**Incoming Package Inspection SOP**

INSTRUCTIONS: The below document is identified as a draft to be customized in consultation with INSTITUTION NAME personnel to ensure it accurately describes 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 packages that are destined to enter the INSTITUTION NAME.

1. **Purpose**

The purpose of this document is to describe the process for inspecting incoming packages at INSTITUTION NAME.

1. **Principle**
   1. Establishing an Access Control Point (ACP) at a centralized mail and package handling operations in a separated location (“mail center”) from other INSTITUTION NAME buildings are one of the best ways to minimize risk to INSTITUTION NAME personnel and the public.
   2. Having a separate mail center reduces risk by limiting exposure to potentially dangerous mail and packages to a single location and fewer people. Establishing a single location allows for a trained staff to work with increased efficiency and with standardized procedures. A properly constructed mail center is a highly effective preventative security measure.
   3. The following are suggested physical layout characteristics for mail centers:
      1. Make all work areas visible to supervisors.
      2. Use one-way glass, closed-circuit video surveillance cameras, or elevated supervisor stations.
      3. Eliminate desk drawers and similar places of concealment.
      4. Ensure adequate supervision of mail center staff, who may have access to thousands of dollars’ worth of merchandise, remittances, and company credit cards.
      5. Control access to your mail center and handling areas. The use of sign-in/out sheets, card key access-control systems, and photo ID badges are all effective security procedures. Extend this control to all employees, including cleaning and maintenance staff.
      6. Enforce limited access to your mail center. Only authorized employees should be allowed in the working areas of your mail center.
      7. Use a counter or desk to separate the area where employees pick up mail from the rest of the mail center.
      8. Have mail center personnel screened according to the INSTITUTION NAME Personnel Reliability Plan.
      9. Clearly label authorized receptacles mail.
      10. Ensure that mailroom location, furniture, and mail flow provide maximum security.
      11. Install alarms and surveillance equipment in the mail center.
      12. Limit mailroom access to authorized personnel.
      13. Eliminate mail distribution delays.
      14. Lock high-value items overnight in secure storage rooms.
      15. Verify and secure accountable items.
      16. Use containers and sacks when possible.
      17. Do not leave mail in an unsecured area and deliver outgoing mail directly to Postal Service custody.
      18. Ensure employee parking is separated from the mail delivery area.
      19. Immediately report lost or rifled mail to the security department
      20. Ensure supervisors can see all employees and work areas.
      21. Screen contractors who provide delivery services.
      22. Periodically test mail for loss and for quality control.
      23. Establish procedures for handling unexplained or suspicious letters and packages (the focus of this SOP).
2. **Responsibility**

# It is the responsibility of all personnel assigned to mail and package handling to follow the procedures described in this document.

# 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 Emergency and Incident Response 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. Any packages that are delivered to INSTITUTION NAME are first examined at the INSTITUTION NAME mail center. Packages are to be examined by visual or other non-intrusive means prior to physical entry into the interior of the INSTITUTION NAME campus. An X-ray machine for package inspection shall be located at the mail center. The package may be scanned via X-ray at the discretion of the employee and/or security who deal with mail delivery. Additionally, a Class 2, B2 Biological Safety Cabinet (BSC) shall be located at the mail center, along with all required materials to operate the BSC for mail and package inspections.
  2. Employees and security personnel who deal with mail delivery are to be trained to notify the Security Department following the receipt of a suspicious package or X-ray of an incoming package thought to be suspicious, and to not allow physical delivery of the package to within the administrative or laboratory zones of the facility until the Security Manager has cleared the suspect package in the mail center.
  3. A suspicious package is any package or item that does not appear to be consistent with what is expected during normal daily operations. The following are indicators to be considered:
     1. Misspelled words on the package
     2. Addressed to a title only or to an incorrect title
     3. Badly taped or sealed package
     4. Lopsided or uneven with respect to packaging
     5. Oily stains, discolorations, or crystallization on the wrapping
     6. Leaking or appears to have leaked any fluid
     7. Excessive tape or string used
     8. Protruding wires
     9. Return address does not exist or does not make sense with respect to the indicated contents of the package
  4. In the event a suspicious package is identified; the following procedures are to be followed:
     1. **Remain Calm, do not use** two-way radios or cellular phones; radio signals have the potential to detonate any potential explosive device.
     2. **Do not** touch or move a suspicious package, wait for it to be evaluated by trained responders.
     3. Evaluate the threat potential and consider evacuating the building immediately.
     4. Contact the security department and inform them of the situation.
     5. The Security Manager will respond and determine the need to notify the BSO (if there is any indication the material is biological). Additionally, the Security Manager may, at their discretion, contact the following:
        1. RO for the mail/package destination.
        2. Director
        3. Off-Site Response Force
     6. If the BSO is requested, the Security Manager will consult the BSO to determine the best course of action (e.g., inspect the package in the BSC or x-ray machine, evacuate, request Off-Site Response Force).
     7. The Security Manager will identify to whom the suspicious package is addressed and contact them to determine if they were expecting the package. They will verify the sending entity’s information and conduct any investigation needed to clear the package.
     8. If the package cannot be cleared or the Security Manager chooses for any other reason, they may request a response by the Off-Site Response Force, informing them of the situation during the request.
     9. Evacuate the area as needed. The typical evacuation is 300 meters away from the potential explosive but is dependent on the environment and other surrounding hazards.
     10. Follow all directions of the Incident Commander (IC). Refer to the INSTITUTION NAME Emergency and Incident Response Plan for details on IC designation and roles.
     11. Wait for the “All Clear” from the IC before re-entering the affected area.

# Safety Instructions

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

# Reference

* INSTITUTION NAME Security and Biosecurity Plan
* INSTITUTION NAME Personnel Reliability Plan
* INSTITUTION NAME Emergency and Incident Response 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