

SOP: Physical Document Filing and Security Measures

This SOP details the **physical document filing and security measures** necessary to ensure organized, secure, and efficient management of all physical records. It covers proper classification, labeling, storage, access control, and regular auditing of documents to prevent loss, damage, or unauthorized access. The procedure aims to maintain the confidentiality, integrity, and availability of physical documents essential for organizational operations and compliance with regulatory requirements.

1. Purpose

To establish standard procedures for filing, securing, and managing physical documents to protect against loss, unauthorized access, and ensure compliance with legal, regulatory, and organizational requirements.

2. Scope

This SOP applies to all departments and personnel responsible for the creation, handling, storage, and disposal of physical documents within the organization.

3. Responsibilities

- **Records Custodian:** Maintains overall responsibility for document management and security.
- **Department Heads:** Ensure staff compliance with this SOP within their units.
- **All Staff:** Adhere to filing, access, and security procedures outlined herein.

4. Procedure

1. Document Classification

- Classify documents based on sensitivity: Confidential, Internal Use, or Public.
- Clearly mark classification on the document cover or folder.

2. Labeling and Indexing

- Label files with unique identifiers (e.g., file number, title, date).
- Maintain an up-to-date index or log book for all stored documents.

3. Storage

- Store documents in secure, lockable filing cabinets or rooms designated for record storage.
- Ensure storage areas are clean, dry, and protected from fire, flood, pests, and sunlight.

4. Access Control

- Restrict access to authorized personnel only.
- Keep a sign-in/sign-out register or implement a key/card access system for storage areas.

5. Document Retrieval and Return

- Log all document retrievals and returns in the register.
- Return files immediately after use and ensure they are placed back in their original location.

6. Auditing and Monitoring

- Conduct periodic audits (at least annually) to verify document location and condition.
- Identify and report any missing, damaged, or misplaced records.

7. Disposal of Documents

- Follow approved retention schedules for document disposal.
- Shred or incinerate sensitive/confidential documents under supervision.

5. Security Measures

- Keep storage areas locked when unattended.
- Install fire alarms, smoke detectors, and fire extinguishers in storage areas.
- Use CCTV or security patrols for high-sensitivity record rooms.
- Prohibit food, drinks, and unauthorized electronic devices in storage areas.

6. Non-Compliance

- Violation of this SOP may result in disciplinary action as per organizational policies.

7. Review and Revision

- This SOP shall be reviewed annually or when significant changes in regulations or business practices occur.

Document Owner: [Insert Responsible Department]
Effective Date: [Insert Date]
Review Date: [Insert Date]