in table 2 of Annex II. Category 4 sources could cause a temporary injury to a person who was close to them for several weeks. Permanent injuries are not likely. These sources are used in low-dose brachytherapy, thickness gauges, etc.

q) **Category 5 radioactive sources:** Radioactive sources the activity of which is equal to or greater than the exempt value and is up to 0.01 D, but less than the value for Category 4 shown in table 2 of Annex II. Category 5 sources could – but very unlikely – cause temporary minor injuries. An example of their use is a static eliminator of electricity charge.

r) **Access control**: Administrative and physical measures preventing unrestricted access to the sites of nuclear material and radioactive sources in use or storage or allowing access to sensitive information only to the authorized persons that need such access to perform their job duties.

s) **Security culture:** The assembly of characteristics and attitudes of organizations and individuals, which establishes a method of paying attention to the matters of security of nuclear material and radioactive sources in accordance with their importance.

t) **Mobile device:** Part of equipment containing radioactive material and on wheels or equipped to be mobile or designed to be handheld.

u) **Not later than delivery time:** The date and time set by the consignor and the consignee as the time of launching a search if a consignment has not reached the consignee. This interval may not be longer than six hours after the expected time of delivery.

v) **Unauthorized access:** Access to nuclear material or radioactive sources without an approval of a responsible person.

w) **Unauthorized removal**: The theft or any other unlawful way of removing nuclear material or radioactive sources from their authorized locations.

x) **Contingency plan:** An integral part of the security plan that identifies possible security events, ensures initial actions and assigns responsibilities in such events.

y) **Sensitive information:** Information the unauthorized disclosure, modification, alteration, destruction or an unauthorized denial of use of which could compromise nuclear security.

z) **Consignor**: A legal person authorized to prepare a consignment for transport and referred to as "consignor" in transport documents.

aa) **Reliability and trustworthiness:** Characteristics of an individual based on which that individual may be regarded as reliable and trustworthy so that unescorted access of that individual to nuclear material and radioactive sources does not pose a risk to the health of the population, safety and security. Determination of reliability and trustworthiness for this purpose shall be based on the results of background checks.

bb) **Associated facility:** A facility in which nuclear material or radioactive sources are produced, processed, used, handled, stored or disposed of.

cc) **Security threat:** An intention of a person or group of persons to commit a malicious act involving nuclear material or radioactive sources.

dd) **Carrier:** A legal person authorized for the transport of nuclear material and radioactive sources, and referred to as "carrier" in transport documents.

ee) **Consignee:** A legal person authorized for the receipt of nuclear material and radioactive sources, and referred to as "consignee" in transport documents.

ff) **Principle of official or business need ("need to know" principle):** Possession of sensitive information only within the boundaries established by the law and only to the extent needed to perform assignments within the relevant boundaries.

gg) **Threat assessment:** An intelligence-based analysis of the intentions of a person or group of persons to cause undesirable consequences with regard to nuclear material or radioactive sources.

hh) **Sabotage:** Deliberate damage to nuclear material or radioactive sources inuse, storage or transport or to an associated facility or conveyance in which nuclear material or radioactive sources are used, stored or transported, that could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.

ii) **Security management system:** A set of measures ensuring appropriate resources for the security of nuclear material and radioactive sources, including the development of appropriate procedures and plans for their security, and the procedures for handling sensitive information and protection against their unauthorized disclosure.

jj) **Categorization system:** A system in use in order to implement the graded approach by associating degrees of protection with specific types and quantities of radioactive sources, thus ensuring greater levels of protection for radioactive material for which a malicious act could result in higher consequences.

kk) **Set of radioactive sources**: Radioactive sources in the close proximity of each other and with the same physical barriers protecting access to them.

ll) **Unescorted access:** Access without escort to nuclear material or radioactive sources, granted to individuals with a proper authorization.

mm) **Malicious acts involving nuclear material and/or radioactive source:** An illegal act intended to cause death or physical injury, material damage or

damage to property or the environment. This includes attempted or completed unauthorized removal, sabotage, and as well the use of material and sources for deliberate radiation exposure of the people and the environment through dispersion of radioactive material or external exposure.

Article 5
(Security culture)

The authorization holder shall establish a management system which is appropriate to the scope and nature of the authorized practice, thus ensuring that:

a) security-related procedures are established and are a top priority;
b) problems affecting security are promptly identified and corrected in a manner commensurate with their importance;
c) security responsibilities of each individual are clearly identified, and each individual has appropriate training and qualifications;
d) lines of authority for making decisions important for security are clearly defined;
e) organizational arrangements and lines of communications are established so as to result in an appropriate flow of information on security among the various organizational levels.

Article 6
(General responsibilities of the authorization holder)

(1) Prime responsibility for the security of nuclear material and/or radioactive sources shall rest with the authorization holder.

(2) The authorization holder shall be responsible for the establishment and application of security measures for nuclear material and/or radioactive sources, including preparation, regular review and implementation of the security plan.

(3) The authorization holder shall appoint a person that will be responsible for the security of nuclear material and/or radioactive sources. The person responsible for radiation protection may perform duties of the person responsible for the security of nuclear material and/or radioactive sources.

(4) The authorization holder shall notify the State Regulatory Agency for Radiation and Nuclear Safety (hereinafter: Agency) of the intention to make any modification of practice that may affect the security of nuclear material and/or radioactive sources.

Article 7
(Security training)

(1) The authorization holder shall provide training in the security of nuclear material and/or radioactive sources to ensure that all persons that use, store or transport material and/or sources have appropriate knowledge and skills in order to perform their assigned duties.

(2) The basic training shall include instructions on:

a) responsibility to promptly notify authorization holder of the circumstances that cause or could cause violation of provisions of this regulation;
b) responsibility of the authorization holder to promptly notify police authority and the Agency of an attempted or completed unauthorized removal or sabotage;
c) an appropriate response a security alarm.

