

SOP Template: Documentation and Record-Keeping Procedures

This SOP defines **documentation and record-keeping procedures** essential for maintaining accurate, organized, and secure records. It covers the proper methods for data entry, document storage, retrieval systems, confidentiality protocols, and the retention schedule to ensure compliance with legal and regulatory requirements. The goal is to support efficient information management, facilitate audits, and preserve the integrity of organizational records.

1. Purpose

To establish standardized procedures for documentation and record-keeping to ensure data accuracy, integrity, security, and easy retrieval.

2. Scope

This SOP applies to all departments and staff responsible for creating, handling, storing, and retrieving organizational records.

3. Responsibilities

- **Record Custodians:** Ensure records are properly maintained and updated.
- **All Staff:** Follow documentation and confidentiality procedures as outlined.
- **Management:** Monitor compliance and provide necessary training.

4. Procedures

4.1 Data Entry

- Ensure all records are accurate, complete, and legible.
- Enter information promptly after each transaction or event.
- Use organization-approved forms and digital templates when applicable.
- Review entries for errors or omissions before submission.

4.2 Document Storage

- Store physical records in secure, organized filing systems (e.g., labeled cabinets, restricted-access rooms).
- Electronic records should be stored on secure servers or approved cloud services with regular backups.
- Classify records by type, date, and department for easy retrieval.
- Ensure all storage locations are protected from hazards (e.g., fire, flooding, unauthorized access).

4.3 Record Retrieval

- Establish a systematic indexing or cataloging system for all records.
- Grant retrieval access only to authorized personnel.
- Maintain a log of record access and retrieval activities.
- Return records to storage promptly after use.

4.4 Confidentiality Protocols

- Restrict access to sensitive records to authorized staff.
- Secure records using passwords, locks, or encryption as appropriate.
- Never disclose confidential information to unauthorized persons.
- Report any suspected data breach immediately to management.

4.5 Record Retention and Disposal

Record Type	Retention Period	Disposal Method
Employee Records	7 years after termination	Shredding (physical), Secure deletion (digital)
Financial Records	10 years	Shredding (physical), Secure deletion (digital)
Client Files	5 years after service completion	Shredding (physical), Secure deletion (digital)

General Correspondence	2 years	Shredding (physical), Secure deletion (digital)
------------------------	---------	---

- Follow industry, legal, and regulatory standards on record retention.
- Document the destruction of records in a disposal log.
- Records pending disposal should be clearly marked and stored separately.

5. Compliance and Auditing

- Regularly review record-keeping practices for compliance with relevant regulations (e.g., GDPR, HIPAA).
- Conduct annual audits of records and associated processes.
- Report findings to management and implement corrective actions as needed.

6. Training

- Provide onboarding and periodic training for all staff on documentation practices and confidentiality requirements.
- Update training materials as procedures and regulations evolve.

7. Revision History

Version	Date	Description	Approved By
1.0	2024-06-15	Initial SOP Template Release	Documentation Manager