SOP: Document Retention and Archiving Standards

This SOP defines the **document retention and archiving standards** to ensure systematic management, storage, and disposal of organizational records. It includes guidelines on classification, retention periods, secure storage, and authorized access to documents, aiming to maintain compliance with legal requirements, protect sensitive information, and support efficient retrieval and audit processes.

1. Purpose

To establish uniform standards for the retention, storage, archiving, and disposal of documents in accordance with applicable laws and organizational policies.

2. Scope

This SOP applies to all employees and third parties handling company records in physical or electronic formats.

3. Definitions

- **Record:** Any document, file, or item containing organizational information.
- **Retention Period:** The required time frame for which a record must be kept.
- **Archiving:** The process of storing inactive records for long-term preservation.
- **Disposal:** The secure destruction of records after the retention period expires.

4. Roles & Responsibilities

- **Document Owners:** Ensure proper classification and ongoing oversight of documents.
- **Records Management Team:** Implement and maintain retention and archiving processes.
- **Authorized Users:** Access documents as per defined permissions and protect confidentiality.

5. Document Classification

Documents must be classified according to their content and sensitivity, typically as:

- Confidential
- Internal Use
- Public

Classifications must be clearly indicated on all documents.

6. Retention Periods

Document Type	Retention Period	Archival Location
Financial Records	7 years	Secure Archive Room / Encrypted Storage
HR Records	6 years after termination	HR Vault / Secure Digital Archive
Client Contracts	7 years after expiry	Contract Archive / Legal Repository
General Correspondence	2 years	Departmental Archive

Document owners are responsible for adherence to retention schedules and updating records as applicable laws change.

7. Secure Storage & Archiving

- Physical records must be stored in locked, access-controlled areas.
- Electronic records must be encrypted and stored on secure, backed-up servers.
- Archived documents should be indexed for efficient retrieval.

8. Access Control

- Access to documents is restricted to authorized personnel only.
- Access logs should be maintained and regularly reviewed.
- Requests for access require documented manager approval.

9. Disposal and Destruction

- Upon expiration of the retention period, records must be securely destroyed (e.g., shredding, digital wiping).
- Disposal actions must be logged and, if necessary, witnessed or certified.
- No records under legal hold or audit investigation may be deleted.

10. Compliance & Audit

- Periodic audits should verify compliance with this SOP.
- Non-compliance must be reported to the Records Management Team for corrective action.

11. Revision & Review

This SOP should be reviewed annually or upon significant regulatory change. All updates must be documented in the revision history below.

12. Revision History

Version	Date	Description	Author
1.0	2024-06-20	Initial draft	Records Manager