(3) During the selection of personnel for training, the authorization holder shall consider responsibilities and duties of every individual in their authorized use and response to possible situations involving unauthorized removal or sabotage of nuclear material, radioactive sources and facilities.

(4) The authorization holder shall provide additional training in case of major changes in the security system and as well for new personnel. This training shall include:

a) reports on relevant security problems and lessons learned;
b) reports on the relevant results of Agency inspections;
c) reports on the relevant results of review, testing and maintenance of the security plan.

(5) The authorization holder shall keep the documentation on basic and additional trainings for three years from the training completion date. Training records shall contain the training dates, covered topics, and attendance lists.

(6) The authorization holder shall ensure that the person responsible for the security of nuclear material in Categories I–III and/or Category 1 radioactive sources has a certificate of a competent ministry of interior for the purpose of proper and efficient performance of assigned duties.

(7) The authorization holder shall regularly inform his personnel about the security measures in accordance with the security procedures for nuclear material and/or radioactive sources.

Article 8
(Organization of security)

(1) The authorization holder shall establish and maintain a security system by implementing a system of physical and technical protection measures with the aim of preventing unauthorized access, unauthorized removal or other malicious acts involving nuclear material, radioactive sources and facilities.

(2) The holder of the authorization for nuclear material in Categories I-III and the holder of the authorization for Category 1 radioactive sources shall have an internal guarding service organized under the applicable legislation.

(3) The authorization holder shall manage the information associated with the security of nuclear material and/or radioactive sources under the principle of

official or business need.

Article 9
(Coordination with police authorities)

The authorization holder shall coordinate activities with a competent police authority to the extent necessary to respond to threats against a facility of the authorization holder, and as needed in other cases for the purpose of:

a) detection, delay and response to unauthorized activities involving nuclear material, radioactive sources and facilities; and
b) assessment of threats involving nuclear material, radioactive sources and facilities.

Article 10
(Reporting on the security event)

(1) The holder of the authorization for use, storage and transport shall promptly notify the nearest police authority in case of unauthorized access, unauthorized removal, sabotage or any other malicious act involving nuclear material and/or radioactive sources.

(2) The holder of the authorization for use, storage and transport shall also notify the Agency of the events referred to in paragraph (1) immediately after notifying the police authority.

(3) A written report about the events referred to in paragraphs (1) and (2) shall be sent to the Agency within 24 hours at the latest.

(4) The consignee of nuclear material and/or radioactive sources shall notify the consignor of the date and time of receipt of shipment.

(5) Consignors and consignees of nuclear material and radioactive sources shall set the date and time for initiating search if the consignment has not reached the consignee. That period may not be longer than six hours after expected time of delivery.

PART TWO – SECURITY OF NUCLEAR MATERIAL

Article 11
(Categorization of nuclear material)

The categorization of nuclear material nuclear material in Categories I-III for the purpose of security is shown in table 1 of Annex I.

Article 12
(Other nuclear material)

For the purpose of security, other nuclear material includes quantities (masses) of nuclear material that falls beyond Category III referred to in Article 11, and natural uranium, depleted uranium, and thorium.

Article 13
(Requirements for the security of nuclear material in Categories I-III)

(1) The provisions of the Convention on the Physical Protection of Nuclear Material ("Official Gazette of the SFRY – International Agreements" no. 9/85) and amendments to the Convention on the Physical Protection of Nuclear Material ("Official Gazette of BiH – International Agreements" no. 3/10) shall apply to nuclear material in Categories I-III.

(2) The security measures as defined in the publication *Nuclear Security Series No. 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5), 2011, by the International Atomic Energy Agency (hereinafter: IAEA) shall apply to the security in use, storage and transport of nuclear material in Categories I-III.

Article 14
(Requirements for the security of other nuclear material)

(1) The authorization holder shall apply general security measures for the use and storage of nuclear material to ensure that the security is preserved.

(2) The measures referred to in paragraph (1) shall include:

a) ensuring reliability and trustworthiness of the personnel through the keeping of proper records;
b) ensuring the protection of nuclear material against unauthorized access, unauthorized removal, sabotage or other malicious acts;
c) storage of nuclear material at a secure location;
d) at least monthly verification that nuclear material is present at its location;
e) preparation of a contingency plan with the aim of responding to unauthorized removal of nuclear material or sabotage;
f) assistance to relevant authorities to implement rapid and comprehensive measures to locate and recover lost or stolen nuclear material.

(3) The consignor shall carry out the following measures for the transport requiring minimum security level:

a) proper selection of an authorized carrier and a consignor;
b) bind the consignee to notify the consignor of the consignment delivery.

PART THREE – SECURITY OF RADIOACTIVE SOURCES IN USE AND STORAGE

CHAPTER I – MAIN REQUIREMENTS FOR THE SECURITY OF RADIOACTIVE SOURCES IN USE AND STORAGE

Article 15
(Establishment of a security system)

The authorization holder shall establish a security system in accordance with the categorization of radioactive sources.

Article 16
(Categorization of radioactive sources)

(1) In accordance with the radiation risk and security requirements, radioactive sources shall be categorized as follows:

a) Category 1 – very high risk – extremely dangerous sources;
b) Category 2 – high risk – very dangerous sources;
c) Category 3 – medium risk – dangerous sources; and
d) Categories 4 and 5 – low risk – less dangerous sources.

(2) The categorization of radioactive sources into Categories 1–5 according to the A/D ratio is shown in table 1 of Annex II.

(3) Activities corresponding to thresholds for radioactive sources in Categories 1-3 are shown in table 2 of Annex II.

(4) Sealed sources in Categories 4 and 5 shall be categorized on a case-by-case basis by using the appropriate formula referred to in Annex II.

(5) Open sources used in medicine are classified into Categories 4 and 5. The nature of open sources and their short half-life requires their categorization on a case-by-case basis.

