Standard Operating Procedure (SOP)

Record-Keeping, Audit Trails, and Document Retention Policies

This SOP establishes comprehensive guidelines for **record-keeping, audit trails, and document retention policies**. It covers the systematic documentation of all relevant data, maintaining secure and accurate audit trails to ensure accountability, and defining retention periods for different types of documents in compliance with regulatory requirements. The purpose is to support transparency, facilitate audits, protect sensitive information, and ensure proper management and retrieval of records throughout their lifecycle.

1. Purpose

To ensure comprehensive, accurate, and compliant handling of all documents through effective record-keeping, establishment of audit trails, and enforcement of document retention schedules.

2. Scope

This SOP applies to all employees, contractors, and departments involved in generating, handling, storing, or retrieving organizational records in paper or electronic format.

3. Definitions

- **Record-Keeping:** The act of creating, storing, managing, and disposing of documents and data.
- **Audit Trail:** A chronological record of system and user activities used to verify the accuracy and integrity of records.
- **Document Retention Policy:** Guidelines specifying how long documents should be kept before they are securely disposed of.

4. Responsibilities

- **Department Heads:** Ensure adherence to SOP within their teams.
- **Records Manager:** Oversees implementation and compliance of all record-keeping procedures.
- **IT Department:** Manages electronic audit trails and secure storage solutions.
- **All Employees:** Responsible for accurate record-keeping and following retention guidelines.

5. Procedure

1. **Record Creation and Classification**
    - Classify documents by type (e.g., administrative, financial, HR, legal, operational).
    - Assign unique identifiers where necessary.
    - Ensure all entries are accurate, complete, and timely.
2. **Record Maintenance and Storage**
    - Store records in secure, access-controlled environments (physical or electronic).
    - Regularly back up electronic records.
    - Store sensitive data in encrypted formats.
3. **Audit Trails**
    - Enable audit logging on systems managing critical records.
    - Document creation, access, modification, and deletion activities.
    - Retain audit logs for a minimum duration as per policy (see section 6).
    - Review audit trails periodically for unauthorized activities.
4. **Retention and Disposal**
    - Follow the retention periods as defined below (see section 6).
    - Ensure records due for disposal are securely destroyed (shredding, data wiping, etc.).
    - Document the destruction and obtain approvals as required.
5. **Compliance and Review**
    - Periodically review this SOP for regulatory updates and process improvements.
    - Conduct audits to ensure ongoing compliance.

6. Document Retention Schedule

Document Type	Retention Period	Notes
Financial Records	7 years	Invoices, statements, tax returns
HR Records	6 years after employment ends	Employee files, contracts

Legal Documents	Permanent or as specified by law	Contracts, litigation documents
Operational Records	3 years	Meeting minutes, project records
Email Correspondence	2 years	Unless linked to specific projects or legal holds
Audit Logs	1 year minimum	System and user activity logs

7. Security and Confidentiality

- Access to sensitive records and audit trails is strictly limited by role and necessity.
- All staff are trained on data privacy and secure handling procedures.
- Breaches must be reported immediately and investigated.

8. References

- Applicable local, state, and federal regulations
- Data protection and privacy laws (e.g., GDPR, HIPAA, etc.)
- Company Information Security Policy

9. Revision History

Version	Date	Summary of Changes	Approved By
1.0	[Insert Date]	Initial draft	[Insert Name/Role]

This SOP is a controlled document. Uncontrolled copies may not reflect the current policy. Direct all questions or required updates to the Records Manager.