Standard Operating Procedure (SOP)

Controlled Document Storage and Archival Methods

Purpose:

This SOP details **controlled document storage and archival methods**, covering the systematic processes for secure storage, proper categorization, retention schedules, access control, and efficient retrieval of important documents. The goal is to ensure document integrity, confidentiality, compliance with regulatory requirements, and easy accessibility throughout the document lifecycle.

Scope:

This SOP applies to all personnel responsible for managing controlled documents, both physical and digital, within the organization.

Responsibilities:

- **Document Owner:** Ensures proper classification, labeling, and handover to authorized storage personnel.
- **Records Management Staff:** Manages storage, tracking, access, retrieval, and destruction processes.
- **IT Administrator:** Maintains security and integrity of digital storage systems.
- **All Employees:** Must comply with procedures for document handling, storage, and access.

Procedure:

1. **Document Categorization and Classification**
   - Classify documents as per their sensitivity (e.g., confidential, restricted, public).
   - Label each document with a unique identifier, description, owner, and version number.
   - Enter document details into the Document Control Register.
2. **Storage of Physical Documents**
   - Store documents in secure, access-controlled storage areas (e.g., locked cabinets, document vaults).
   - Maintain environmental controls as necessary (humidity, temperature, fire protection).
   - Only authorized personnel may access physical document storage.
3. **Storage of Electronic Documents**
   - Utilize approved document management systems (DMS) with audit trails and role-based access.
   - Backup electronic records according to IT policy and store backups securely offsite or in the cloud.
   - Ensure data encryption for sensitive records in storage and during transmission.
4. **Access Control**
   - Grant document access strictly on a need-to-know basis.
   - Maintain logs of document access and retrieval (manual or electronic).
   - Review access permissions semi-annually and update as required.
5. **Document Retrieval**
   - Request retrieval through the Records Management Staff or via the DMS, as applicable.
   - Track each retrieval and return in the Document Control Register or DMS audit log.
   - Return physical documents to the original storage location promptly after use.
6. **Document Retention and Disposal**
   - Follow approved retention schedules based on document type and regulatory/organizational requirements.
   - Conduct periodic reviews to identify and segregate records for destruction or permanent archival.
   - Destroy physical documents by shredding; delete electronic records securely using IT-sanctioned methods.
   - Document destruction with date, method, and responsible person's signature.
7. **Archival Process**
   - Transfer documents exceeding active use to archival storage, with clear labeling and control.
   - Store archival records in a secure, environmentally controlled location or sanctioned digital archive.

    - Maintain an up-to-date archive index for efficient retrieval.

Retention Schedule Example:

Document Type	Retention Period	Final Disposition
Regulatory Filings	10 years	Shred (physical) / Secure Delete (digital)
Quality Records	7 years	Shred / Secure Delete
Financial Reports	7 years	Shred / Secure Delete
Employee Records	Termination + 5 years	Shred / Secure Delete
General Correspondence	2 years	Shred / Secure Delete

References:

- Relevant regulatory and legal requirements (e.g., GDPR, HIPAA, SOX, 21 CFR Part 11)
- Organizational policy documents on document management
- IT Security Policy and Data Management Guidelines

Revision History:

Date	Version	Description of Change	Author/Approver
2024-06-20	1.0	Initial template release	QA Manager