Article 17
(Security levels)

(1) The security system based on graded approach consists of four security levels:

a) Security Level A relating to Category 1 radioactive sources;
b) Security Level B relating to Category 2 radioactive sources;
c) Security Level C relating to Category 3 radioactive sources;
d) Security Level D relating to radioactive sources in Categories 4 and 5.

(2) The main elements of assigning the category of radioactive sources to the security level are shown in table 3 of Annex II.

Article 18
(Goals of security levels)

(1) Security levels have appropriate goals that define the overall result that the security system should achieve for the given security level.

(2) The goal of Security Level A is to prevent unauthorized removal of radioactive sources.

(3) The goal of Security Level B is to minimize the likelihood of unauthorized removal of radioactive sources.

(4) The goal of Security Level C is to reduce the likelihood of unauthorized removal of radioactive sources.

(5) The goal of Security Level D is to establish and implement the measures that enable safe use of sources and their adequate protection.

CHAPTER II – REQUIREMENTS FOR PHYSICAL AND TECHNICAL PROTECTION

Article 19
(Secured areas)

(1) The authorization holder shall ensure that radioactive sources in Categories 1–3 are used and/or stored within the established secured areas that may be permanent or temporary.

(2) All secured areas shall be established as permanent with the exception of temporary secured areas that shall be established during servicing, delivery or replacement of a radioactive source.

(3) Authorized individuals shall be allowed to access the sources in the secured areas through:

a) the established control points that allow access to nuclear material and radioactive sources isolated by means of continuous physical barriers; the physical barrier is a natural or artificial means adequate for the isolation of radioactive sources within the secured areas;
b) the direct control of secured areas by the personnel designated for such control;
c) a combination of continuous physical barriers and direct control.

(4) The authorization holder shall ensure that a sufficient number of authorized individuals continuously monitor a temporary secured area during the source maintenance, delivery or replacement.

(5) Where physical barriers or intrusion detection systems in a secured area are not operational, a sufficient number of authorized individuals shall continuously do the monitoring.

(6) Unauthorized personnel or visitors shall be under escort in the secured area.

(7) An area defined as the controlled area for the purpose of radiation safety may be used for the purpose of defining the secured area.

Article 20
(Surveillance, detection and assessment)

(1) The authorization holder shall establish and maintain continuous surveillance and measures for the detection of any unauthorized entry in the secured area.

(2) The authorization holder shall ensure means to maintain continuous surveillance and detection in case of loss of main electricity supply for the equipment, or ensure an alarm and a response in case of loss of continuous surveillance and detection of unauthorized entry.

(3) The authorization holder shall conduct surveillance and detection through one of the following systems:

a) an intrusion detection system connected with the central station for surveillance within and outside the building;
b) an electronic alarm system;
c) a video surveillance system;
d) direct visual surveillance within and outside the secured area.

(4) The authorization holder should have mechanical, electronic or chemical means for the detection of unauthorized removal of radioactive sources from the secured area.

(5) The authorization holder shall at the shortest time possible assess any attempted or completed unauthorized entry into a secured area.

(6) The holder of authorization for technical service for radioactive waste management shall establish and maintain a system for video surveillance of the waste storage facility on the site and from a remote location.

(7) The Agency shall have unrestricted access to the video surveillance system referred to in paragraph (6).

CHAPTER III – SECURITY OBJECTIVS AND MEASURES
FOR THE SECURITY LEVELS A, B, C, AND D

Article 21
(Security objectives and measures for the Security Level A)

(1) In order to achieve the goal of the Security Level A, the authorization holder shall at all times implement security functions of detection, prevention and response to any attempted unauthorized removal of radioactive sources.

(2) In order to implement the detection function, the authorization holder shall implement the following measures:

(a) immediate detection of any unauthorized access to the secured area and the location of radioactive source by means of an electronic intrusion system detection or through continuous surveillance by the personnel;
(b) immediate detection of any attempted unauthorized removal of the radioactive source by means of electronic tamper detection equipment or through continuous surveillance by the personnel;
(c) immediate assessment of the detection by means of a video surveillance (CCTV) from a remote location or by the personnel or security guards;
(d) communicate with the security response personnel in the shortest possible time;
(e) ensuring conditions for the detection of potential loss of radioactive source through daily checks of the source presence carried out by measuring the radiation level, the use of a system indicating any attempted access to the source or in another way.

(3) In order to implement the delay function, the authorization holder shall ensure through at least two-barrier system, e.g., walls and grids or other adequate measures, that sufficient delay following detection be provided to prevent illegal acts and enable adequate reaction of the security response personnel.

(4) In order to implement the response function, the authorization holder shall ensure an immediate response to the generated alarm by using sufficient personnel, equipment and technical resources to prevent unauthorized removal of radioactive sources.

Article 22
(Security objectives and measures for the Security Level B)

(1) In order to achieve the goal of the Security Level B, the authorization holder shall at all times implement security functions of detection, delay and response to any attempted unauthorized removal of radioactive sources.

(2) In order to implement the detection function, the authorization holder shall implement the following measures:

(a) immediate detection of any unauthorized access to the secured area and the location of radioactive source by means of an electronic intrusion detection system or through continuous surveillance by the personnel;
(b) detection of any attempted unauthorized removal of the radioactive source by means of electronic tamper detection equipment or through periodical checks by the personnel;
(c) immediate assessment of detection through a video surveillance (CCTV) from a remote location or by the personnel or security guards;
(d) communication with security response personnel in the shortest possible time;

(e) ensuring conditions to detect potential loss of radioactive source through weekly checks of the source presence by using measurement of radiation, tamper detection system or another measure.

(3) In order to implement the delay function, the authorization holder shall provide at least a two-barrier system, e.g., walls and fences, or implement other adequate measures in order to minimize the likelihood of unauthorized removal of radioactive sources.

