641—37.43 (136C) General security program requirements.

37.43(1) *Security plan.*

a. Each licensee identified in 37.41(1)*"a"* shall develop a written security plan specific to its facilities and operations. The purpose of the security plan is to establish the licensee's overall security strategy to ensure the integrated and effective functioning of the security program required by these rules. The security plan must, at a minimum:

(1) Describe the measures and strategies used to implement the requirements of these rules; and

(2) Identify the security resources, equipment, and technology used to satisfy the requirements of these rules.

b. The security plan must be reviewed and approved by the individual with overall responsibility for the security program.

c. A licensee shall revise its security plan as necessary to ensure the effective implementation of agency requirements. The licensee shall ensure that:

(1) The revision has been reviewed and approved by the individual with overall responsibility for the security program; and

(2) The affected individuals are instructed on the revised plan before the changes are implemented.

d. The licensee shall retain a copy of the current security plan as a record for three years after the security plan is no longer required. If any portion of the plan is superseded, the licensee shall retain the superseded material for three years after the record is superseded.

37.43(2) *Implementing procedures.*

a. The licensee shall develop and maintain written procedures that document how the requirements of these rules and the security plan will be met.

b. The implementing procedures and revisions to these procedures must be approved in writing by the individual with overall responsibility for the security program.

c. The licensee shall retain a copy of the current procedure as a record for three years after the procedure is no longer needed. Superseded portions of the procedure must be retained for three years after the record is superseded.

37.43(3) *Training.*

a. Each licensee shall conduct training to ensure that those individuals implementing the security program possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively. The training must include instruction in:

(1) The licensee's security program and procedures to secure category 1 or category 2 quantities of radioactive material, and in the purposes and functions of the security measures employed;

(2) The responsibility to report promptly to the licensee any condition that causes or may cause a violation of agency requirements;

(3) The responsibility of the licensee to report promptly to the local law enforcement agency and licensee any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material; and

(4) The appropriate response to security alarms.

b. In determining those individuals who shall be trained on the security program, the licensee shall consider each individual's assigned activities during authorized use and response to potential situations involving actual or attempted theft, diversion, or sabotage of category 1 or category 2 quantities of radioactive material. The extent of the training must be commensurate with the individual's potential involvement in the security of category 1 or category 2 quantities of radioactive material.

c. Refresher training must be provided at a frequency not to exceed 12 months and when significant changes have been made to the security program. This training must include:

(1) Review of the training requirements of rule 641—37.43(136C) and any changes made to the security program since the last training;

(2) Reports on any relevant security issues, problems, and lessons learned;
(3) Relevant results of agency inspections; and
(4) Relevant results of the licensee's program review and testing and maintenance.

d. The licensee shall maintain records of the initial and refresher training for three years from the date of the training. The training records must include dates of the training, topics covered, a list of licensee personnel in attendance, and related information.

37.43(4) *Protection of information.*

a. Licensees authorized to possess category 1 or category 2 quantities of radioactive material shall limit access to and unauthorized disclosure of their security plan, implementing procedures, and the list of individuals that have been approved for unescorted access.

b. Efforts to limit access shall include the development, implementation, and maintenance of written policies and procedures for controlling access to, and for proper handling and protection against unauthorized disclosure of, the security plan and implementing procedures.

c. Before granting an individual access to the security plan or implementing procedures, licensees shall:

(1) Evaluate an individual's need to know the security plan or implementing procedures; and

(2) If the individual has not been authorized for unescorted access to category 1 or category 2 quantities of radioactive material, safeguards information, or safeguards information-modified handling, the licensee must complete a background investigation to determine the individual's trustworthiness and reliability. A trustworthiness and reliability determination shall be conducted by the reviewing official and shall include the background investigation elements contained in 37.25(1).

d. Licensees need not subject the following individuals to the background investigation elements for protection of information:

(1) The categories of individuals listed in rule 641—37.29(136C); or

(2) Security service provider employees, provided written verification that the employee has been determined to be trustworthy and reliable, by the required background investigation in 37.25(1), has been provided by the security service provider.

e. The licensee shall document the basis for concluding that an individual is trustworthy and reliable and should be granted access to the security plan or implementing procedures.

f. Licensees shall maintain a list of persons currently approved for access to the security plan or implementing procedures. When a licensee determines that a person no longer needs access to the security plan or implementing procedures or no longer meets the access authorization requirements for access to the information, the licensee shall remove the person from the approved list as soon as possible, but no later than seven working days, and take prompt measures to ensure that the individual is unable to obtain the security plan or implementing procedures.

g. When the security plan is not in use, the licensee shall store its security plan and implementing procedures in a manner to prevent unauthorized access. Information stored in nonremovable electronic form must be password protected.

h. The licensee shall retain as a record for three years after the document is no longer needed:

(1) A copy of the information protection procedures; and

(2) The list of individuals approved for access to the security plan or implementing procedures.

[**ARC 1479C**, IAB 6/11/14, effective 7/16/14]