Sundhedsstyrelsen
National Institute of Radiation Protection
Knapholm 7, DK-2730 Herlev
Phone +45 4454 3454, email sis@sis.dk December 2009

Guidance on Security Requirements for Sealed Radioactive Sources

This Guidance explains the security and emergency response requirements stated in chapter 10 in The National Board of Health Order No. 985/2007 on sealed radioactive sources. Sealed radioactive sources above certain activity levels are divided into security groups A, B or C. The activity levels for the different groups can be found in Annex 2 in Order No. 985. Different security requirements apply to the three security groups.

Vulnerability analysis
A vulnerability analysis must be established for radioactive sources in security group A or B. Approval of the analysis has to be obtained from The National Institute of Radiation Protection (NIRP) before the radioactive sources can be purchased. The vulnerability analysis must identify threats, weaknesses and potential hazards that can affect the security of the radioactive sources. The vulnerability analysis must form the basis of the planning and implementation of preventive and damage limiting measures that reduce the risk to an acceptable level. Potential hazards that can affect the security of radioactive sources are fire, water damage, power failure, theft, vandalism, sabotage, terror etc.

Security plan
On the basis of the approved vulnerability analysis a security plan must be established and implemented. The security plan must as a minimum include:

- Identification of an individual responsible for the security of the radioactive sources. This individual could be the person in charge of radiation protection in the company, but it is not required that the responsible individual has radiation protection skills.

- Procedures ensuring that radioactive sources in security group A are accounted for on a daily basis, and radioactive sources in security group B are accounted for on a weekly basis. Records of these daily and weekly accounts must be registered.

- An access control system. This could be an electronic access control system with an event log covering an appropriate length of time, logging each access to the area, as well as the name of the individual and the time of access.

- At least two technical barriers for security A sources and one technical barrier for security group B sources. A technical barrier could be storing the radioactive source in a room with a locked door or securing the radioactive source to a stable part of the building e.g. chained to a hard point with a padlock. Door locks must be Danish SKAFOR security class red or corresponding. A patented, copy protected key system must be used.

- A 24-hour alarm system that detects unauthorized access to the area and ensures immediate response, i.e. the security company must arrive no later than 35 minutes after the alarm activation. The alarm system must be ID based and indicate the location of the activated alarm.

- Procedures for security approval of authorized individuals. The procedure must specify when a security approval is necessary and what level of security approval is needed. In some cases a clean criminal record could be sufficient documentation.

- Measures ensuring that sensitive information on radioactive sources or security related matters are not transferred to unauthorized individuals. Retrieval of oath of secrecy from authorized individuals is required.

It is not always possible to achieve the specified security requirements for radioactive sources used in the field or under transport. Therefore appropriate compensating measures must be implemented. This could be by securing the package containing the radioactive source to the vehicle either by a chain locked to the body of the vehicle or to loops incorporated in the vehicle. Parking of the vehicle in a garage that is locked and/or under 24-hour surveillance is another possibility. The compensating measures must be approved by NIRP.

Security measures must not compromise radiation safety and must not be a hindrance for intervention in case of an emergency.

An authorized individual must always be in charge of the security plan. The plan must be updated on a regular basis.

Emergency response plan
On the basis of the approved vulnerability analysis an emergency response plan must be established and implemented. The plan must be activated during incidents that compromise the security of the radioactive sources. The plan must as a minimum include:

- Measures and notification of the police and NIRP in case of accidents with radioactive sources including theft or loss of a radioactive source
- Measures in case of fire
- Measures in case of threats of/or other criminal incidents
- An emergency communication plan.

Emergency measures can include evacuation, warning and follow-up on incidents. An emergency communication plan includes normally a series of alarm calls that are to be initiated immediately after an alarm has occurred. The responsibility for the activation of the emergency communication plan must be placed by authorized individuals or a unit reachable at all times.

An authorized individual must always be in charge of the emergency response plan. The emergency response plan must be evaluated periodically and kept updated i.e. updating of contacts, phone numbers etc.

On request, NIRH must be given access to all relevant documentation concerning security plans and emergency response plans.