(4) In order to implement the response function, the authorization holder shall ensure immediate initiation of response to interrupt unauthorized removal of sources by using equipment and procedures for immediate initiation of response.

Article 23

(Security objectives and measures for the Security Level C)

(1) In order to achieve the goal of the Security Level C, the authorization holder shall at all times implement security functions of detection, delay, and response to any attempted unauthorized removal of radioactive sources.

(2) In order to implement the detection function, the authorization holder shall implement the following measures:

(a) detection of attempted unauthorized removal of radioactive sources by using intrusion detection equipment or periodic checks by personnel;
(b) immediate verification of detection through an assessment by personnel or security guards;
(c) obtaining information about the loss of a radioactive source through monthly checks, tamper detection equipment, etc.

(3) In order to implement the delay function, the authorization holder shall ensure a barrier, e.g., locked closet, source container or surveillance by personnel or other adequate measures in order to minimize the likelihood of unauthorized removal of radioactive sources.

(4) In order to implement the response function, the authorization holder shall implement appropriate measures in case of unauthorized removal of a source by using procedures for action in accordance with the contingency plan, which is an integral part of the security plan.

Article 24

(Security objectives and measures for the Security Level D)

In order to achieve the goal of the Security Level D, the authorization holder shall implement specific security management measures laid down in Article 35.

CHAPTER IV – SECURITY MNAGEMENT SYSTEM
FOR THE SECURITY LEVELS A, B, C, AND D

Article 25
(Security management)

The security management system for radioactive sources in Categories 1–3 shall consist of the following elements:

a) Access control;
b) Background check of the personnel;
c) Determination and protection of sensitive information;
d) Security plan and contingency plan;
e) Enhanced security measures;
f) Reporting system for security events.

Article 26
(Ways of access control)

(1) The authorization holder and the person responsible for the security of radioactive sources shall ensure that the control of access to the source efficiently prevents unauthorized individuals to access the source.

(2) Security Level A requires identification and verification by a combination of two or more methods, e.g., a magnetic card reader and a personal ID number, or keys and key control or other adequate measures.

(3) Security Levels B and C require a single identification technique, e.g., a magnetic card reader, personal ID number, computer password, visual identification by another authorized person or other adequate measures.

Article 27
(Access authorization)

(1) The authorization holder shall issue authorization for unescorted access to radioactive sources in Categories 1–3 to the selected personnel members and keep records thereof.

(2) The authorization referred to in paragraph (1) shall be granted on the basis of background check results.

Article 28
(Background check)

(1) The trustworthiness and reliability of the personnel with unescorted access to radioactive sources in Categories 1–3, source location and sensitive information shall be ensured through a background check.

(2) The check referred to in paragraph (1) shall be conducted in cooperation with relevant police authorities and shall consist of at least identity check, review of previous employments, and verification of references.

(3) The authorization holder shall every three years check with the relevant authority whether there is a criminal proceeding against the authorized individual or whether such individual is convicted of a crime carrying prison sentence except for crimes against traffic safety or whether such individual is held accountable for a violation of public order involving violence.

(4) If the check has discovered that there is an ongoing criminal proceeding against an authorized individual, except for crimes against traffic safety, or that such individual is held accountable for a violation of public order including violence, the authorization holder shall prohibit unescorted access to radioactive sources to such individual.

Article 29
(Identification and protection of sensitive information)

(1) The authorization holder shall identify and protect sensitive information against unauthorized disclosure.

(2) The authorization holder shall protect the buildings and premises that are used to store confidential documentation, files and registers.

(3) Sensitive information shall include:

a) Content of the security plan;
b) Plan implementation procedures;
c) Details about the building construction and the building diagram;
d) Details about protection systems (alarms, cameras);
e) Records containing the names of authorized individuals;
f) Register of sources (number, type, form and exact location);
g) Information about background checks of the personnel; and
h) Information that could help disassemble a source, used to access the source.

(4) The access to sensitive information referred to in paragraph (3) shall be approved in accordance with applicable legislation.

(5) The authorization holder shall keep the records of individuals granted with access to the security plan or plan implementation procedures. Once the authorization holder determines that a personnel member is no longer required to access the plan or the procedures, that personnel member shall be deleted from the relevant records within seven days.

Article 30
(Security plan)

(1) The security plan shall establish a comprehensive strategy of the authorization holder's actions to ensure the security of radioactive sources.

(2) The security plan shall:

a) identify measures to be taken for the purpose of security;
b) identify resources needed for security.

(3) The person responsible for the security of radioactive sources shall approve the plan by putting own initials on the security plan before its adoption by the authorization holder.

(4) The Agency shall send the security plan for radioactive sources in Categories 1-3 to the State Investigation and Protection Agency, that is, to its Section for Combat against Terrorism and Trafficking in Atomic, Biological and Chemical Weapons for information.

(5) The authorization holder shall keep the security plan at least three years from the date of its expiry.

Article 31
(Implementation procedures for the security plan)

(1) The authorization holder shall draw up and maintain written procedures documenting the methods of fulfilling security plan requirements.

(2) The person responsible for the security of radioactive sources shall approve the plan by putting own initials on the implementation procedures and their amendments before their adoption by the authorization holder.

(3) The authorization holder shall keep the procedures at least three years from the date of their expiry.

