SOP Template: Temporary Mail Storage and Secure Archiving

This SOP details **temporary mail storage and secure archiving** procedures, including proper handling of incoming and outgoing mail, secure classification and storage methods, access controls, retention timelines, and protocols for eventual disposal or permanent archiving. The purpose is to ensure the confidentiality, integrity, and availability of mail items while maintaining compliance with organizational policies and legal requirements.

1. Scope

This procedure applies to all staff involved in the receipt, handling, storage, archiving, and disposal of internal and external mail.

2. Responsibilities

- **Mailroom Staff:** Receive, document, classify, and store mail.
- **Supervisors:** Ensure adherence to procedures and authorize access.
- **IT/Admin:** Oversee digital archiving and destruction processes.
- **All Employees:** Adhere to confidentiality and security protocols.

3. Procedure

3.1 Handling Incoming Mail

- Log all incoming mail in the **Mail Register** upon receipt.
- Inspect for security threats and unauthorized items.
- Classify mail as **Confidential**, **Internal**, or **General** as per policy.
- Distribute promptly to intended recipients or store securely if undelivered.

3.2 Outgoing Mail Handling

- Log all outgoing mail in the **Outgoing Mail Register** with recipient details.
- Package and label according to security requirements.
- Coordinate with authorized couriers or postal services.

3.3 Temporary Storage of Mail

- Store undelivered or classified mail in a **designated, access-controlled area**.
- Restrict access only to authorized personnel.
- Review and reconcile mail inventory daily.

3.4 Secure Archiving

- Transfer mail/items for archiving to secure storage after **[X Days]** in temporary storage.
- Digitize documents when possible and log in the archival management system.
- Retain records per **Retention Schedule** (see below).
- Keep physical and electronic archives locked and access-controlled.

3.5 Access Controls

- Maintain updated access lists for storage and archives.
- Grant/deny access at supervisor's discretion, with proper logging of access events.
- Audit access logs quarterly for unauthorized activity.

3.6 Retention Timeline & Disposal

Type of Mail	Retention Period	Disposal Method
General Correspondence	6 months	Shredding / Secure Deletion
Legal/Financial Documents	5 years	Shredding / Secure Deletion

Confidential Information	7 years	Shredding / Secure Deletion
Permanent Records	Indefinite	Archive Securely

3.7 Final Disposal

- Destroy expired records by shredding or secure digital deletion, witnessed by a supervisor.
- Log disposal actions, method used, and personnel involved.

4. Compliance & Security

- Comply with relevant organizational, legal, and regulatory data protection standards.
- Report and investigate any suspected breaches in mail handling or storage.
- Review and update this SOP annually or as needed.

5. References

- Organizational Data Protection Policy
- Local and National Regulations on Records Retention
- Archival Management Guidelines

6. Revision History

Date	Version	Description of Changes	Approved By
2024-06-10	1.0	Initial SOP Release	[Name]