SOP: Secure Handling of Confidential or Sensitive Mail

This SOP details the **secure handling of confidential or sensitive mail**, including proper identification and labeling, access restrictions, secure transportation methods, controlled distribution, and protocols for reporting any breaches or suspicious activities. The aim is to protect sensitive information from unauthorized access, ensure privacy, and maintain the integrity of confidential communications throughout the mail handling process.

1. Purpose

To establish procedures for the secure handling, transport, storage, and distribution of confidential or sensitive mail to protect sensitive information from unauthorized access or disclosure.

2. Scope

This SOP applies to all employees, contractors, and relevant third parties involved in the handling, processing, or delivery of confidential or sensitive mail within the organization.

3. Definitions

Term	Definition
Confidential Mail	Any physical or electronic mail containing sensitive, proprietary, or private information.
Sensitive Mail	Mail that could harm individuals or the organization if disclosed to unauthorized persons.
Authorized Personnel	Individuals with explicit permission to handle or access confidential or sensitive mail.

4. Responsibilities

- **Mailroom Staff**: Ensure all receiving, logging, and distribution procedures are followed.
- **Supervisors/Managers**: Oversee training, compliance, and breach reporting.
- **Authorized Recipients**: Maintain security of all confidential mail received and report any breaches immediately.

5. Procedures

5.1 Identification and Labeling

- Confidential or sensitive mail must be clearly marked with "CONFIDENTIAL" or an equivalent label.
- Only authorized personnel should apply or remove such labels.

5.2 Access Restrictions

- Only designated, trained staff may receive, open, process, or distribute confidential mail.
- Mail must be stored in a locked, secure location with access logs maintained.

5.3 Secure Transportation

- Transport confidential mail in tamper-evident envelopes or locked containers.
- Hand-deliver mail to authorized recipients. Avoid leaving sensitive mail in unattended or public areas.

5.4 Controlled Distribution

- Require recipient signature upon delivery.
- Record date, time, and recipient details for all distributed confidential mail.

5.5 Reporting Breaches or Suspicious Activities

- Immediately report any loss, theft, tampering, or suspicious activity to management and security.
- Document all incidents as per the organization's incident response protocol.

6. Training

All relevant personnel must complete annual training in secure mail handling and information security best practices.

7. Document Control

- **SOP Owner:** [Department/Individual Name]
- **Approval Date:** [Date]
- **Next Review Date:** [Date]
- **Version:** [Version Number]