Article 32
(Guidelines for the security plan development)

(1) Content of the security plan could include the following information:

a) Introduction

1) Name of the organization;
2) Type of the organization (hospital/university/industry/other);
3) Description of the site;
4) Address;
5) Telephone number;
6) E-mail;

7) Name of the persons responsible for radiation protection.

b) Organization of security

1) Name of the person responsible for security;
2) Contact phone number of the person responsible for security;
3) Whether the person referred to in b)1 is a full or part-time employee;
4) Details about personnel in guarding service;
5) Details about managers.

c) Diagram of the building

A diagram of the building showing the perimeter around the site and the building with the map of surroundings with a scale of 1:100.

d) Perimeter

1) Site perimeter description;
2) Details about fence;
3) Details about doors;
4) Details about security lighting:
5) Details about the intrusion detection system;
6) Details about the CCTV system.

e) Area of responsibility of the guardhouse at the entrance

1) Details about security and personnel;
2) Lighting;
3) Automatic access control systems;
4) Communication systems (including arrangements for support in case of a security event).

f) Access control points

1) Details about doors and traffic lights for pedestrians and vehicles;
2) Control procedures;
3) Systems for passage of personnel;
4) Issuance of temporary passes to visitors, contractors and others;
5) Vehicle inspection;
6) Access arrangements for personnel;
7) Access arrangements for contractors (including escort);
8) Access arrangements for visitors (including escort);
9) Arrangements for search in case of intrusion;
10) Monitoring of access by a CCTV;
11) Key control and locking doors.

g) Area security

1) If the area is not defined, description of access to the area of source location;

2) Access control arrangements;
3) Use of intrusion detection system;
4) Response to the alarm of the intrusion detection system;
5) Methods to identify authorized personnel;
6) Continuous control.

h) Keeping of the radioactive sources

A list of buildings or locations (names and numbers) at which radioactive sources are used or stored:

1) Buildings or locations;
2) Description, categorization and use of source;
3) Activity measured in GBq;
4) Security arrangements for store rooms;
5) Additional access control arrangements;
6) Intrusion detection devices.

i) Security of information

Detailed arrangements for the protection of sensitive information referred to in Article 29(3).

j) Background checks

Detailed arrangements about the checks of identity and trustworthiness of the personnel authorized for unescorted access to radioactive sources and sensitive information, and as well for those in charge of the building security.

k) Maintenance, repair and testing of security systems

1) Testing in pre-determined intervals (e.g., weekly);
2) Details about alternative power supply in case of power failure;
3) Reporting procedures for repair of malfunctions of the security system;
4) Arrangements for maintaining security regime in case of malfunctioning security equipment or during regular maintenance or minimal repair.

l) Plan for security events – Control and reporting

1) Details about contingency plans/plans for incidents, and instructions for personnel;
2) Arrangements for annual testing of contingency plans;
3) A list of security instructions for personnel and the person responsible for general security of the building;
4) A list of planned options to enhance security in case of an increased threat.

(2) The Agency shall assess content of the security plan during the procedure of granting authorization on a case-by-case basis.

Article 33
(Security plan updates)

(1) The authorization holder shall continuously monitor effectiveness of the security plan and take steps to eliminate possible deficiencies.

(2) The security plan shall be updated as needed but at least once a year.

(3) Any update of the security plan shall be approved by the person responsible for, and if the plan is revised, the person responsible for security shall inform all relevant personnel about the amendments.

(4) The authorization holder shall notify the Agency of all amendments to the security plan within seven days from the date of entry into force of the amendments.

Article 34
(Enhanced security measures)

(1) In case of a suspected increased security threat, the authorization holder shall enhance security measures.

a) Enhanced security measures include:

1) for the source in use, return of the source to a secured store room;
2) 24-hour guarding service, additional video surveillance or additional alarm system;
3) notifying a relevant police authority and the Agency of the suspected threat;
4) check of security procedures, building diagrams and radiation safety practices in cooperation with a relevant police authority and other authorities competent to respond to malicious acts involving radioactive source.

(2) Enhanced security measures shall remain effective as long the security threat referred to in paragraph (1) exists.

(3) Enhanced security measures shall always apply during the transport of radioactive sources in Categories 1 and 2, and as well in cases such as replacement, repair and maintenance of the radioactive source.

Article 35
(Security management for Security Level D)

For the purpose of security management, the holder of authorization for radioactive sources in Categories 4 and 5 shall:

a) ensure the safe use of sources by implementing applicable legislation;
b) ensure trustworthiness of the personnel;
c) ensure protection of radioactive sources from unauthorized access;

d) store the source in a secured container and at a secured location;
e) verify that the radioactive source is present at its location at least once in three months.

CHAPTER V – OTHER SECURITY REQUIREMENTS

Article 36
(Communication)

(1) The authorization holder for radioactive sources in Categories 1–3 shall establish and maintain continuous communication between the personnel, and electronic transfer and processing of relevant data between the locations of security systems.

(2) In case of loss of main communication means or dana transfer and processing, the authorization holder for radioactive sources in Categories 1–3 shall ensure alternative communication options for personnel and alternative options of transfer and processing. Alternative communication systems and data transfer may not be subject to same flaws as the main systems.

Article 37
(Requirements for mobile devices)

(1) The mobile devices containing radioactive sources in Categories 1–3 shall require two physically separate solid barriers (e.g., lock, container with padlock, chain) to secure the radioactive source against unauthorized removal when a mobile device is not monitored.

(2) The mobile device containing radioactive sources in Categories 1–3 that is in or on the conveyance or on the trailer without being monitored shall require disabled start of the conveyance or trailer.

PART FOUR – SECURITY OF RADIOACTIVE SOURCES IN TRANSPORT

CHAPTER I – MAIN REQUIREMENTS FOR THE SECURITY OF RADIOACTIVE SOURCES IN TRANSPORT

Article 38
(Transport security measures)

Transport security shall be achieved by:

a) minimizing the total time of transport;
b) limiting the number and duration of transport interruptions;
c) providing protection during transport or transit and providing storage in a manner consistent with the category of the radioactive source;
a) implementing a transport security plan.

Article 39
(Ways of preventing theft and sabotage)

(1) Minimizing the likelihood of theft and sabotage of radioactive sources in transport shall be achieved by a combination of measures that include detection, delay and response.

