



Biorisk Documentation

Biosecurity Inspector Training

Staten Serums Institut
31 August – 2 September 2009

www.biosecurity.sandia.gov

SAND No. 2009-5485C

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.





Biorisk Documentation: Discussion

- **Policies**
 - Prepared by:
 - Purpose: to
- **Plans or Manuals**
 - Prepared by:
 - Purpose:
- **Standard Operating Procedures (SOPs)**
 - Prepared by:
 - Purpose:



Biosecurity Plan

- ***Biosecurity plans* are procedures and mitigation strategies ultimately designed to protect biological materials and related valuable assets against unauthorized**
 - Access
 - Theft
 - Loss
 - Release
 - Sabotage
- **Incident response plans describe methods by which facilities respond to various incidents**
 - Natural
 - Medical
 - Biosecurity
 - Security
- **Based on facility-wide risk assessment**
- **Coordinate with facility-wide plans and procedures**



Biosecurity Plan Contents

- **Summary of Risk Assessment**
 - Site-specific
 - Agent-specific
 - Facility wide
 - Summarize threats, vulnerabilities, risks
- **Plan language**
 - Refers to the assessments and conclusions
 - Identify and elaborate on resulting security measures
- **Detailed descriptions of procedures and protocols necessary to mitigate unacceptable risks to protect valuable materials**
 - Physical security
 - Information security
 - Material in transit
 - Material accountability and control
 - Personnel
- **Incident Response Plans**



US Select Agent Rule: Security Plan

- **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.
 - Describe procedures for physical security, inventory control, and information systems control
 - Contain provisions for the control of access to select agents and toxins
 - Contain provisions for routine cleaning, maintenance, and repairs
 - Establish procedures for removing unauthorized or suspicious persons
 - Describe procedures for addressing loss or compromise of keys, passwords, combinations, etc. and protocols for changing access numbers or locks following staff changes
 - 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
 - Contain provisions for ensuring that all individuals with access approval from understand and comply with the security procedures



Biorisk Documentation: Discussion

- **Review the Security Plan Template in your binder that is provided by the US Select Agent Program**
 - What are the strengths and weaknesses of the template?
 - How should a security plan for a laboratory in Denmark differ?



Purpose of SOPs

- **Ensure all relevant individuals understand the process**
- **Document how activities shall be performed**
 - Facilitate consistency
 - Ensure compliance with regulations
- **Types of SOPs**
 - Repetitive technical activities
 - Sample receipt and processing
 - Diagnostic test procedures
 - Administrative procedures
 - The process for proper documentation of training
 - Laboratory Access Authorization
 - Response Activities
 - Building evacuation
 - Suspicious individuals and activities
 - Medical emergencies



Documentation

- **Documentation**
 - Retention times should be determined for all types of documentation
 - Methods of documentation should be determined for each type of information requiring documentation
 - Maintain control of documentation containing potentially sensitive information
 - Personnel records
 - Access control or security systems
 - Biological agent specific information
 - The plan should describe methods of control for potentially sensitive documentation
 - Samples of all forms should be included in an appendix of the plan



Extra Slides



Biosecurity Plan: Physical Security

- **Description of physical security systems**
 - Systems in place
 - System applications
- **Procedures for entry and exit**
 - During business hours
 - After business hours
- **Alarm response procedures**
- **Response actions for security breaches**



Biosecurity Plan: Information Security

- **Descriptions of systems in place to protect information**
 - Electronic
 - Passwords
 - Firewalls
 - Encryption
 - Hard copy records
 - Information classification
 - Mechanisms in place to control sensitive information
 - “Need to know”
 - Backup systems
 - Key control program for mechanical keys
 - Theft, loss
 - Unauthorized duplication



Biosecurity Plan: Material in Transit

- **Procedures for how biological materials are handled**
 - Packaging requirements
 - Internal transfer processes
 - External transfer processes
 - Shipment tracking
 - Material monitored until pick up by appropriate carrier
 - Verify receipt of shipment
 - Verification of receiving persons
 - Legitimate need and proper approval
 - Material receipt procedures



Biosecurity Plan: Material Control and Accountability

- **Inventories**
 - Policies and procedures for conducting and maintaining inventories
 - Appropriate for material
 - Stock cultures
 - Animals
 - Toxins
 - Self-replicating organisms
 - Current
 - Limited access
 - Password
 - Keys



Biosecurity Plan: Personnel

- **Descriptions of provisions for different types of personnel (escorted and unescorted)**
 - Maintenance personnel
 - Visitors
 - Repair personnel
 - Cleaning staff
- **Granting access**
- **Removing access**
- **Suitability screening**
 - Background investigation
 - Credential verification
 - Education verification



Biosecurity Plan: Incident Response

- **Response procedures**
 - Theft, loss, misuse, release
 - Suspicious persons
 - Suspicious activities
 - Suspicious items
 - Natural disasters
 - Medical
 - Life threatening
 - Non-life threatening
 - Power outage/electrical failure
 - Equipment failure
 - Proper reporting mechanisms
 - Proper methods to securing an area
- **Reporting procedures**
 - Theft, loss, release
 - Incidents
 - Documentation



Biosecurity Plan: Training

- **Types**
 - Initial training
 - Ongoing training
 - Refresher training
- **Required for all plans and procedures**
- **Consider method to validate successful completion of training**



Biosecurity Plan: Drills and Exercises

- **Plans and procedures should be validated by performing either drills or exercises**
 - After initial development
 - After an event
 - When procedures are changed or new procedures are developed
 - Review and revise on a routine basis
 - Annually
 - Every two to three years at least