COSMOS
Navigate the Compliance Universe

42 C.F.R. § 73.11

Security.

(a) An individual or entity required to register under this part must develop and implement a written security plan. The security plan must be sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release.

(b) The security plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use. A current security plan must be submitted for initial registration, renewal of registration, or when requested.

(c) The security plan must:

(1) Describe procedures for physical security, inventory control, and information systems control,

(2) Contain provisions for the control of access to select agents and toxins including the safeguarding of animals (including arthropods) or plants intentionally or accidentally exposed to or infected with a select agent, against unauthorized access, theft, loss or release.

(3) Contain provisions for routine cleaning, maintenance, and repairs,

(4) Establish procedures for removing unauthorized or suspicious persons,

(5) Describe procedures for addressing loss or compromise of keys, keycards, passwords, combinations, etc. and protocols for changing access permissions or locks following staff changes,

(6) Contain procedures for reporting unauthorized or suspicious persons or activities, loss or theft of select agents or toxins, release of select agents or toxins, or alteration of inventory records, and

(7) Contain provisions for ensuring that all individuals with access approval from the HHS Secretary or Administrator understand and comply with the security procedures.

(8) Describe procedures for how the Responsible Official will be informed of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins; and describe procedures for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of such activity.

(9) Contain provisions for information security that:

(i) Ensure that all external connections to systems which manage security for the registered space are isolated or have controls that permit only authorized and authenticated users;

(ii) Ensure that authorized and authenticated users are only granted access to select agent and toxin related information, files, equipment (*e.g.*, servers or mass storage devices) and applications as necessary to fulfill their

roles and responsibilities, and that access is modified when the user's roles and responsibilities change or when their access to select agents and toxins is suspended or revoked;

(iii) Ensure that controls are in place that are designed to prevent malicious code (such as, but not limited to, computer virus, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to spaces registered under this part or records in § 73.17;