Standard Operating Procedure (SOP): Document Storage, Backup, and Archiving Procedures

This SOP defines the **document storage, backup, and archiving procedures** to ensure the secure management and preservation of organizational records. It covers guidelines for proper document categorization, secure physical and digital storage methods, regular data backup schedules, encryption and access controls, long-term archival strategies, and compliance with regulatory retention requirements. The goal is to maintain data integrity, prevent loss, and enable efficient retrieval of documents when needed.

1. Purpose

To outline procedures for secure storage, routine backup, and systematic archiving of documents, ensuring organizational records are protected, retrievable, and compliant with legal and regulatory standards.

2. Scope

This SOP applies to all employees, contractors, and departments handling organizational records in both physical and electronic formats.

3. Definitions

- **Document:** Any recorded information, whether in paper or electronic form.
- **Backup:** The process of making copies of data for recovery in case of data loss.
- **Archive:** Documents retained for long-term reference and legal compliance, stored separately from active records.
- **Retention Period:** The minimum time a document must be kept before disposal.

4. Responsibilities

- **Records Manager:** Oversees implementation and compliance with this SOP.
- **IT Department:** Manages digital storage, backup, access controls, and archiving systems.
- **Department Heads:** Ensure adherence to categorization and storage procedures within their teams.
- **All Staff:** Follow storage and retrieval protocols for both physical and electronic documents.

5. Document Categorization

- Classify documents as: Confidential, Internal Use, or Public.
- Label documents with creation date, author, and retention period.
- Maintain a document inventory list or log with classification, storage location, and access rights.

6. Storage Procedures

6.1 Physical Documents

- Store in fireproof, secure cabinets or locked rooms with controlled access.
- Limit access to authorized personnel.
- Keep storage areas clean, dry, and protected from direct sunlight and pests.

6.2 Digital Documents

- Save in designated, access-controlled network folders or approved cloud platforms.
- Apply encryption to sensitive files during storage and transmission.
- Regularly review and update access permissions.

7. Data Backup Procedures

Type	Frequency	Location
Full Backup	Weekly	On-site & Off-site/Cloud
Incremental Backup	Daily	On-site & Cloud

- Conduct and log backup operations as per schedule.
- Test restore procedures quarterly to ensure data integrity.
- Encrypt all backup data.
- Restrict access to backup media to authorized personnel only.

8. Archiving and Retention

- Transfer inactive records to long-term archives after their active use phase ends.
- Store archives in secured, controlled environments (physical or digital).
- Label archives with retention period, destroy date, and access controls.
- Follow legal and regulatory retention schedules applicable to the document type.
- Securely and irreversibly destroy records past their retention periods, following approved destruction methods (shredding, DOD-wipe, etc.).

9. Compliance and Audit

- Conduct regular audits of storage, backup, and archival processes for adherence to this SOP.
- Report breaches or non-compliance to the Records Manager immediately.

10. Revision and Review

- This SOP shall be reviewed annually, or upon significant change in regulations or internal processes.

11. References

- Company Information Security Policy
- Applicable Legislative and Regulatory Requirements (e.g., GDPR, HIPAA)

APPENDIX: Quick Reference Checklist

- Are all documents categorized and labeled?
- Are storage areas (physical/digital) secure and access-controlled?
- Are backup schedules documented and followed?
- Are backup and restore procedures tested regularly?
- Are archival and destruction done per retention policies?
- Are non-compliance and security incidents reported?