SOP: Documentation and Record-Keeping for All Mail Transactions

1. Purpose

This SOP details the processes for **documentation and record-keeping for all mail transactions**, including accurate logging of incoming and outgoing mail, maintaining organized records for tracking and auditing purposes, ensuring confidentiality and data protection, timely updating of mail status, and compliance with legal and organizational requirements. The goal is to enhance mail management efficiency, accountability, and traceability through systematic documentation practices.

2. Scope

This procedure applies to all personnel responsible for handling, documenting, and maintaining records of incoming and outgoing mail within the organization.

3. Responsibilities

- Mailroom staff: Primary responsibility for recording all mail transactions accurately and maintaining records.
- Department heads: Monitor compliance and perform periodic audits of records.
- All staff: Ensure confidential mail is handled according to data protection policies.

4. Procedures

4.1 Logging Incoming Mail

- Upon receipt, log each mail item with the following details:
    - Date and time of receipt
    - Sender's name and address
    - Recipient's name and department
    - Brief description of contents (if applicable)
    - Unique transaction/reference number
- Update the mail log (physical logbook or digital system) in real-time.

4.2 Logging Outgoing Mail

- Before dispatch, log each outgoing item with the following details:
    - Date and time of dispatch
    - Sender's name and department
    - Recipient's name and address
    - Brief description of contents (if applicable)
    - Carrier/Courier information (if applicable)
    - Tracking/reference number
- Timely update the mail status in the record system to track delivery and receipt.

4.3 Record Organization & Maintenance

- Maintain all mail records in an organized manner (by date, department, or transaction number).
- Ensure physical records are kept in secure, access-controlled locations.
- Back up digital records regularly and protect them with appropriate cybersecurity measures.
- Retain records for the required duration per policy or legal requirements before secure disposal.

4.4 Confidentiality and Data Protection

- Restrict access to mail records to authorized personnel only.
- Handle confidential or sensitive mail in accordance with organizational data protection guidelines.
- Report any breaches in confidentiality or lost mail records immediately as per incident response policy.

4.5 Audit and Compliance

- Conduct regular audits of mail transaction logs to check for accuracy, completeness, and compliance.

- Document audit findings and carry out corrective actions if discrepancies are found.
- Ensure that procedures align with applicable legal and organizational records management requirements.

5. Documentation

Document	Format	Retention Period	Storage Location
Mail Log Book/Database	Physical/Digital	5 years (or as specified)	Mailroom/Designated server
Audit Reports	Digital	3 years	Compliance Office/Records Archive
Incident Reports	Digital	7 years	Security Office

6. References

- Organizational Data Protection Policy
- Records Retention Schedule
- National/Local Regulatory Requirements

Reviewed by: _____ | Date: _____

Next Review Due: _____