(2) The above measures may be complemented with other measures relating to the recovery of stolen material and mitigation of possible radiological consequences, endangerment of the health of people and the environment to additionally reduce the risk.

Article 40
(Security levels in transport)

(1) Transport security is classifed into three levels:

a) Enhanced security level;
b) Basic security level;
c) Minimum security level.

(2) Enhanced security level shall apply to radioactive sources in Categories 1 and 2, and consignments transported in B(U/M) Type packages except irradiated nuclear fuel and fissile material.

(3) Basic security level shall apply to Category 3 radioactive sources and consignments transported in Type A packages.

(4) Minimum security level shall apply to radioactive sources in Categories 4 and 5, excepted packages, LSA-I material, SCO-I material and industrial packages IP-1, IP-2 and IP-3.

(5) The authorization holder for the transport of radioactive sources shall establish one of the three security levels on the basis of the activity of the package content and the type of package to be transported.

(6) In addition to the security levels referred to in paragraphs (2), (3) and (4), additional security measures may be established as needed and upon proposal of the Agency.

Article 41
(Table of levels)

Security levels based on the type of radioactive material and the type of package are shown in table 1 of Annex III.

CHAPTER II – ENHANCED SECURITY LEVEL

Article 42
(General security requirements)

(1) Consignors, carriers and consignees shall ensure that all persons engaged in the transport of radioactive sources implement transport security measures in accordance with their responsibilities and the threat level.

(2) A radioactive source temporarily stored in a transit site shall be subject to security measures consistent with the measures to be applied to the radioactive sources in use and storage.

(3) The consignee shall have procedures in place for the case that a radioactive source package is not delivered within the planned time frame. If it is determined that the package is lost, stolen or damaged, it is necessary to initiate procedures to locate and recover it.

(4) Radioactive sources shall be transported in packages that are tested and have a design certificate from an authorized institution in the manufacturing country. Packages weighing more than 2,000 kg shall be transported in open conveyances, but consignors, carriers and consignees shall check the integrity of locks and seals before the transport.

(5) In case of the transport of radioactive source in open conveyances, the Agency shall establish additional security measures taking into account of the type of radioactive material and a prevailing threat.

Article 43
(Basic security training)

(1) In addition to a basic radiation protection training, consignors, carriers and consignees shall ensure a security awareness training to the persons engaged in transport.

(2) The training referred to in paragraph (1) shall contain information about the nature of security related threats, types of security concerns, methods to address such concerns, and steps to take in case of security incidents.

Article 44
(Identification of the carrier and the consignor)

Every person engaged in the transport of radioactive sources shall have a valid photographic identification document, and the crew shall have a copy of the approval for transport in the conveyance.

Article 45
(Security inspection of the conveyance)

(1) The carrier shall perform a security inspection of the conveyance prior to the commencement of the transport.

(2) The security inspection referred to in paragraph (1) normally includes a visual inspection of the conveyance and detection of any additional objects on the conveyance that could affect transport.

(3) The carrier shall ensure that all security measures remain effective for the duration of the transport.

Article 46
(Written instructions)

(1) The carrier shall provide crew members with written instructions on all required security measures.

(2) Security measures shall also include a response procedure in case of a security incident during transport.

(3) In normal conditions, the written instructions referred to in paragraph (1) shall contain only the main contact details in case of compromised security.

Article 47
(Exchange of security related information)

(1) Consignors, carriers and consignees need to cooperate with each other with regard to the exchange of security related information.

(2) As needed, security related information shall be exchanged with the Agency and as well with other relevant security agencies in Bosnia and Herzegovina and abroad.

(3) In case of a transport incident with transboundary effects, the Agency shall notify IAEA.

Article 48
(Determining reliability and trustworthiness)

Prior to the commencement of transport, consignors, carriers and consignees shall verify the reliability and trustworthiness of persons engaged in transport in accordance with responsibilities of all those engaged in transport.

Article 49
(Advance notification)

(1) The consignee shall provide advance notification to the consignee of the planned consignment, mode of transport, and expected delivery time.

(2) Prior to the commencement of transport, the consignee shall confirm to the consignor the readiness to accept the consignment at the expected time and notify the consignor on receipt or non-receipt, whichever is the case.

(3) Consignord, carriers and consignees shall notify the Agency in advance of every transport of radioactive sources under the legislation.

Article 50
(Tracking devices)

(1) Carriers shall ensure methods or devices for tracking conveyances transporting radioactive sources for the duration of the transport.

(2) Continuous tracking of the conveances transporting Category 1 radioactive sources shall eb achieved by installing a GPS receiver in the conveyance.

(3) The tracking of the conveyances transporting Category 2 radioactive sources shall be achieved by installing a GPS receiver or by regular communication using devices at pre-defined transit points.

(4) The shipment containing packages shall be tracked by marking each package with a bar code.

Article 51
(Communication with the conveyance)

The carrier shall ensure continuous communication of the crew in conveyances transporting radioactive sources in Categories 1 and 2 with persons responsible for the implementation of the transport security plan.

Article 52
(Additional security measures for transport by road, railway and inland waterway)

(1) For the transport of radioactive sources by road, rail and inland waterway the carrier shall provide devices, equipment or other methods to detect, delay and respond to an atempted theft, sabotage or other malicious acts against conveyances or cargo.

(2) Such devices and equipment shall be operational for the duration of the transport.

(3) The carrier shall ensure continuous tracking of the road transport, and where it is not possible, it is necessary to find other appropriate methods.

Article 53
(Transport security plan)

(1) Consignors, carriers and consignees engaged in the transport of radioactive sources in Categories 1 and 2 shall adopt a transport security plan in accordance with the provisions of this regulation, and as well ensure its implementation.

(2) The plan referred to in paragraph (1) shall be periodically amended to preserve the security level during its implementation and in case of any change of the transport plan.

(3) In case of the transport of radioactive sources in Categories 1 and 2, the carrier shall submit the plan to the Agency during the procedure of issuing individual approval for transport.

