

LABORATORY SECURITY

Introduction

ASU recognizes the unique characteristics and hazards of a laboratory workplace. As a result of the disaster of September 11th, domestic terrorism, and other potentials for threats in our workplace, ASU has determined those campus laboratories and other facilities present vulnerabilities to University security. ASU has been developing an enterprise Security Policy that incorporates building access, construction design standards, emergency response, and associated policies to address these threats.

The “Lab Safety & Security Initiative” originated in September 2003 and included a comprehensive risk analysis method for categorizing and prioritizing security system installations on campus laboratory facilities. Funds were allocated to install the ISSAC door access system using the Suncard as the key to secure individual campus laboratories. The goal was “To provide an enterprise system for all campuses with coordinated Policies and Procedures for a true integrated security access control system”.

Laboratory Security issues included:

- Laboratory doors are closed and locked at all times.
- The Suncard is the only authorized method of entry and the hard keys will be eliminated.
- Tampering or disabling of any security device is grounds for immediate disciplinary action.
- Principle Investigators or Laboratory Managers are responsible for ensuring compliance.
- Managers of the system, i.e. hardware and software, must be ASU employees and pass a background check.

Applicable ASU Guidelines

- Security Plan (pending)
- Chemical Hygiene Plan
- Senior Security Committee (pending)
- Building Access Policy (DPS206)

Applicable Regulations

- Uniform Building Code, Ch 3, §§ 304.2.2.1

Summary of Requirements

All individuals granted access to laboratories with electronic access doors and/or containing specialized security systems must comply with the security policy and procedures:

- Laboratory doors must be kept closed and locked at all times except when entering the area.
- The access card is the only authorized method to register individual access to the area. Override keys, tailgating etc... are not allowed.
- Cardholders are required to register access of a secured laboratory by using the individually assigned card access for individual entry. |
- Cardholders are expected to immediately report the presence of unfamiliar individuals and/or suspicious activities in laboratories immediately to University Police or the Sites Security Service.
- Security devices are never to be disabled.
- Cardholders must immediately report disabled/broken or otherwise compromised security devices to FACMAN or the designated building manager.

- Research or other activities involving the use of laboratory space, materials or equipment without the knowledge and approval of the responsible Principal Investigator/Designated Responsible Faculty member is strictly prohibited.
- Visitors are properly registered by the employee who allows visitors through the access system door and the employee is responsible for the visitor while in the laboratory.

Emergency Response personnel accessing laboratories while in response to emergency situations that may cause immediate and serious harm to people or the environment are exempt.

Training

ASU provides employees with information and training to understand the ISSAC door access system. EH&S offers training on risk assessment for those laboratories that require more sophisticated security system.

Employees must be informed and/or trained on the contents of the ASU laboratory security program and construction standards and supporting documents when considering new constructing activities or remodeling existing spaces.

ASU Resources

This list has not been finalized and depends on additional documents being created and approved.

ASU Access Control Policy
Arizona State University Emergency Operations Manual
SUNCARD Policy
Door Access Request and Approval Procedure
ISAAC User Guide (Segment Manager)
ISAAC Key Control Manager (formerly Area Manager) Guide
ISAAC Technical Support Manual (System Administrators/IT Staff)
ISAAC Hardware Service and Support Manual
ISAAC System Administrator Procedures
Door Access Request and Approval Procedures
Emergency Response, Hard Key Override, Alarms for areas with Electronic Door Access

Updated 11/21/06