**Planning and Implementing Practical Exercises and Drills SOP**

INSTRUCTIONS: The below document is identified as a draft to be customized in consultation with INSTITUTION NAME personnel to ensure it is accurately describing site procedures and requirements.

* **Black text** can be considered generic text that may be appropriate for inclusion.
* ***Red text*** should be considered guidance or examples and must be reviewed and replaced with facility-specific information.
1. **Scope**

This document applies to all Security and Biosecurity Exercises and Drills at INSTITUTION NAME.

1. **Purpose**

The purpose of this document is to describe the planning and implementation of practical exercises and drills at INSTITUTION NAME.

1. **Principle**
	1. Regular exercises and drills are a critical component of the security and biosecurity program at INSTITUTION NAME. Proper exercises and drills ensure security methods, plans, and staff are working effectively. They also serve to improve performance which can save lives and property during an incident.
	2. The types of exercises and drills that may be conducted are:
		1. **Tabletop exercise** - A low-stress discussion of coordination and policy. They provide a good environment for problem-solving and an opportunity for key personnel and stakeholders to become acquainted with the Security, Biosecurity, and Emergency Plan and to one another. They also provide good preparation for a drill or functional exercise.
		2. **Drill** - A coordinated, supervised exercise, normally used to test a single specific operation or function. There is no attempt to coordinate a response from all parties that would be involved in an actual incident or emergency.
		3. **Functional exercise** - A fully simulated interactive exercise that tests the capability of an organization to respond to a simulated emergency incident. The exercise tests multiple functions of the organization’s operational plan. It is a coordinated response to a situation in a time-pressured, realistic simulation.
2. **Responsibility**
	1. It is the responsibility of the Security Manager to ensure that security & biosecurity exercises and drills are scheduled, conducted, and documented at least annually.
	2. The Security Manager will develop the exercises and drills in conjunction with the Biorisk Management (BRM) team.
3. **Definition and Abbreviations**

**Alternate Responsible Official:** The person with authority and responsibility to ensure security requirements for restricted and biological restricted areas are met in the absence of the RO.

**Assistant Biological Safety Officer (ABSO):** The person who is responsible for identification and management of biological safety in particular, and biological risks in general, throughout the INSTITUTION NAME, in liaison with other members of the Biorisk Management Committee, Department Heads, and the staff of the INSTITUTION NAME in the absence of the BSO.

**Biological Restricted Area:** Biological Safety Level (BSL) 2 and 3 laboratories and any areas containing identified Especially Dangerous Pathogens (EDPs) and Valuable Biological Materials (VBMs) or areas where access to EDPs/VBMs is possible. Entry will be subject to special access restrictions. Physical security controls will be used to control access and secure property and materials. Biological Restricted Areas may be of different types depending on the nature and varying degree of access to EDPs/VBMs, or other relevant matter contained in the area.

**Biological Safety Officer (BSO):** The individual responsible for the identification and management of biological safety in particular, and biological risks in general, throughout the INSTITUTION NAME, in liaison with other members of the Biorisk Management Committee, Department Heads, and the staff of the INSTITUTION NAME. The BSO is the senior RO for all matters related to safety and biological safety at INSTITUTION NAME.

**Certifying Official(s)**: The person (or committee of people) responsible for certifying personnel for access to Restricted and Biological Restricted Areas.

**Deputy Security Manager:** A full-time employee (FTE), the Deputy Security Manager Is responsible for assisting the Security Manager in managing the security operations for INSTITUTION NAME. In addition, in the absence of the Security Manager or when the Security Manager must fulfill other, exclusive functions (e.g., Incident Commander), the Deputy Security Manager is responsible for the day-to-day security of INSTITUTION NAME, its personal assets, equipment, materials, cultures, specimens, and the protection of the public and the environment as related to security and biological security at INSTITUTION NAME.

**Especially Dangerous Pathogen (EDP)**: Those pathogens on the United States Select Agents List and others that may be determined by the (enter governing body here), or other governing body, to have the potential to pose a severe threat to the public, animal or plant health, or to animal or plant products.

**Incident Commander:** The person with overall responsibility for all aspects of an emergency response, including quickly developing incident objectives, managing all incident operations, application of resources as well as responsibility for all persons involved.

**Personnel Reliability Plan:** The plan to ensure that each individual who is authorized to access EDPs, and to escort and/or supervise personnel with access to Biological Restricted Areas and EDPs, including BSO/ABSO, Security Managers, Responsible and Certifying Officials, meet the highest standards of integrity, trust, personal reliability, and accountability so as to ensure these individuals do not pose a risk to the public health and safety, the environment or national security.

**Responsible Official (RO):** An individual, as designated by the Director of INSTITUTION NAME, who has the authority and responsibility to ensure security requirements for restricted and biological restricted areas are met.

