

# Standard Operating Procedure (SOP): Document Retention and Disposal Policies

This SOP defines the **document retention and disposal policies**, including guidelines for the classification, storage, retention periods, secure disposal methods, compliance with legal and regulatory requirements, and responsibilities for managing organizational records. The purpose is to ensure the systematic management of documents to protect sensitive information, support operational efficiency, and meet audit and compliance standards.

## 1. Purpose

To establish standardized procedures for retaining and disposing of organizational documents, ensuring compliance with legal, regulatory, and operational requirements, and to safeguard sensitive information.

## 2. Scope

This SOP applies to all employees, contractors, and third-party service providers involved in the creation, management, storage, or disposal of documents within the organization, both in physical and electronic formats.

## 3. Definitions

- **Document:** Any recorded information, regardless of format (paper, electronic, etc.)
- **Retention Period:** The length of time a document must be kept before it is disposed of.
- **Secure Disposal:** Methods of destroying documents to ensure sensitive data is irretrievable.
- **Classification:** The process of categorizing documents based on their content, sensitivity, and retention requirements.

## 4. Roles and Responsibilities

- **Records Manager:** Oversees implementation of this SOP and ongoing compliance.
- **Department Managers:** Ensure proper classification, storage, retention, and disposal of department documents.
- **Employees:** Adhere to these policies and report any non-compliance issues.
- **IT Department:** Manages secure storage and deletion of electronic records.

## 5. Document Classification

Documents should be classified as follows:

- **Confidential:** Sensitive or proprietary information, access restricted.
- **Internal Use Only:** Not for public release, general employee access permitted.
- **Public:** Approved for public dissemination.

## 6. Storage Guidelines

- Physical records must be stored in locked, secure environments.
- Electronic records must be stored on approved, access-controlled systems with regular back-ups.
- No unauthorized copies should be created or retained.

## 7. Retention Periods

Document Type	Retention Period	Reference
Financial Records	7 years	GAAP, IRS
Employee Records	6 years after termination	State & Federal Labor Laws
Contracts	7 years after expiry	Legal

Client Communications	5 years	Industry Regulations
General Correspondence	2 years	Best Practice

\*Consult legal counsel to customize retention periods according to applicable laws and regulations.

## 8. Secure Disposal Methods

- **Physical Records:** Cross-cut shredding, incineration, or certified secure disposal services.
- **Electronic Records:** Use of secure deletion tools/software to erase data, ensuring it is unrecoverable.
- **Media Disposal:** Degaussing or physical destruction of storage media, as appropriate.

## 9. Compliance and Auditing

- Periodic audits to review compliance with retention and disposal policies.
- Documentation of all records destroyed, including date, method, and responsible personnel.
- Immediate reporting of any data breaches or non-compliance incidents.

## 10. Training and Review

- Annual employee training on document retention/disposal requirements and updates.
- Review and update this SOP bi-annually or as required by regulatory changes.

## 11. References

- Applicable federal, state, and industry regulations
- Organizational data protection and privacy policies

## 12. Revision History

Version	Date	Description	Author
1.0	2024-06-01	Initial Template	[Author Name]