Ohio Administrative Code

Rule 3701:1-37-18 Monitoring, detection, and assessment.

Effective: November 3, 2019

(A) Monitoring and detection:

(1) Licensees shall establish and maintain the capability to continuously monitor and detect without delay all unauthorized entries into its security zones. Licensees shall provide the means to maintain continuous monitoring and detection capability in the event of a loss of the primary power source, or provide for an alarm and response in the event of a loss of this capability to continuously monitor and detect unauthorized entries.

(2) Monitoring and detection must be performed by:

(a) A monitored intrusion detection system that is linked to an onsite or offsite central monitoring facility;

(b) Electronic devices for intrusion detection alarms that will alert nearby facility personnel;

(c) A monitored video surveillance system;

(d) Direct visual surveillance by approved individuals located within the security zone; or

(e) Direct visual surveillance by a licensee designated individual located outside the security zone.

(3) A licensee subject to rules 3701:1-37-14 to 3701:1-37-22 of the Administrative Code shall also have a means to detect unauthorized removal of the radioactive material from the security zone. This detection capability must provide:

(a) For category one quantities of radioactive material, immediate detection of any attempted unauthorized removal of the radioactive material from the security zone. Such immediate detection capability must be provided by:

(i) Electronic sensors linked to an alarm;

(ii) Continuous monitored video surveillance; or

(iii) Direct visual surveillance.

(b) For category two quantities of radioactive material, weekly verification through physical checks, tamper indicating devices, use, or other means to ensure that the radioactive material is present.

(B) Assessment: licensees shall immediately assess each actual or attempted unauthorized entry into the security zone to determine whether the unauthorized access was an actual or attempted theft, sabotage, or diversion.

(C) Personnel communications and data transmission: for personnel and automated or electronic systems supporting the licensees monitoring, detection, and assessment systems, licensees shall:

(1) Maintain continuous capability for personnel communication and electronic data transmission and processing among site security systems; and

(2) Provide an alternative communication capability for personnel, and an alternative data transmission and processing capability, in the event of a loss of the primary means of communication or data transmission and processing. Alternative communications and data transmission systems may not be subject to the same failure modes as the primary systems.

(D) Response: licensees shall immediately respond to any actual or attempted unauthorized access to the security zones, or actual or attempted theft, sabotage, or diversion of category one or category two quantities of radioactive material at licensee facilities or temporary job sites. For any unauthorized access involving an actual or attempted theft, sabotage, or diversion of category one or category two quantities of radioactive material, the licensees response shall include requesting, without delay, an armed response from the LLEA.