**Restricted Area:** An area designated by the Director of INSTITUTION NAME (or by request of the Responsible Official (RO), Security Manager, or BSO) that houses valuable, sensitive, or hazardous material and requires access control.

**Security Manager:** A full-time employee (FTE), the Security Manager is responsible for the day-to-day security of INSTITUTION NAME, its personal assets, equipment, materials, cultures, specimens, and the protection of the public and the environment as related to security and biological security at INSTITUTION NAME. The Security Manager is the senior RO for all matters related to the security and biosecurity at INSTITUTION NAME.

**Valuable Biological Materials (VBMs)**: Biological materials that require (according to their owners, users, custodians, caretakers, or regulators) administrative oversight, control, accountability, and specific protective and monitoring measures in laboratories to protect their economic and historical (archival) value, and/or the population from their potential to cause harm. VBM may include pathogens and toxins, as well as non-pathogenic organisms, vaccine strains, foods, genetically modified organisms (GMOs), cell components, genetic elements, and extraterrestrial samples.

1. **Reagents:**

 Not applicable

1. **Materials:**

Not applicable

1. **Related Directives**

INSTITUTION NAME Security and Biosecurity Plan

INSTITUTION NAME Personnel Reliability Plan

INSTITUTION NAME Job Description - Security Manager

INSTITUTION NAME Job Description – Deputy Security Manager

INSTITUTION NAME Job Description – Certifying Official

INSTITUTION NAME Job Description – Incident Commander

INSTITUTION NAME Job Description – Biological Safety Officer

INSTITUTION NAME Job Description – Assistant Biological Safety Officer

### Procedure

* 1. Before a drill or exercise is conducted, the Security Manager or designee notifies all appropriate agencies, including the local fire, police, medical first responders, and government ministry.
	2. Upon completion of the drill or exercise, the Security Manager will prepare a report detailing the results of the exercise. The report should include the details of the drill and any conclusions or lessons learned which may result in a revision of the BRM Plan. A copy of reports detailing drills or exercises involving biological agent incident response should be completed and reviewed in a timely manner.
	3. Examples of Security Drill types that should be planned for and be practiced both in theoretical tabletop exercises and in practical exercises include:
		1. Attempted break-in (day/night) one or more persons.
			1. Identification of attempt
			2. Notification of external response force
			3. Protecting staff
			4. Notifying site management
			5. Delaying and/or apprehending the perpetrators
			6. Remedial actions to improve processes
		2. Protest blocking access to the site.
			1. Blocking access to the site in a diplomatic way, not escalating the situation
			2. Notification of site management
			3. Notification of off-site response force
			4. Notification to staff regarding the situation
			5. Remedial actions to improve processes
		3. Bomb threat and building evacuation.
			1. Identification of potential bomb location
			2. Notification of emergency services
			3. Notification of management
			4. Movement of staff to safe areas within the building or evacuation to a safe area of the site, or even off-site
			5. Remedial actions to improve processes
		4. Armed intruder on-site (day / night).
			1. Facility lockdown
			2. Notification of management
			3. Notification of staff
			4. Notification of off-site response force
			5. Monitoring of intruder location until arrival of response force
			6. Actions to apprehend the intruder maximizing INSTITUTION NAME and Security staff safety
			7. Remedial actions to improve processes
		5. Response by off-site response force.
			1. Verifying effective communications
			2. Verifying response times for the various emergency response organizations – off-site security response force, Security, Medical, Fire
			3. Verifying procedures with off-site response groups – where to meet during differing events, communications tree management of emergencies on-site – command and control
			4. Remedial actions to improve processes
		6. Response to a missing EDP/VBM or other critical assets from storage areas.
			1. Reporting to Security
			2. Security actions
			3. Biosafety actions
			4. Investigation process and possible actions
			5. External reporting requirements
			6. Remedial actions to improve processes
	4. Response to accidental release of an EDP, other infectious or hazardous chemicals – airborne, via drains, via waste taken off-site without decontamination.
		+ 1. Reporting
			2. Notification of management
			3. Verification of event
			4. Protection of INSTITUTION NAME staff
			5. Protection of the local community if deemed necessary
			6. Protection of the environment
			7. Contact with relevant local authorities and Ministries
			8. Management of situation – internal to INSTITUTION NAME /external to INSTITUTION NAME
			9. Remedial actions to improve processes

# Safety Instructions

# Comply with all INSTITUTION NAME safety policy, while following the procedures described in this document.

#  Reference

* INSTITUTION NAME Security and Biosecurity Plan
* INSTITUTION NAME Personnel Reliability Plan
* World Health Organization Biorisk Management Laboratory Biosecurity Guidance, September 2006
* European Committee for Standardization, Comité Europé De Normalisation (CEN) Europäisches Komitee Fűr Normung, Workshop Agreement (CWA) 15793
* United States Federal Select Agent Program