SOP Template: Archiving and Record-Keeping of All Related Documents

This SOP details the **archiving and record-keeping** process for all related documents, ensuring proper organization, secure storage, and easy retrieval of records. It covers document categorization, retention periods, digital and physical storage methods, access control, backup procedures, and compliance with legal and regulatory requirements to maintain accurate and reliable documentation over time.

1. Purpose

To establish a systematic process for archiving and record-keeping, ensuring documents are organized, securely stored, retrievable, and compliant with regulatory requirements.

2. Scope

This SOP applies to all staff involved in creating, handling, archiving, and retrieving organizational documents in both physical and digital formats.

3. Responsibilities

- **Document Owners:** Classify and submit documents for archiving.
- **Records Management Team:** Maintain the archive, oversee storage, manage access, and ensure compliance.
- **IT Department:** Manage and backup digital records.
- **All Employees:** Follow established procedures for document handling and archiving.

4. Procedure

1. **Document Categorization**
   - Assign document type, category, and unique identifier.
   - Label physical files accordingly; include metadata for digital documents.
2. **Retention Periods**
   - Refer to the [Document Retention Schedule](#).
   - Review and update retention periods annually or as regulations change.
3. **Archiving Physical Documents**
   - Store in secure, access-controlled locations.
   - Use labeled folders/boxes and maintain a log of stored items.
   - Protect from damage (moisture, heat, insects, etc.).
4. **Archiving Digital Documents**
   - Store on secure file servers or document management systems (DMS).
   - Organize by category and include relevant metadata.
   - Maintain regular digital backups.
5. **Access Control**
   - Restrict access based on user roles and document classification.
   - Maintain an access log for sensitive information.
6. **Backup Procedures**
   - Back up digital records daily, store offsite copies weekly.
   - Test backup restoration quarterly to ensure data integrity.
7. **Disposal of Records**
   - Shred physical records after retention period unless legal hold is in place.
   - Permanently delete digital records per protocol; document the disposal.
8. **Compliance & Audits**
   - Audit records management practices annually.
   - Ensure adherence to data protection, privacy, and industry regulations.

5. Document Retention Schedule (Example)

Document Type	Retention Period	Storage Method
Contracts	7 years after expiration	Physical & Digital
Financial Records	7 years	Digital

HR Records	10 years after termination	Secure Digital
Project Documentation	5 years after project closure	Digital
Compliance Reports	Permanent	Digital

6. Related Documents & References

- Data Protection Policy
- Information Security SOP
- Local and national data retention regulations

7. Revision History

Version	Date	Description	Author
1.0	2024-06-25	Initial template creation	[Your Name]