(4) The person responsible for the security of radioactive sources shall approve the plan by putting own initials on the plan before its adoption by the authorization holder.

Article 54
(Content of the transport security plan)

The content of the transport security plan shall include:

a) Information about the source to be transported that shall include:

   1) radionuclide;
   2) activity measured on a specified date;
   3) physical and chemical form;
   4) serial number;
   5) overpack for transport; and
   6) category of the source to be transported.

b) A reason for transporting radioactive material;
c) A description of the conveyance transporting radioactive material and of security arrangements for the shipment during transfers to another conveyance or other stops on the way;
d) Allocation of security responsibilities to the persons properly authorized to perform their responsibilities;
e) Names, addresses and telephone numbers of all parties involved in transport, which have to be available 24 hours a day;
f) An assessment of all existing or possible security risks relating to the transport of radioactive material, and as well activities to identify risks;
g) A description of procedural measures for resolving security problems, as follows:

   1) procedures for notifying, as needed, a relevant ministry of interior and the Agency;
   2) response procedure for traffic accidents involving conveyances transporting radioactive material;
   3) a procedure for planning primary and alternative routes;
   4) a procedure and equipment for timely notification and action in case of security threats, breach of security measures or security-related incidents;
   5) information about the training of persons engaged in the transport of radioactive sources in relation to risk assessment and threat level;
   6) the way of communication between the parties involved in the transport.

h) A procedure for evaluation and testing of the transport security plan.

Article 55
(Sensitive information)

The content of the plan referred to in Article 54 shall represent sensitive information.

CHAPTER III – BASIC AND MINIMUM SECURITY LEVELS

Article 56
(Requirements for basic security level)

Transport security requirements for basic security level are identical to the requirements for enhanced security level, except the requirements referred to in Articles 49, 50, 51, 53 and 54.

Article 57
(Requirements for minimum security level)

(1) Consignors, carriers and consignees shall apply reasonable security measures for the transport that requires minimum security level, which will ensure that the security is preserved during the transport of radioactive sources.

(2) The consignor shall implement the following measures for the transport that requires minimum security level:

a) Verification that the radioactive source is present;
b) Proper selection of an authorized carrier and a consignee;
c) Imposing an obligation on the consignee to notify him of the receipt of consignment.

CHAPTER IV – ADDITIONAL SECURITY MEASURES

Article 58
(Additional security measures)

(1) In addition to the measures referred to in Articles 42–54, the Agency may request carriers, consignors and consignees to apply additional security measures referred to in Article 59.

(2) The Agency shall request police escort for the transport of Category 1 radioactive sources and if needed for other categories as well.

Article 59
(Content of additional security measures)

Additional security measures may consist of the following:

a) Additional security training;
b) Establishment of an additional system for tracking the conveyance;
c) Additional security inspection of the conveyance before loading the cargo;
d) Conveyances specially designed or adapted to additional security requirements;
e) Additional review of the security plan;
f) An exercise to check efficiency of the security plan,
g) Additional written instructions detailing responsibilities of authorized individuals relating to security;
h) The use of reliable and secure communication systems during transport.

PART FIVE – TRANSITIONAL AND FINAL PROVISIONS

Article 60
(Harmonization of operations)

The legal persons that use, store or transport nuclear material and radioactive sources shall harmonize their operations with the provisions of this regulation within six months from the day of entering this regulation into force.

Article 61
(Penalties)

Any violation of the provisions of this regulation shall be punished under the applicable legislation.

Article 62
(Entering into force)

This regulation shall enter into force on the eighth day following that of its publication in the "Official Gazette of BiH."

No: 04-02-983/13
Sarajevo, 25.10.2013.

Director
Emir Dizdarevic

ANNEX I: CATEGORIZATION OF NUCLEAR MATERIAL

***Table 1*: Categorization of nuclear material**

Material	Form	Category I	Category II	Category III
Plutonium[a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
Uranium U-235	Unirradiated[b] – U-235 enriched to 20% or more – U-235 enriched to more than 10% but less than 20% – U-235 enriched to less than 10% but above natural	– 5 kg or more	– Less than 5 kg but more than 1 kg – 10 kg or more	– 1 kg or less but more than 15 g – Less than 10 kg but more than 1 kg – 10 kg or more
Uranium U-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
Irradiated nuclear fuel			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[c]	

[a] All plutonium except that with isotopic concentration exceeding 80% in Pu-238

[b] Material not irradiated in a reactor or material irradiated in a reactor or irradiated in reactor but with a radiation level equal to or less than 1 Gy/hr at 1 m unshielded

[c] Other fuel classified as Category I or II before irradiation by virtue of its nuclear material content may be reduced one category level if the radiation level from the fuel exceeds 1 Gy/hr at 1 m unshielded.

ANNEX II: THE CATEGORIZATION OF RADIOACTIVE SOURCES OR AGGREGATIONS OF RADIOACTIVE SOURCES

If a sufficiently high activity of a radioactive source results in a radiation dose that causes deterministic effects for an exposed individual, the source can be considered a "dangerous source." The source activity that gives such a dose is denoted as "D value."

The category of a radioactive source is determined in accordance with the value of the source activity (A), expressed in TBq, and the corresponding D value for the radionuclide (D), shown in table 2 of this Annex. The correlation between the source category and A/D ratio of the source is shown in table 1 of this Annex.

The category of an aggregation of radioactive sources of the same radionuclide is determined in accordance with the value of the A/D ratio, and calculated by using the following formula:

$$A / D = \frac{\sum_i A_i}{D},$$

where A_i is the activity of each individual source expressed in TBq, and D is D value for radionuclide, as shown in table 2 of this Annex. The correlation between the category of the aggregation of sources with the same radionuclide and the A/D ratio of the aggregation is shown in table 1 of this Annex.

