SOP: Document Retention and Destruction Schedules

This SOP establishes **document retention and destruction schedules** to ensure proper management of records throughout their lifecycle. It defines the time frames for retaining various types of documents, outlines secure storage methods, and specifies procedures for the systematic and compliant destruction of records. The goal is to maintain regulatory compliance, protect sensitive information, and optimize organizational record-keeping practices.

1. Purpose

To define standardized procedures for document retention, secure storage, and destruction to ensure compliance with legal, regulatory, and organizational requirements.

2. Scope

This SOP applies to all staff, contractors, and departments handling physical or electronic records within the organization.

3. Responsibilities

- **Records Manager:** Oversees retention and destruction procedures, maintains master schedules, audits compliance.
- **Department Heads:** Ensure staff follow procedures for their document types.
- **All Employees:** Comply with retention schedules and destruction protocols.

4. Document Retention Schedule

Document Type	Retention Period	Storage Method	Responsible Party
Financial Records (invoices, ledgers, tax returns)	7 years	Secure file server & locked cabinets	Finance Department
Human Resource Files (personnel files, payroll)	7 years after termination	HRMS & secure room	HR Department
Contracts & Agreements	7 years after expiration	Encrypted digital storage	Legal Department
Medical/Client Records	10 years after last service	HIPAA-compliant server	Service Department
General Correspondence	3 years	Shared drives	All Departments
Board Meeting Minutes	Permanently	Archive vault & digital backup	Corporate Secretary

5. Storage Procedures

- All sensitive records are stored in locked cabinets or password-protected digital systems.
- Access is restricted by role and only to authorized personnel.
- Backups of electronic records are performed weekly and stored offsite or in secure cloud environments.

6. Destruction Procedures

1. Records identified as past the retention period are flagged for destruction by the Records Manager.
2. **Physical Records:** Secure shredding by authorized staff or vendor with documented certificate of destruction.
3. **Electronic Records:** Permanent deletion using secure wipe tools or NFTs; emails purged from backup and mail server.

4. For highly sensitive documents, dual authorization is required before destruction.
5. Destruction logs must be maintained for audit trail.

7. Compliance & Audit

- Record retention and destruction practices will be reviewed annually for compliance.
- Non-compliance may result in disciplinary action and/or legal consequences.

8. Revision History

Version	Date	Description	Approved By
1.0	2024-06-15	Initial SOP release	Compliance Officer