The category of an aggregation of radioactive sources of different radionuclides is determined in accordance with the A/D ratio of the aggregation and calculated by using the following formula:

$$A / D = \sum_n \frac{\sum_i A_{i,n}}{D_n},$$

where $A_{i,n}$ is the activity of each individual source i of radionuclide n, expressed in TBq, and D_n is D value for radionuclide n, as shown in table 2 of this Annex. The correlation between the category of the aggregation of sources of different radionuclides and the A/D ratio of the aggregation is shown in table 1 of this Annex.

Table 1: **Categorization of sources according to A/D ratios**

Category	Ratio of activity to D value (A/D[a])	Security level
1	A/D ≥ 1000	A
2	1000 > A/D ≥10	B
3	10 > A/D ≥ 1	C
4	1 > A/D ≥ 0.01	D
5	0.01 > A/D > exempt[b]/ D	D

[a] D values are indicated in the IAEA publication TECDOC-953, Vienna, 2003.
[b] Exempt values are shown in Annex I, table I, of the Regulation on the notification and authorization of practices involving radiation sources.

***Table 2*: Activities corresponding to thresholds for radioactive sources in Categories 1, 2 and 3**

Radionuclide	Category 1 1000 D		Category 2 10 D		Category 3 D	
	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]
Am-241	6.E+ 6.E+ 01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Am-241/Be	6.E+ 01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Cf-252 2.E+	01	5.E+02	2.E-01	5.E-00	2.E-02	5.E-01
Cm-244	5.E+ 5.E+ 01	1.E+03	5.E-01	1.E+01	5.E-02	1.E+00
Co-60 3.E+	01	8.E+02	3.E-01	8.E+00	3.E-02	8.E-01
Cs-137 1.E+	02	3.E+03	1.E+00	3.E+01	1.E-01	3.E+00
Gd-153	1.E+ 03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Ir-192 8.E+	01	2.E+03	8.E-01	2.E+01	8.E-02	2.E+00
Pm-147	4.E+ 4.E+ 04	1.E+06	4.E+02	1.E+04	4.E+01	1.E+03
Pu-238	6.E+ 01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Pu-239[b]/Be	6.E+ 6.E+ 01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ra-226	4.E+ 01	1.E+03	4.E-01	1.E+01	4.E-02	1.E+00
Se-75 2.E+	02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+ 03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Tm-170	2.E+ 2.E+ 04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Yb-169	3.E+ 02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Au-198*	2.E+ 02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Cd-109*	2.E+ 04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Co-57* 7.E+	02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Fe-55* 8.E+	05	2.E+07	8.E+03	2.E+05	8.E+02	2.E+04
Ge-68* 7.E+	02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Ni-63* 6.E+	04	2.E+06	6.E+02	2.E+04	6.E+01	2.E+03
Pd-103*	9.E+ 9.E+ 04	2.E+06	9.E+02	2.E+04	9.E+01	2.E+03
Po-210*	3.E+ 6.E+ 01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ru-106 (Rh-106)* 3.E+	02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Tl-204*	2.E+ 2.E+ 04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02

[a] The primary values are given in TBq while Ci values are provided for practical purposes.

[b] Criticality and safeguard issues will need to be considered for multiples of D.

∗ These radionuclides are very rarely used in individual radioactive sources.

Table 3: **Main elements of assigning the categories of radioactive sources to the security levels**

<table>
<tr><th>Security levels</th><th>Sources in Category 1

Security level A</th><th>Sources in Category 2

Security level B</th><th>Sources in Category 3

Security level C</th><th>Sources in Categories 4 and 5

Security level D</th></tr>
<tr><td rowspan="7">Security management</td><td colspan="4">Compliance with all general radiation safety regulations</td></tr>
<tr><td colspan="3">Control of access to the source location</td></tr>
<tr><td colspan="3">Basic background check of the personnel</td></tr>
<tr><td colspan="3">Plan for the protection of sensitive information</td></tr>
<tr><td colspan="3">Security plan for storage and use</td></tr>
<tr><td colspan="3">Actions in case of increased threat</td></tr>
<tr><td colspan="3">Reporting system</td></tr>
<tr><td>Detection</td><td>Immediate detection of unauthorized access by means of a remote intruder alarm</td><td>Immediate detection of unauthorized access by means of an intruder alarm</td><td>Ensuring means to detect unauthorized removal of sources</td><td></td></tr>
<tr><td>Delay</td><td>Source protected against unauthorized access with two physical security measures</td><td>Source protected against unauthorized access with two physical security measures</td><td>Source protected against unauthorized access with one physical security measure</td><td></td></tr>
<tr><td>Response</td><td>Immediate police response to a verified alarm</td><td>Immediate response of the police and personnel to an alarm</td><td></td><td></td></tr>
</table>

ANNEX III: TRANSPORT

Table 1: Security levels in transport

No.	Type of radioactive material in transport	Type of package in use	Transport security level
1.	Reference sources	Excepted	Minimum
2.	Consumer goods	Excepted	Minimum
3.	LSA I/II/III	IP-1, IP-2 or IP-3	Minimum
4.	LSO I/II	IP-1, IP-2 or IP-3	Minimum
5.	Radiopharmaceuticals	Type A	Basic
6.	Nuclear gauges	Type A	Basic
7.	Neutron sources for well logging	Type A	Basic
8.	Manual brachytherapy sources	Type A	Basic
9.	Industrial radiography sources	Type B (U/M)	Enhanced
10.	MDR and HDR brachytherapy sources	Type B (U/M)	Enhanced
11.	Teletherapy sources	Type B (U/M)	Enhanced
12.	Gama irradiators	Type B (U/M)	Enhanced
13.	Sealed sources for disposal	Type A or Type B (U/M)	Basic for Type A and enhanced for Type B(U/M)
14.	Specific cases	Special shipment	Additional security measures required